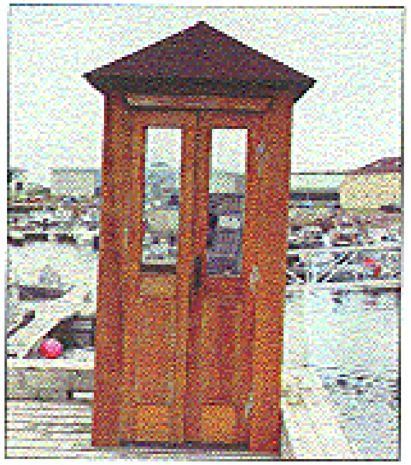
Payphones on Planet Earth

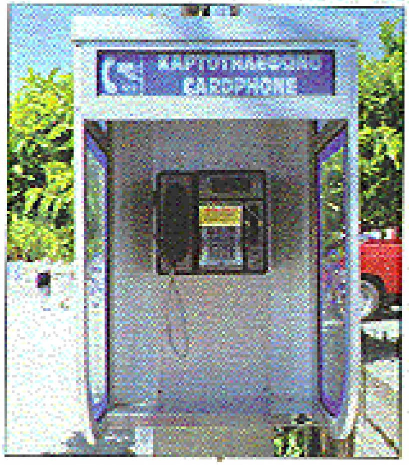
St. Pierre



Few people know of the islands of St. Pierre & Miquelon just off the coast of Newfoundland. These North American islands are actually part of France! And this phone, found on a wharf, belongs to France Telecom.

Marc Cormier

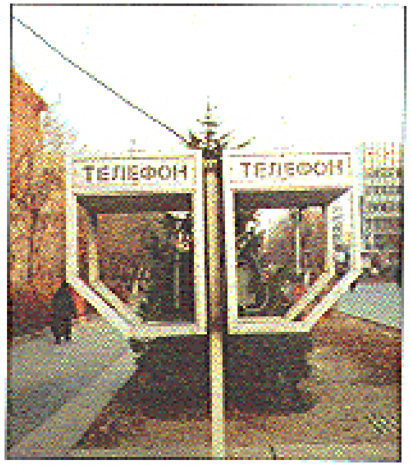
Greece



From Knossos on the island of Crete.

David Ruderman

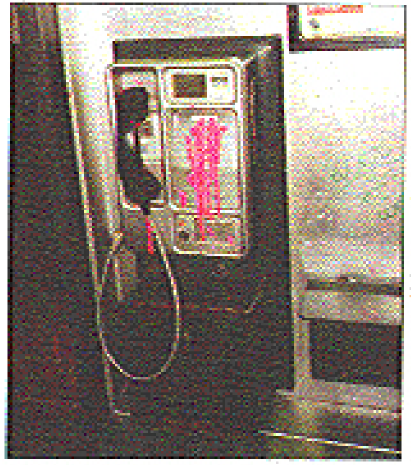
Kazakhstan



Found in the city of Almaty.

Juarez

England



A vandalized phone in London with possible murder evidence.

Mik

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

2600

$4.50 US $5.50 CAN

S T A F F

Editor-In-Chief
Emmanuel Goldstein

Layout
Ben Sherman

Cover Design
Zofia, The Chopping Block Inc.

Office Manager
Tampruf

"First and foremost, every White House person who has got access to classified information knows that you should not ever transmit any classified material either by cellular phone, non-protected phone, or by beeper. That is drilled into us fairly well. And as a general proposition, we are alerted to the sensitivity of all electronic communications — walkie-talkies, cellular phones, and beepers. And I think there are probably some staffers who now had a fairly painful reminder that these are indeed public transmissions. So their private matters are now more widely known. It probably will be a useful deterrent." - White House Press Secretary Mike McCurry commenting September 22, 1997 on the release by 2600 staffers of White House pager transmissions. He seems to agree with us that these are indeed "public transmissions." Maybe he can get the word to Louis Freeh.

Writers: Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, John Drake, Paul Estev, Mr. French, Bob Hardy, Thomas Icom, Joe630, Kingpin, Kevin Mitnick, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Thee Joker, Mr. Upsetter.

Network Operations: Phiber Optik, Manos.

Network Operations: Mark0.

Webmaster: Kiratoy.

Voice Mail: Netweasel.

Inspirational Music: Alan Lamb, ATR, The Skolars, Eric Morris, The Oppressed.

Shout Outs: Izaac, Iggy, Porkchop, Wicked, Digiflesh, Mazzy, Stinky, Sedena, Meenie, DHP, Support, Ace, Maxx, Espidre & Wasted.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAisAvdgAAAEEAKDyMmRGmirxC4G3AsIxskKpCP71vUFRRzVXpLIo3+Jr10+9
PGFwAP23Tg1Xho5a8c3J8hstYCowzsI168nRORB4J8Rwd+tMz5l8KeKi9LzlSM1R
hLNJTm8vRjzHd8nQ8ed3734wLMCyEpozzavu/0UthMLb6UCPC2srXlHoedr1AAUR
t3ZlbW1FbnV1bEB3ZWxsLnNmLnNhLnVz
=W1M8
-----END PGP PUBLIC KEY BLOCK-----
```

evidence

*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, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds).
Overseas - $30 individual, $65 corporate.
Back issues available for 1984-1996 at $25 per year, $30 per year overseas.
Individual issues available from 1988 on at $6.25 each, $7.50 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: 516-751-2600, 2600 FAX Line: 516-474-2677.

Sobering Facts

You may be wondering why this issue is so incredibly late. You may also, depending on who you listen to, be surprised to see it at all.

We've basically been hit with a crisis that is part of the risk any publisher takes. We owe it to our readers to explain just what's been going on.

When we send issues to stores, we have to go through a process that involves companies known as distributors. The vast majority of stores will not deal directly with publishers and most publishers don't have the time or staff to deal directly with individual stores. This is where distributors come in. They take care of contacting stores and getting our issues to them. In turn the stores pay them and the distributors pay us. By the time we get paid, it's generally at least half a year since the issue was printed. The distributors keep around half the cover price (some actually want more than this) and we have to pay for shipping. In the past we would get unsold issues returned which meant that we could still sell them as back issues. The distributors began to phase this out, sending us the covers of unsold issues and then eventually just a piece of paper saying that a certain number went unsold. Each unsold issue turned into a 100% loss for us. But that really wasn't a major deal for us since our sales percentage wasn't bad thanks to our readers. However, it shows how the publishing industry has turned increasingly against the publisher. And it sets the stage for the problem that has befallen us.

For a number of years a distributor based in Austin, Texas known as Fine Print has been getting us onto shelves in Barnes and Noble, Borders, Hastings, and a large number of independent stores nationwide. They've done this for all kinds of independent zines for years. But, during those same years, there were all kinds of financial mismanagements taking place there which we didn't have a hint of until fairly recently. It started with a lot of smaller zines not getting paid at all. Some were eventually forced out of business. Early in 1997, Fine Print filed for Chapter 11 protection, owing us nearly $100,000 - printing costs for three issues. And the ironic part of it was that we had no choice but to continue doing business with them since under court order they had to pay their current debts immediately which was more than we would get from our other distributors. Dropping Fine Print would put us in a position where we had to survive for over half a year with no significant payments. Plus, doing this would have hurt Fine Print's chances of coming back, perhaps irreparably. We decided to continue dealing with them until the reorganization plan was finalized and hope for the best.

The first signs of trouble came this summer when we began to not get paid for the current debts as well. We started to run out of money to pay bills, our web site development had to be frozen, paid staff became unpaid staff, and numerous expansions and new projects had to be indefinitely postponed or canceled. We were advised by numerous professional sorts to consider bankruptcy ourselves.

The biggest nail in the coffin came as a result of Beyond Hope, our second hacker conference which took place this summer. By all accounts, the conference was a terrific learning experience and a huge success. Financially, though, we lost over $10,000 on it, mostly due to last minute greed and deception on the part of the venue and our network provider. Ordinarily, we could have handled this and we would have even considered it a worthy expense for all of the positive things that came out of it. However, coupled with the Fine Print problems, it was enough to practically make our financial wounds fatal.

Practically. Because there's one thing we have that most businesses and corporations lack. That is a spirit and a knack for survival. The people who read *2600* and give us moral support were the main reasons we knew we could beat the crap we were facing. And that's exactly what we intend to do. We've had to sacrifice a lot and it hasn't been pleasant. But we have an obligation to those who have gotten us this far and to take the easy way out would be a slap in the face to everyone who has gotten us this far and to everything we believe in. That is why, no matter how bad things get, we won't declare bankruptcy and absolve ourselves of responsibility to our debtors and our readers. We know how that feels and we won't continue the cycle.

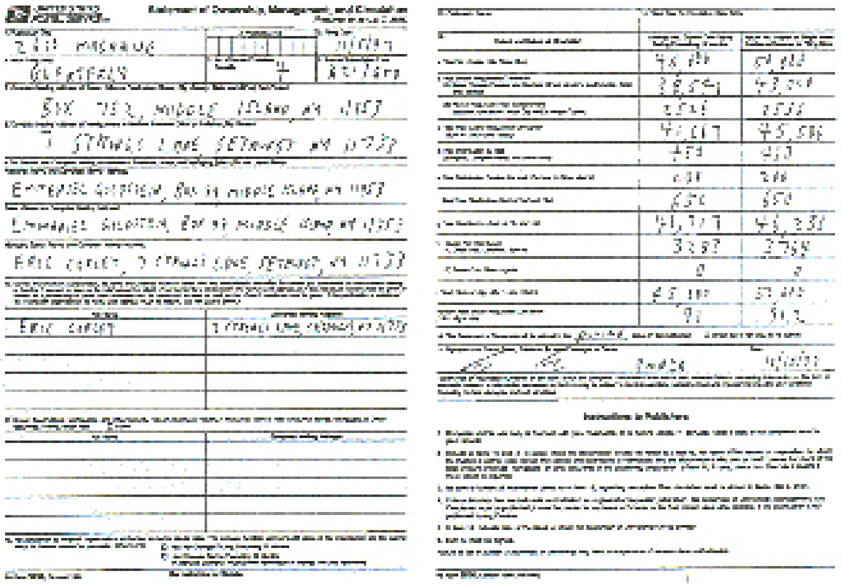
Let's make something else clear as well: we don't want people to send us money to get us out of this. It wouldn't be good for us to know that we could get into all kinds of financial jams and have someone always there to bail us out. But we have come up with a plan where our readers can help and at the same time get stuff back. We've dropped prices on a number of things that we sell that we already have in stock. Since we already have all of this merchandise, we don't have to worry about paying for it. If enough people buy these things, we'll have more money to work with and we'll be able to hopefully pay a larger percentage of our bills if not all of them. Look for details on specifics in various ads in this issue.

Because of the lateness this has caused, we have suspended putting the season of our issues on the front cover. If the Autumn issue comes out nearer to Winter, a lot of places may pull it off the shelves too soon. We are trying to tighten up our schedule so that, inside of a year, we will be back on track.

The reorganization plan was recently announced by Fine Print and the cash settlement offered to us was a whopping $150. Needless to say, we're now taking the plunge and moving our accounts to other distributors where it will take a while for the sales to reach us. Once that happens, again within the next year, we expect things to start turning around. After all, had we been getting paid all along, we'd be in pretty good shape right now.

We're sorry to put a damper on what should be a positive period. Beyond Hope was an inspiration to a large part of the hacker community and was technically as flawless as we had hoped for. Once we climb out of the hole we will begin planning the next one. We've made tremendous progress getting our weekly radio show out on the net and now, thanks to bandwidth donations, regular live listeners include people all over the world. It will take a great deal more than financial disaster to stop hacker progress.

We bear no animosity towards Fine Print. Please don't turn off their phones - they have enough problems. They helped to get us into a lot of places we may never have reached. We hope they work out their problems and once again help independent zines reach a greater number of people. There's no question that people are hungry for information and alternative ideas in every region of the country. The most important thing is to make sure the ideas keep on flowing.



Statement of Ownership, Management, and Circulation

2600 MAGAZINE

QUARTERLY

BOX 752, MIDDLE ISLAND NY 11953

7 STRONG'S LANE SETAUKET NY 11733

EMMANUEL GOLDSTEIN, BOX 99 MIDDLE ISLAND NY 11953

EMMANUEL GOLDSTEIN, BOX 99 MIDDLE ISLAND NY 11953

ERIC CORLEY, 7 STRONG'S LANE SETAUKET NY 11733

ERIC CORLEY	7 STRONG'S LANE SETAUKET NY 11733

[illegible]	46,186	54,662
[illegible]	38,581	43,258
[illegible]	2,536	2,538
[illegible]	41,117	45,596
[illegible]	478	413
[illegible]	238	248
[illegible]	656	650
[illegible]	41,773	46,235
[illegible]	3,387	2,769
[illegible]	0	0
[illegible]	45,160	57,4[illegible]
[illegible]	97	9[illegible]

Instructions to Publishers

B U S T E D !

A COMPLETE GUIDE TO GETTING CAUGHT

by Agent Steal
From Federal Prison, 1997
agentsteal@usa.net
Contributions and editing by Minor Threat

The likelihood of getting arrested for computer hacking has increased to an unprecedented level. No matter how precautionary or sage you are you're bound to make mistakes. And the fact of the matter is if you have trusted anyone else with the knowledge of what you are involved in, you have made your first mistake. For anyone active in hacking I cannot begin to stress the importance of the information contained in this file. To those who have just been arrested by the Feds, reading this file could mean the difference between a three-year or a one-year sentence. To those who have never been busted, reading this file will likely change the way you hack, or stop you from hacking altogether. I realize my previous statements are somewhat lofty, but in the 35 months I spent incarcerated I've heard countless inmates say it: "If I knew then what I know now." I doubt that anyone would disagree: The criminal justice system is a game to be played, both by prosecution and defense. And if you have to be a player, you would be wise to learn the rules of engagement. The writer and contributors of this file have learned the hard way. As a result we turned our hacking skills during the times of our incarceration towards the study of criminal law and, ultimately, survival. Having filed our own motions, written our own briefs and endured life in prison, we now pass this knowledge back to the hacker community. Learn from our experiences... and our mistakes.

Part I - Federal Criminal Law

A. The Bottom Line - Relevant Conduct

For those of you with a short G-phile attention span I'm going to cover the single most important topic first. This is probably the most substantial misunderstanding of the present criminal justice system. The subject I am talking about is referred to in legal circles as "relevant conduct." It's a bit complex and I will get into this. However, I have to make this crystal clear so that it will stick in your heads. It boils down to two concepts:

1) Once you are found guilty of even one count, every count will be used to calculate your sentence.

Regardless of whether you plea bargain to one count or 100, your sentence will be the same. This is assuming we are talking about hacking, code abuse, carding, computer trespass, property theft, etc. All of these are treated the same. Other crimes you committed (but were not charged with) will also be used to calculate your sentence. You do not have to be proven guilty of every act. As long as it appears that you were responsible, or someone says you were, then it can be used against you. I know this sounds insane, but it's true; it's the preponderance of evidence standard for relevant conduct. This practice includes using illegally seized evidence and acquittals as information in increasing the length of your sentence.

2) Your sentence will be based on the total monetary loss.

The Feds use a sentencing table to calculate your sentence. It's simple; More Money = More Time. It doesn't matter if you tried to break in 10 times or 10,000 times. Each one could be a count but it's the loss that matters. And an unsuccessful attempt is treated the same as a completed crime. It also doesn't matter if you tried to break into one company's computer or 10. The government will quite simply add all of the estimated loss figures up, and then refer to the sentencing table.

B. Preparing For Trial

I've been trying to be overly simplistic with my explanation. The United States Sentencing Guidelines (U.S.S.G.) are in fact quite complex. So much so that special law firms are forming that deal only with sentencing. If you get busted, I would highly recommend hiring one. In some cases it might be wise to avoid hiring a trial attorney and go straight to one of these "Post Conviction Specialists." Save your money, plead out, do your time. This may sound a little harsh, but considering the fact that the U.S. Attorney's Office has a 95% conviction rate, it may be sage advice. However, I don't want to gloss over the importance of a ready for trial posturing. If you have a strong trial attorney, and have a strong case, it will go a long way towards good plea bargain negotiations.

C. Plea Agreements and Attorneys

Your attorney can be your worst foe or your finest advocate. Finding the proper one can be a difficult task. Costs will vary and typically the attorney asks you how much cash you can raise and then says, "that amount will be fine." In actuality a simple plea and sentencing should run you around $15,000. Trial fees can easily soar into the 6 figure category. And finally, a post conviction specialist will charge $5000 to $15,000 to handle your sentencing presentation with final arguments.

You may however, find yourself at the mercy of The Public Defenders Office. Usually they are worthless; occasionally you'll find one who will fight for you. Essentially it's a crap shoot. All I can say is if you don't like the one you have, fire them and hope you get appointed a better one. If you can scrape together $5000 for a sentencing (post conviction) specialist to work with your public defender, I would highly recommend it. This specialist will make certain the judge sees the whole picture and will argue in the most effective manner for a light or reasonable sentence. Do not rely on your public defender to thoroughly present your case. Your sentencing hearing is going to flash by so fast you'll walk out of the courtroom dizzy. You and your defense team need to go into that hearing fully prepared, having already filed a sentencing memorandum.

The plea agreement you sign is going to affect you and your case well after you are sentenced. Plea agreements can be tricky business and if you are not careful or are in a bad defense position (the case against you is strong), your agreement may get the best of you. There are many issues in a plea to negotiate over. But essentially my advice would be to avoid signing away your right to appeal. Once you get to a real prison with real jailhouse lawyers you will find out how badly you got screwed. That issue notwithstanding, you are most likely going to want to appeal. This being the case you need to remember two things: bring all your appealable issues up at sentencing and file a notice of appeal within 10 days of your sentencing. Snooze and lose.

I should however, mention that you can appeal some issues even though you signed away your rights to appeal. For example, you cannot sign away your right to appeal an illegal sentence. If the judge orders something that is not permissible by statute, you then have a constitutional right to appeal your sentence.

I will close this subpart with a prison joke. Q: How can you tell when your attorney is lying? A: You can see his lips moving.

D. Conspiracy

Whatever happened to getting off on a technicality? I'm sorry to say those days are gone, left only to the movies. The courts generally dismiss many arguments as "harmless error" or "the government acted in good faith." The most alarming trend, and surely the root of the prosecution's success, is the liberally worded conspiracy laws. Quite simply, if two or more people plan to do something illegal, and one of them does something in furtherance of the objective (even something legal), then it's a crime. Yes, it's true. In America it's illegal to simply talk about committing a crime. Paging Mr. Orwell. Hello?

Here's a hypothetical example to clarify this. Bill G. and Marc A. are hackers (can you imagine?). Bill and Marc are talking on the phone and unbeknownst to them the FBI is recording the call. They talk about hacking into Apple's mainframe and erasing the prototype of the new Apple Web Browser. Later that day, Marc does some legitimate research to find out what type of mainframe and operating system Apple uses. The next morning, the Feds raid Marc's house and seize everything that has wires. Bill and Marc go to trial and spend millions to defend themselves. They are both found guilty of conspiracy to commit unauthorized access to a computer system.

E. Sentencing

At this point it is up to the probation department to prepare a report for the court. It is their responsibility to calculate the loss and identify any aggravating or mitigating circumstances. Apple Computer Corporation estimates that if Bill and Marc had been successful it would have resulted in a loss of $2 million. This is the figure the court will use. Based on this basic scenario our dynamic duo would receive roughly three-year sentences.

As I mentioned, sentencing is complex and many factors can decrease or increase a sentence, usually the latter. Let's say that the FBI also found a file on Marc's computer with 50,000 unauthorized account numbers and passwords to The Microsoft Network. Even if the FBI does not charge him with this, it could be used to increase his sentence. Generally the government places a $200-per-account attempted loss on things of this nature (i.e., credit card numbers and passwords are access devices). This makes for a $10 million loss. Coupled with the $2 million from Apple, Marc is going away for about nine years. Fortunately there is a Federal Prison not too far from Redmond, WA so Bill could come visit him.

Some of the other factors to be used in the calculation of a sentence might include the following: past criminal record, how big your role in the offense was, mental disabilities, whether or not you were on probation at the time of the offense, if any weapons were used, if any threats were used, if your name is Kevin Mitnick (heh), if an elderly person was victimized, if you took advantage of your employment position, if you are highly trained and used your special skill, if you cooperated with the authorities, if you show remorse, if you went to trial, etc.

These are just some of the many factors that could either increase or decrease a sentence. It would be beyond the scope of this article to cover the U.S.S.G. in complete detail. I do feel that I have skipped over some significant issues. Nevertheless, if you remember my two main points in addition to how the conspiracy law works, you'll be a long way ahead in protecting yourself.

F. Use of a Special Skill

The only specific "sentencing enhancement" I would like to cover would be one that I am responsible for setting a precedent with. In U.S. v Petersen, 98 F.3d. 502, 9th Cir., the United States Court of Appeals held that some computer hackers may qualify for the special skill enhancement. What this generally means is a 6 to 24 month increase in a sentence. In my case it added eight months to my 33 month sentence bringing it to 41 months. Essentially the court stated that since I used my "sophisticated" hacking skills towards a legitimate end as a computer security consultant, then the enhancement applies. It's ironic that if I were to have remained strictly a criminal hacker then I would have served less time.

The moral of the story is that the government will find ways to give you as much time as they want to. The U.S.S.G. came into effect in 1987 in an attempt to eliminate disparity in sentencing. Defendants with similar crimes and similar backgrounds would often receive different sentences. Unfortunately, this practice still continues. The U.S.S.G. are indeed a failure.

G. Getting Bail

In the past, the Feds might simply have executed their raid and then left without arresting you. Presently this method will be the exception rather than the rule and it is more likely that you will be taken into custody at the time of the raid. Chances are also good that you will not be released on bail. This is part of the government's plan to break you down and win their case. If they can find any reason to deny you bail, they will. In order to qualify for bail, you must meet the following criteria:

- You must be a resident of the jurisdiction in which you were arrested.
- You must be gainfully employed or have family ties to the area.
- You cannot have a history of failure to appear or of escape.
- You cannot be considered a danger or threat to the community.

In addition, your bail can be denied for the following reasons:

- Someone came forward and stated to the court that you said you would flee if released.
- Your sentence will be long if convicted.
- You have a prior criminal history.
- You have pending charges in another jurisdiction.

What results from all of this "bail reform" is that only about 20 percent of persons arrested make bail. On top of that it takes one to three weeks to process your bail papers when property is involved in securing your bond.

Now you're in jail, more specifically you are either in an administrative holding facility or a county jail that has a contract with the Feds to hold their prisoners. Pray that you are in a large enough city to justify its own Federal Detention Center. County jails are typically the last place you would want to be.

H. State vs. Federal Charges

In some cases you will be facing state charges with the possibility of the Feds "picking them up." You may even be able to nudge the Feds into indicting you. This is a tough decision. With the state you will do considerably less time but will face a tougher crowd and conditions in prison. Granted, Federal prisons can be violent too, but generally as a non-violent white collar criminal you will eventually be placed into an environment with other low security inmates. More on this later.

Until you are sentenced, you will remain as a "pretrial inmate" in general population with other inmates. Some of the other inmates will be predatory but the Feds do not tolerate much nonsense. If someone acts up, they'll get thrown in the hole. If they continue to pose a threat to the inmate population, they will be left in segregation (the hole). Occasionally, inmates who are at risk or who have been threatened will be placed in segregation. This isn't really to protect the inmate. It is to protect the prison from a lawsuit should the inmate get injured.

I. Cooperating

Naturally when you are first arrested the suits will want to talk to you. First at your residence and, if you appear to be talkative, they will take you back to their offices for an extended chat and a cup of coffee. My advice at this point is tried and true and we've all heard it before: remain silent and ask to speak with an attorney. Regardless of what the situation is, or how you plan to proceed, there is nothing you can say that will help you. Nothing. Even if you know that you are going to cooperate, this is not the time.

This is obviously a controversial subject, but the fact of the matter is that roughly 80 percent of all defendants eventually confess and implicate others. This trend stems from the extremely long sentences the Feds are handing out these days. Not many people want to do 10 to 20 years to save their buddies' hides when they could be doing 3 to 5. This is a decision each individual needs to make. My only advice would be to save your close friends and family. Anyone else is fair game. In the prison system the blacks have a saying: "Getting down first." It's no secret that the first defendant in a conspiracy is usually going to get the best deal. I've even seen situations where the big fish turned in all his little fish and received 40 percent off his sentence.

Incidentally, being debriefed or interrogated by the Feds can be an ordeal in itself. I would *highly* recommend reading up on interrogation techniques ahead of time. Once you know their methods it will be all quite transparent to you and the debriefing goes much more smoothly.

When you make a deal with the government you're making a deal with the devil himself. If you make any mistakes they will renege on the deal and you'll get nothing. On some occasions the government will trick you into thinking they want you to cooperate when they are not really interested in anything you have to say. They just want you to plead guilty. When you sign the cooperation agreement there are no set promises as to how much of a sentence reduction you will receive. That is to be decided after your testimony, etc. and at the time of sentencing. It's entirely up to the judge. However, the prosecution makes the recommendation and the judge generally goes along with it. In fact, if the prosecution does not motion the court for your "downward departure" the courts' hands are tied and you get no break.

As you can see, cooperating is a tricky business. Most people, particularly those who have never spent a day in jail, will tell you not to cooperate. "Don't snitch." This is a noble stance to take. However, in some situations it is just plain stupid. Saving someone's ass who would easily do the same to you is a tough call. It's something that needs careful consideration. Like I said, save your friends then do what you have to do to get out of prison and on with your life.

I'm happy to say that I was able to avoid involving my good friends and a former employer in the massive investigation that surrounded my case. It wasn't easy. I had to walk a fine line. Many of you probably know that I (Agent Steal) went to work for the FBI after I was arrested. I was responsible for teaching several agents about hacking and the culture. What many of you don't know is that I had close FBI ties prior to my arrest. I was involved in hacking for over 15 years and had worked as a computer security consultant. That is why I was given that opportunity. It is unlikely however, that we will see many more of these types of arrangements in the future. Our relationship ran afoul, mostly due to their passive negligence and lack of experience in dealing with hackers. The government in general now has their own resources, experience, and undercover agents within the community. They no longer need hackers to show them the ropes or the latest security hole.

Nevertheless, if you are in the position to tell the Feds something they don't know and help them build a case against someone, you may qualify for a sentence reduction. The typical range is 20 to 70 percent. Usually it's around 35 to 50 percent. Sometimes you may find yourself at the end of the prosecutorial food chain and the government will not let you cooperate. Kevin Mitnick would be a good example of this. Even if he wanted to roll over, I doubt it would get him much. He's just too big of a fish, too much media. My final advice in this matter is get the deal in writing before you start cooperating.

The Feds also like it when you "come clean" and accept responsibility. There is a provision in the Sentencing Guidelines, 3E1.1, that knocks a little bit of time off if you confess to your crime, plead guilty and show remorse. If you go to trial, typically you will not qualify for this "acceptance of responsibility" and your sentence will be longer.

J. Still Thinking About Trial

Many hackers may remember the Craig Neidorf case over the famous 911 System Operation documents. Craig won his case when it was discovered that the manual in question that he had published in *Phrack* magazine, was not proprietary as claimed but available publicly from AT&T. It was an egg in the face day for the Secret Service.

Don't be misled by this. The government learned a lot from this fiasco and even with the laudable support from the EFF, Craig narrowly thwarted off a conviction. Regardless, it was a trying experience (no pun intended) for him and his attorneys. The point I'm trying to make is that it's tough to beat the Feds. They play dirty and will do just about anything, including lie, to win their case. If you want to really win you need to know how they build a case in the first place.

K. Search and Seizure

There is a document entitled "Federal Guidelines for Searching and Seizing Computers." It first came to my attention when it was published in the 12-21-94 edition of the *Criminal Law Reporter* by the Bureau of National Affairs (Cite as 56 CRL 2023). It's an intriguing collection of tips, cases, mistakes, and, in general, how to bust computer hackers. It's recommended reading.

Search and seizure is an ever-evolving jurisprudence. What's not permissible today may, through some convoluted Supreme Court logic, be permissible and legal tomorrow. Again, a complete treatment of this subject is beyond the scope of this article. But suffice it to say if a Federal agent wants to walk right into your bedroom and seize all of your computer equipment without a warrant he could do it by simply saying he had probable cause (PC). PC is anything that gives him an inkling to believe you were committing a crime. Police have been known to find PC to search a car when the trunk sat too low to the ground or the high beams were always on.

L. Surveillance and Wiretaps

Fortunately the Feds still have to show a little restraint when wielding their wiretaps. It requires a court order and they have to show that there is no other way to obtain the information they seek, a last resort if you will. Wiretaps are also expensive to operate. They have to lease lines from the phone company, pay agents to monitor them 24 hours a day and then transcribe them. If we are talking about a data tap, there are additional costs. Expensive interception/translation equipment must be in place to negotiate the various modem speeds. Then the data has to be stored, deciphered, decompressed, formatted, protocoled, etc. It's a daunting task and usually reserved for only the highest profile cases. If the Feds can seize the data from any other source, like the service provider or victim, they will take that route. I don't know which they hate worse though, asking for outside help or wasting valuable internal resources.

The simplest method is to enlist the help of an informant who will testify "I saw him do it!", then obtain a search warrant to seize the evidence on your computer. Ba da boom, ba da busted.

Other devices include a pen register which is a device that logs every digit you dial on your phone and the length of the calls, both incoming and outgoing. The phone companies keep racks of them at their security departments. They can place one on your line within a day if they feel you are defrauding them. They don't need a court order, but the Feds do.

A trap, or trap and trace, is typically any method the phone company uses to log every number that calls a particular number. This can be done on the switching system level or via a billing database search. The Feds need a court order for this information too. However, I've heard stories of cooperative telco security investigations passing the information along to an agent.

Naturally that would be a "harmless error while acting in good faith." (legal humor)

I'd love to tell you more about FBI wiretaps but this is as far as I can go without pissing them off. Everything I've told you thus far is public knowledge. So I think I'll stop here. If you really want to know more, catch Kevin Poulsen (Dark Dante) at a cocktail party, buy him a Coke, and he'll give you an earful. (hacker humor)

In closing this subpart I will say that most electronic surveillance is backed up with at least part-time physical surveillance. The Feds are often good at following people around. They like late model mid-sized American cars, very stock, with no decals or bumper stickers. If you really want to know if you're under surveillance, buy an OptoElectronics Scout or Xplorer frequency counter. Hide it on your person, stick an earplug in your ear (for the Xplorer) and take it everywhere you go. If you hear people talking about you, or you continue to hear intermittent static (encrypted speech), you probably have a problem.

M. Your Pre-sentence Investigation Report, PSI or PSR

After you plead guilty you will be dragged from the quiet and comfort of your prison cell to meet with a probation officer. This has absolutely nothing to do with getting probation. Quite the contrary. The P.O. is empowered by the court to prepare a complete and, in theory, unbiased profile of the defendant. Everything from education, criminal history, psychological behavior, offense characteristics plus more will be included in this voluminous and painfully detailed report about your life. Every little dirty scrap of information that makes you look like a sociopathic, demon worshiping, loathsome criminal will be included in this report. They'll put a few negative things in there as well.

My advice is simple. Be careful what you tell them. Have your attorney present and think about how what you say can be used against you. Here's an example:

P.O.: Tell me about your education and what you like to do in your spare time.

Mr. Steal: I am preparing to enroll in my final year of college. In my spare time I work for charity helping orphan children.

The PSR then reads "Mr. Steal has never completed his education and hangs around with little children in his spare time." Get the picture?

J. Proceeding Pro Se

Pro Se or Pro Per is when a defendant represents himself. A famous lawyer once said, "a man that represents himself has a fool for a client." Truer words were never spoken. However, I can't stress how important it is to fully understand the criminal justice system. Even if you have a great attorney it's good to be able to keep an eye on him or even help out. An educated client's help can be of enormous benefit to an attorney. They may think you're a pain in the ass but it's your life. Take a hold of it. Regardless, representing yourself is generally a mistake.

However, after your appeal, when your court appointed attorney runs out on you, or you have run out of funds, you will be forced to handle matters yourself. At this point there are legal avenues, although quite bleak, for post-conviction relief.

But I digress. The best place to start in understanding the legal system lies in three inexpensive books. First the *Federal Sentencing Guidelines* ($14.00) and *Federal Criminal Codes and Rules* ($20.00) are available from West Publishing at 800-328-9352. I consider possession of these books to be mandatory for any pretrial inmate. Second would be the *Georgetown Law Journal*, available from Georgetown University Bookstore in Washington, DC. The book sells for around $40.00 but if you write them a letter and tell them you're a Pro Se litigant they will send it for free. And last but not least the definitive Pro Se authority, *The Prisoner's Self-Help Litigation Manual* $29.95 ISBN 0-379-20831-8. Or try http://www.oceanalaw.com/books/n148.htm

O. Evidentiary Hearing

If you disagree with some of the information presented in the pre-sentence report (PSR) you may be entitled to a special hearing. This can be instrumental in lowering your sentence or correcting your PSR. One important thing to know is that your PSR will follow you the whole time you are incarcerated. The Bureau of Prisons uses the PSR to decide how to handle you. This can affect your security level, your halfway house, your eligibility for the drug program (which gives you a year off your sentence), and your medical care. So make sure your PSR is accurate before you get sentenced!

P. Getting Your Property Back

In most cases it will be necessary to formally ask the court to have your property returned. They are not going to just call you up and say "Do you want this Sparc Station back or what?" No, they would just as soon keep it and not asking for it is as good as telling them they can have it.

You will need to file a 41(e) "Motion for Return of Property." The courts' authority to keep your stuff is not always clear and will have to be taken on a case-by-case basis. They may not care and the judge will simply order that it be returned.

If you don't know how to write a motion, just send a formal letter to the judge asking for it back. Tell him you need it for your job. This should suffice, but there may be a filing fee.

Q. Outstanding Warrants

If you have an outstanding warrant or charges pending in another jurisdiction you would be wise to deal with them as soon as possible *after* you are sentenced. If you follow the correct procedure chances are good the warrants will be dropped (quashed). In the worst case scenario, you will be transported to the appropriate jurisdiction, plead guilty, and have your "time run concurrent." Typically in non-violent crimes you can serve several sentences all at the same time. Many Federal inmates have their state time run with their Federal time. In a nutshell: concurrent is good, consecutive bad.

This procedure is referred to as the Interstate Agreement on Detainers Act (IADA). You may also file a "demand for speedy trial" with the appropriate court. This starts the meter running. If they don't extradite you within a certain period of time, the charges will have to be dropped. The *Prisoner's Self-Help Litigation Manual* that I mentioned earlier covers this topic quite well.

R. Encryption

There are probably a few of you out there saying, "I triple DES encrypt my hard drive and 128 character RSA public key it for safety." Well, that's just great, but... the Feds can have a grand jury subpoena your passwords and if you don't give them up you may be charged with obstruction of justice. Of course who's to say otherwise if you forgot your password in all the excitement of getting arrested. I think I heard this once or twice before in a Senate Sub-committee hearing. "Senator, I have no recollection of the aforementioned events at this time." But seriously, strong encryption is great. However, it would be foolish to rely on it. If the Feds have your computer and access to your encryption software itself, it is likely that they could break it given the motivation. If you understand the true art of code breaking you should understand this. People often overlook the fact that your password, the one you use to access your encryption program, is typically less than 8 characters long. By attacking the access to your encryption program with a keyboard emulation sequencer your triple DES/128 bit RSA crypto is worthless. Just remember, encryption may not protect you.

S. Legal Summary

Before I move on to the "Life in Prison" subpart, let me tell you what this all means. You're going to get busted, lose everything you own, not get out on bail, snitch on your enemies, get even more time than you expected, and have to put up with a bunch of idiots in prison. Sound fun? Keep hacking. And, if possible, work on those sensitive .gov sites. That way they can hang an espionage rap on you. That will carry about 12 to 18 years for a first time offender.

I know this may all sound a bit bleak, but the stakes for hackers have gone up and you need to know what they are. Let's take a look at some recent sentences:

Agent Steal (me): 41 months
Kevin Poulsen: 51 months
Minor Threat: 70 months
Kevin Mitnick (estimated): 7-9 years

As you can see, the Feds are giving out some time now. If you are young, a first-time offender, unsophisticated (like MOD), and were just looking around in some little company's database, you might get probation. But chances are that if that is all you were doing, you would have been passed over for prosecution. As a rule, the Feds won't take the case unless $10,000 in damages are involved. The problem is who is to say what the loss is? The company can say whatever figure it likes and it would be tough to prove otherwise. They may decide to, for insurance purposes, blame some huge downtime expense on you. I can hear it now, "When we detected the intruder, we promptly took our system off-line. It took us two weeks to bring it up again for a loss in wasted manpower of $2 million." In some cases you might be better off just using the company's payroll system to cut you a couple of $10,000 checks. That way the government has a firm loss figure. This would result in a much shorter sentence. I'm not advocating blatant criminal actions. I just think the sentencing guidelines definitely need some work.

Part II - Federal Prison

A. State v. Federal

In most cases I would say that doing time in a Federal Prison is better than doing time in the state institutions. Some state prisons are such violent and pathetic places that it's worth doing a little more time in the Federal system. This is going to be changing however. The public seems to think that prisons are too comfortable and as a result Congress has passed a few bills to toughen things up.

Federal prisons are generally going to be somewhat less crowded, cleaner, and more laid back. The prison I was at looked a lot like a college campus with plenty of grass and trees, rolling hills, and stucco buildings. I spent most of my time in the library hanging out with Minor Threat. We would argue over who was more elite. "My sentence was longer," he would argue. "I was in more books and newspapers," I would rebut. (humor)

Exceptions to the "Fed is better" rule would be states that permit televisions and word processors in your cell. As I sit here just prior to release scribbling this article with pen and paper I yearn for even a Smith Corona with one line display. The states have varying privileges. You could wind up someplace where everything gets stolen from you. There are also states that are abolishing parole, thus taking away the ability to get out early with good behavior. That is what the Feds did.

B. Security Levels

The Bureau of Prisons (BOP) has six security levels. Prisons are assigned a security level and only prisoners with the appropriate ratings are housed there. Often the BOP will have two or three facilities at one location. Still, they are essentially separate prisons, divided by fences.

The lowest level facility is called a minimum, a camp, or FPC. Generally speaking, you will find first time, non-violent offenders with less than 10-year sentences there. Camps have no fences. Your work assignment at a camp is usually off the prison grounds at a nearby military base. Other times camps operate as support for other nearby prisons.

The next level up is a low Federal Correctional Institution (FCI). These are where you find a lot of people who should be in a camp but for some technical reason didn't qualify. There is a double fence with razor wire surrounding it. Again you will find mostly non-violent types here. You would really have to piss someone off before they would take a swing at you.

Moving up again we get to medium and high FCI's which are often combined. More razor wire, more guards, restricted movement, and a rougher crowd. It's also common to find people with 20 or 30 plus year sentences. Fighting is much more common. Keep to yourself, however, and people generally leave you alone. Killings are not too terribly common. With a prison population of 1500 to 2000, about one or two a year leave on a stretcher and don't come back.

The United States Penitentiary (U.S.P.) is where you find the murderers, rapists, spies, and the roughest gang bangers. "Leavenworth" and "Atlanta" are the most infamous of these joints. Traditionally surrounded by a 40-foot brick wall, they take on an ominous appearance. The murder rate per prison averages about 30 per year with well over 250 stabbings.

The highest security level in the system is Max, sometimes referred to as "Supermax." Max custody inmates are locked down all the time. Your mail is shown to you over a TV screen in your cell. The shower is on wheels and it comes to your door. You rarely see other humans and if you do leave your cell you will be handcuffed and have at least a three guard escort. Mr. Gotti, the Mafia boss, remains in Supermax. So does Aldridge Ames, the spy.

C. Getting Designated

Once you are sentenced, the BOP has to figure out what they want to do with you. There is a manual called the "Custody and Classification Manual" that they are supposed to follow. It is publicly available through the Freedom of Information Act and it is also in most prison law libraries. Unfortunately, it can be interpreted a number of different ways. As a result, most prison officials responsible for classifying you do pretty much as they please.

continued on page 40

Hacking FedEx

by PhranSyS Drak3

Along with the advent of the computer, man's other crowning achievement is the ability to move parcels from Point A to Point B in a rapid fashion. In other words, Overnight Delivery. Overnight Delivery is a fiercely competitive and ever-changing market, but no other company has utilized as much technology in their rise to the top as Federal Express. In this article, I will attempt to give an overview of FedEx's monolith mainframe, a look at FedEx security methods and even a few tips should anyone decide to try and hack FedEx.

The System

FedEx runs its mainframe off of a Cray supercomputer. This is needed to deal with the overwhelming logistics of mass shipping. Though employee records, customer account information, and other internal functions are on the mainframe, the heart of FedEx's computer system is called COSMOS, which stands for Customer Oriented Services and Management Operating System. COSMOS (consisting of well over 240 screens) is used for dispatching, tracking and tracing shipments, and communicating between FedEx locations. Vital information such as service delays and customer info is also kept in COSMOS. One will be surprised and a bit elated to find the home addresses and phone numbers of celebs like Shawn Kemp of the Seattle SuperSonics and Tom Brokaw of NBC Nightly News fame spread on CRT for all to see. Needless to say, COSMOS is probably the most vital subsystem in FedEx's massive network.

Over two million packages go through Federal Express' air/ground network (referred to by most FedEx employees as simply "the system") each day. Of these two million packages, 60 percent go through the system with no problem. However, the rest may have attention called to them by customers who:

A. Want to change the status of a package such as delivery info, billing changes, or service changes.

B. Want to obtain info on who signed for their package, where, and at what time.

C. Just want to know where their package is as it moves through the system.

Let's assume our case is C. Let's say Wintel Corp. has just shipped you two gigs of ram as a thank you for not bashing them. You'd like to know where it is. You pick up your phone and dial 1-800-GO-FEDEX. Instantly, your call is diverted to one of the many Call Centers in the nation where thousands of FedEx employees are set up to deal with customer calls. Usually for tracking packages, an automated system will read off the data entered in COSMOS. However, if one navigates the automated voice prompts elsewhere or the package status is unclear, the caller will be transferred to a live person. The person who answers (called a Call Center Agent) will then ask for your tracking number. He or she will then proceed to access COSMOS for the information. By the way, since this is an IBM AS400 mainframe interface, all of COSMOS' screens are function key driven. In this case, the screen the Call Center Agent will access is selected with Pf8, thus called the "8" screen by FedEx personnel. This screen tracks every move the package makes. From the time it is scanned to the time it is delivered to its destination, the package is frequently scanned and its status updated. S/he will then read this info and communicate with the appropriate FedEx facility that currently (or last) has the package (using info in COSMOS which shows info on every facility including internal phone numbers and directions to specific locations) and may even transfer you to them. The info in the "8" screen is probably the most dynamic of all of COSMOS' subscreens and is updated thousands of time a minute. All of COSMOS' data is available via remote access to managers, directors, select sales reps, and other need-to-know employees. It is also available to (clever) inquiring minds. I don't think I need to tell the readers the applications possible if one possesses access to data of this sort. Whether or not the applications you choose fall on the side of legality or not is entirely up to you. I'm just providing the readers with a look into one of the largest private systems and a "heads-up" should anyone be interested in a good and challenging hack.

Security in the FedEx Network

Of course other data resides on FedEx's network other than package info. There is the company's intranet, internal bulletin boards with loads of info on everything from Corporate Security memos to employee profiles. One day I even learned a certain station manager's profile including her full name, the names of her two children, what kind of car she drove, and the fact that she enjoyed listening to gospel music in her spare time. My point? Once inside, there is virtually no sense of security other than barring those without appropriate duty codes from accessing certain screens. Even a few of IBM's default passwords for the AS400 Mainframe system work. While internally lax, getting in from the outside is considerably much more strict. Those familiar with any Unix system or mainframe OS know a good admin requires the user to change passwords regularly, will check logs for unauthorized login attempts, and will revoke userids on a "3-and-out" basis for bad passwords. FedEx does all these wonderful things to discourage unauthorized access. But again, those don't make the system hard. What does is a little system I have nicknamed "The Beast" that is one of the most clever devices I have come across in years.

While chatting with a friend of mine who is a sales rep, the subject of security came up. He then pulled out The Beast. It looked like one of the dime-a-dozen credit card sized calculators you'd find in the checkout aisle of your favorite grocery store. It has eleven keys (numbers 0-9 and an enter key) and what appears to be a 10-digit LCD display. How is it used? Well, this sales rep has a username and password to log on with. Nothing unusual there. He also has a four digit PIN. Uncommon, but not all that unusual. What makes this unusual is that after he enters his PIN, the login system spits out a six digit number for him to enter into The Beast. The Beast then spits out yet another number for him to enter into the terminal to complete his login. Oh, I almost forgot. For all you MIT and GaTech-ites who can run complex algorithms in your head in your sleep, there's one final catch: you have ten seconds from when you get the number from The Beast to enter it in the terminal or else you are logged out and the process begins again. With, might I add, a whole new set of confirmation numbers.

Another unintentional, but highly effective, form of security is the tendency of mega corporations to immerse themselves in insider jargon and acronyms. I would even go so far as to say that our good government has only a few more TLA's than FedEx. As is the case with the government, if you try to social engineer yourself info or a password using that drivel in *Secrets of a SuperHacker,* you will be sharing your deepest thoughts with a dialtone. FedEx corporate lingo is very deep and complicated. Outsiders are easily spotted. Especially those of you who call FedEx couriers "drivers."

So You Wanna Try Anyway....

I see a few of you have decided to be persistent despite what I've told you. Even though it is an improbable process, it is not impossible. First off, it is imperative to gather information on your enemy. Two of the hacker's oldest and most basic tools are trashing and social engineering. First of all, trashing. No FedEx station I know has a corporate policy on shredding. I know of many stations and ramps that have shredders in their offices but do not use them. What can be found? A veritable gold mine of information. There are printouts of screens (usually the "8" screen used for package tracking and the "9" screen used for detailed info on traced packages). These are important for understanding how these vital screens look and giving you an idea of how packages are scanned as they move through the system. Internal phone numbers can also be found trashing. Why is this of value? Call the 800 number and get the location of your nearest FedEx station (not Kinko's or Mailboxes Etc... I mean an actual FedEx facility). Now with this info, try and get their phone number. Without extraordinary means such as war dialing or tip-boxing, the number is virtually impossible to obtain. FedEx employees guard station numbers fiercely. Not so much for security reasons, but to keep hundreds of customers from calling stations instead of the Call Centers. Lastly (and most importantly), trashing can bring goodies like manuals and job aids. Didn't I say FedEx operates as backwards as the government? Let's assume there is a manual for Service Agents (who, by the way, know nearly as much, if not more, than managers) in a station. A few pages worth of info happens to change in it as FedEx updates a few processes to change with the times. Instead of the company issuing a memo or an addendum, they will rewrite the whole damn thing, reissue them, and order for the older manuals to be destroyed (i.e., thrown away). If you come across one of these in your trashings, you might as well work for FedEx. I've even lucked up on some old corporate phone directories with over 90 percent of the numbers current. Along with the obvious, these also provide an outline of the corporate structure. This way when you get to the social engineering phase, you'll know that instead of "Bob from Computer Security" that you are "Robert Smith from Data Protection down here in Memphis."

Now that you have some info from trashing, let's use our second basic tool: social engineering. We've gotten a phone number to the station and a few names. It's not too hard to dial up and say you're from a Call Center or Data Protection and con even more info out of the hapless soul on the other end. Again, here's where a little of that inside info we found trashing pays off. What do you ask for? A good place to start is asking a Service Agent about the manager. He or she is the one most likely to have remote access. Say you're an employee from another station looking to transfer to that location. Chit-chat for a while about how you hate where you're at and how the weather/people/whatever are so much nicer there. Don't overuse this as you risk being asked something you can't answer. Now ask for that manager's employee number so you can email him. Congratulations! You now have his COSMOS login. Just remember: know who you "are" and what you are talking about before attempting to SE.

All this is fine and dandy, but what about The Beast? Well, the bad news is the Beast does exist and has big, sharp teeth. The good news? Not everyone with remote access uses the Beast. I know for a fact that regular station managers do not use it. It appears that only employees with high level access to sensitive info that competitors like UPS and Airborne would want are issued a Beast. I'd also venture a guess that this is information like discounted rates for major accounts. Not grunt level data like COSMOS. The other bit of good news is that the Beast is manufactured by an outside company - not FedEx. I'm sure that they want to attract more customers and a phone call or an email from an "interested potential customer" would land you plenty of info on their product.

This device is made by a company called EnigmaLogic. Their address is 2151 Salvio St., Suite 301, Concorde, CA, phone number (510) 827-5702.

I hope this helps a bit. I guess your final question is "How does PhranSyS Drak3 know all this?" Well, it should be obvious to a retarded ape that I am or once was probably an insider. Why, then am I divulging company secrets? There will come a day, my friends, in the not too distant future where mega corporations will control most of the world's vital information. Especially things they would like to keep private for unscrupulous reasons. They will exploit the common man for the almighty dollar as long as no one keeps tabs on them. It's up to us to safeguard and protect ourselves by keeping information free and accessible.

Happy Hunting!

Defeating *67 With Omnipoint

by TtJ

Ever since Caller ID came into existence, the question of how *67 blocks the calling number from appearing on the Caller ID box has been asked by many people. A lot of us were not sure if the Caller ID data delivered by a *67 call contained only the "PRIVATE" message or if the calling number was in fact sent along and simply not displayed. The answer, as some of you might already know, is definitely *the latter!* Assuming that Caller ID is available in your area and someone calls you using *67 in order to remain anonymous, his or her number will still reach your phone switch and, with the right access, you can find out what that number is. This article is not written from a technical perspective, therefore it will not talk about how to manipulate the actual Caller ID data. Instead I will describe how Omnipoint voice mail can make *67 completely useless.

Omnipoint is a company that provides GSM phone service in the Northeastern region of the United States. Besides making and receiving calls, Omnipoint offers a variety of very useful features. One of these features is voice mail. When using message playback on the voice mail, the caller's originating number is announced prior to the message. A rather interesting thing is that this voice mail system will obtain the caller's number even if the caller uses Caller ID Block, namely *67, 1167, or All Call Blocking.

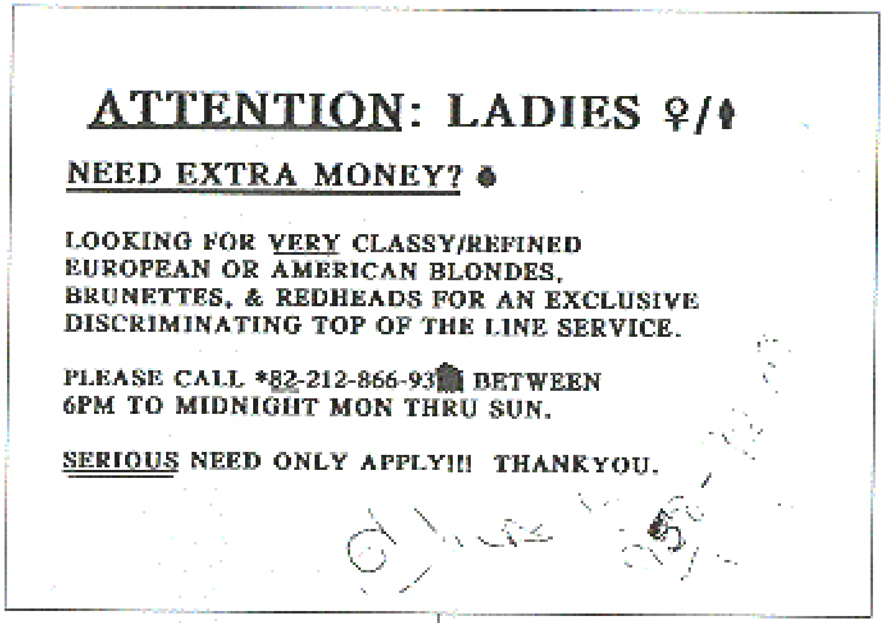
This has led some people to believe that Omnipoint voice mail uses ANI technology. However, this is not true at all. The system obtains the originating number using Caller ID information and it bypasses Caller ID block either because of a "bug" in the system or because of the way the system reads the Caller ID data.

To verify that the technology used here is indeed Caller ID and not ANI, a very simple test is conducted:

1. Use two telephone lines: Line A and Line B.
2. Call Forward Line A to the Omnipoint voice mail.
3. Call Line A using Line B. You'll be connected to the Omnipoint voice mail since Line A is forwarded to it. Leave a message on the voice mail.
4. Call the voice mail and retrieve the message.

If the system read back Line A's number, we would know that ANI was the technology used. However, in this case, Omnipoint voice mail will read you back Line B. This indicates that the system gets the telephone number from Caller ID data because when using Call Forwarding, the switch will always deliver the Caller ID info of the party that initiated the call (of course this is assuming that all the switches involved have Caller ID capability).

The reason why it is very important to point out that this voice mail detects numbers through Caller ID and not ANI is because it makes the system so much more powerful and a lot scarier. If the system used ANI, the only way that it could obtain the caller's number would be if the caller dialed the actual Omnipoint number. Thus, theoretically, the caller could first find out if the number he or she is about to call is in an Omnipoint exchange and then take appropriate precautions when calling this number (just like when calling 700, 800 and 900 numbers). However, since the Omnipoint switch reads Caller ID and ignores *67, any phone line can be forwarded to the voice mail making it impossible for the caller to know beforehand what he or she is getting into. I have no idea if the GSM systems in the rest of the country do the same thing. Considering that Caller ID now works on an interstate level, people from anywhere else in the country can still forward their phone to any Omnipoint number in the Northeast. They can then get the anonymous caller's number by simply accessing the voice mail. Just remember, if there is a number you want to call anonymously do not by any means rely on *67 to block your number.



ATTENTION: LADIES ♀/♦

NEED EXTRA MONEY? ♠

**LOOKING FOR VERY CLASSY/REFINED
EUROPEAN OR AMERICAN BLONDES,
BRUNETTES, & REDHEADS FOR AN EXCLUSIVE
DISCRIMINATING TOP OF THE LINE SERVICE.**

**PLEASE CALL *82-212-866-93[redacted] BETWEEN
6PM TO MIDNIGHT MON THRU SUN.**

SERIOUS NEED ONLY APPLY!!! THANKYOU.

We found this height of sleaze on a phone booth in New York City. Whoever this is wants to make sure he gets the phone numbers of these "classy/refined" women by including *82 as PART OF THE PHONE NUMBER! Of course, he forgot to add the 1 before the 212 so this is likely to confuse whoever tries it. Not to mention that an error will be generated by every call placed WITHIN 212. Well, at least the graphics are classier than the people behind this.

How To Be A Real Dick On IRC

by semiobeing

The purpose of this article is to provide what I consider optimal methodology for hacking IRC channels. In addition, I will provide some of the better channels to hack as well as fun things to do while "owning a channel."

Why Hack IRC?

I have often asked myself this question and the answers are varied and numerous. One of the primary reasons for hacking IRC channels is due to sheer boredom. However a multitude of secondary reasons exist. Foremost among these is something along the lines of "that asshole op insulted me and/or kicked me and/or banned me from the channel and *I want revenge!* This is a perfectly valid excuse and boredom is not a necessary condition for implementing a takeover of an IRC channel. Nor is it a necessary condition that the reason you were insulted and/or kicked and/or banned was because in fact you are an asshole. All that is necessary is the will, the desire, a bit of skill, and of course the tools, which conveniently brings me to my next section.

Requisite Tools

Any decent craftsman needs a good set of tools and IRC hackers are no exception. Without the proper tools you are dead in the water. All of the tools I describe below are available on public ftp sites. Before I launch into a discussion of what you will need, it is important to point out that if you are reading this document from your ppp/slip account you might consider getting a shell account if you are serious about hacking. Hacking IRC from a slip/ppp is much more complicated than doing so from a shell account. There are those who will debate this but my experience has shown that mIRC or any of the other shareware IRC programs for the PC are no match for the speed and ease of use that an IRC shell script allows for. Thus the first tool required for hacking is an excellent IRC shell script. If you have already used IRC via a shell account and are still reading this document you probably already have a script, which means you are well on your way! As far as IRC shell scripts go, my personal favorite is LICE - again available publicly via FTP. Other scripts exist but the richness and power of the LICE commands I believe is second to none. Now while it is possible to stop here and hack ops with just a script, you would effectively be putting yourself needlessly at a handicap. Therefore I recommend these additional two tools: 1) Multi-Collide-Bot (MCB) and 2) Link Looker (LL). These two C programs are your infantry and intelligence respectively. Again, both are available via FTP and both are C programs and therefore need to be compiled.

What It Takes To Gain Control

In order to effectively gain control of an IRC channel you must be the only op on your channel. If you are still clueless at this point, that is to say, you should be the only guy/gal with the @ in front of your nick. Once you have accomplished this, the channel is *yours*. Of course, that is until it is taken back or you decide to cease hacking the channel. There are a number of ways to effectively gain ops on a channel. I will start with the simplest, then move to the increasingly more complex and finesse laden methods.

Far and away the easiest method of gaining ops on a channel is to ask. You laugh, eh? Well don't. Clearly, as hackers grow more prevalent on IRC the asking method becomes more and more unlikely to succeed. This is especially true of the bigger and well established channels that have cultures onto themselves such as #netsex, #teensex, #windows95, #travel, #BDSM, #blaklife, #texas, #hack, and any of the #warez channels as well as a whole host of others. To gain ops in these channels you must become a channel regular (i.e., one who hangs out there frequently and becomes a known and trusted member of the channel). Since you have neither the time nor the desire to make friends on the channel you ultimately want to hack ops on, the asking method is the last thing you want to do on all but the smaller more ethereal channels, where you obviously stand a better although still slim chance of gaining ops through a request.

But of course you didn't come this far to be taught how to ask for ops, so let's proceed with the next lesson. Aside from asking, the most effective way of gaining ops is through splits.

What is a split? A split occurs when the IRC server you are communicating on detaches from the rest of the net. If you are in a channel and by chance the only one on a particular server that splits away, you will not only find yourself alone on the channel, but will now have the opportunity to gain ops. In order to do this you need to leave and rejoin the channel in which case you will now find yourself with the little @ in front of your nick. When your server rejoins you will have ops on the channel. Now you say, "Wow, that's easy enough." Wrong. More likely than not, especially on a bigger channel a number of things are likely to occur that will remove your op status. Remember now the goal here is to keep ops so you can "Have Your Way." Also, and more importantly, if you go into a channel and wait around hoping the server you are on splits, you might grow old and die first. Therefore, what is a wannabe IRC hacker to do? Link Looker is your answer.

Link Looker

Link Looker is a lovely little program that acts as your intelligence officer. Without getting into the complexities or its mechanics, what it effectively does is give you a message anytime a particular server detaches from the net and a message when it rejoins. Is the methodology becoming clearer now? Yes! That's right! When LL tells you that a server is split, you connect to that server and join the channel you seek to hack ops on and hope nobody else split from the channel on that server (if this occurs you will not get ops). If you find yourself alone, you will have ops and a fighting chance to gain control of the channel. It is important to realize that on many channels, just getting ops via a split and waiting for a rejoin is sufficient for gaining control of a channel. This is particularly true of small to medium sized channels as well as channels that are not organized or do not have bots (more on this later). You simply wait for the server to rejoin and once the channel is full you execute your mass deop command (this is in your script and the key element to getting rid of any other ops) and you will be the only op left. The channel is yours and you can go do your thing! On bigger more organized channels, things won't be so easy due to the presence of bots as well as the presence of scripts used by existing human ops.

Bots and Scripts

Bigger more organized channels inevitably have a bot (robot) or multiple bots. Bots are essentially souped up scripts that attempt to maintain ops on a channel by their continuous presence on that channel. Additionally, bots provide a number of channel maintenance tasks such as opping known members of the channel (either automatically or through password requests), providing notes, and other information. Bots however are primarily used for keeping ops on the channel and, depending on the type of bot, defending against IRC hackers. Bots come in many varieties and types but the best of them do a good job of deopping splitters (that's you, silly - you are opped on a split and when you rejoin the bot will deop you). Not only will bots deop you - many of the human ops have scripts (such as LICE) that, depending on the settings employed, will deop you as well. Now, with the prevalence of powerful scripts on IRC a recent phenomena is the occurrence of the desynch. This is a nasty event that takes place when you rejoin from a split and your script deops the existing ops and the existing ops deop you at the same time. What this does is confuse the shit out of the servers and cause them to desynchronize from one another. This is to be avoided at all costs. When this happens you will effectively become desynched from a large portion of the net and most of the channel (depending on what server you rode in on). What's worse is that you will think you have ops (which you will for that server) but in reality you won't and you will be wasting your time. So how with the prevalence of super bots and human ops with scripts do you take the channel? Using MCB of course!

Multi-Collide-Bot (MCB)

Multi-Collide-Bot (MCB) is a powerful

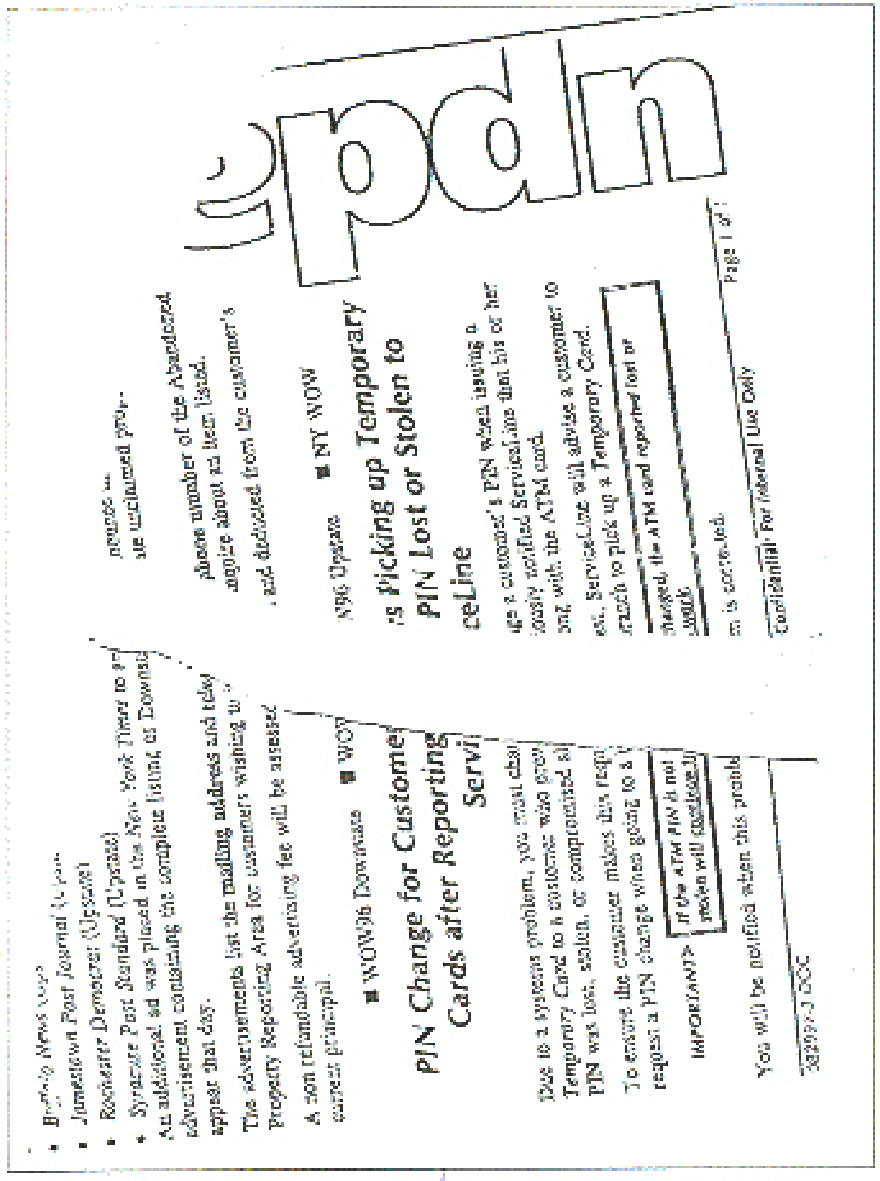
tool and your best friend. MCB is an even lovelier program that creates a clone of a nick you want to kill (almost always an op on the channel you are trying to hack) on a server that has split (yes, the one Link Looker informed you of). Basically you feed MCB the name or names of the nick you want to kill and tell it what split server to establish those clones and upon rejoin, *bam/smack/kill!!* Yes, that's right, the target is thrown out of the channel (losing ops) and must re-establish a connection with a server to get back onto IRC and into the channel. So yes, you have figured it out. If you kill all of the ops on a channel and you ride in on a split you will be the only op in the channel. Let me assure you there is nothing like seeing the nick kill messages of the ops you have targeted as you ride in on the split.

Pre-Takeover Preparation

There are a number of things you can do before you attempt to take over an IRC channel to make things easier and be as well prepared as you can possibly be. Plain and simple you must know who you are attacking. One of the most important things you can do as you sit and observe the channel is to determine which bots and/or human ops are deopping on rejoins. These are the nicks you want to target first. You will fail if you don't kill these nicks and rejoin because you are likely to cause a desynch (discussed above). However, it is essential to make sure you kill all of these ops. Leaving just one op alive means you have lost that battle and must now regroup and wait for another split. It is important to watch out for ops changing their nicks if they detect a split. If they do this, the MCB you tagged with their nick will be useless to you. The way I prevent this is to be on both sides of the split. That is to be opped in the channel on the split server and have a clone in the channel on the other side of the split monitoring the goings on, telling you if ops change nicks or new people are opped (in which case you create a new MCB with their name on it).

Things To Do Once You "Own" the Channel

Once you own the channel, the decision is clearly yours on how you want to proceed and needless to say the number of things you can do is endless. However, let me share with you a number of time tested ideas that are sure to give you a thrill not to mention totally piss off the channel you have now hacked. The first thing you can do is to taunt the former ops of the channel. That is to say, they will probably be cursing you and telling you what a loser you are for hacking the channel. They will say things like "get a life, do something more productive." Remember, don't take it personally. You have to keep in mind that it is the former ops who in fact are the ones who need to get a life, considering the only power they have (or make that *had*) was to have ops in the first place. So you can continue to taunt and if they get really belligerent you can kick them off the channel. They will undoubtedly come back within a second or two and then you can say something like, "Now, now - I am in control of the channel and I will not tolerate such language and behavior. If you are unable to control yourself I will be forced to ban you." Now this is sure to get some violent response from the former op in which case you subsequently kick and ban them and move on to the next person. Another thing I like to do is to word ban. This is particularly easy if you have LICE. What you do is pick a word that if typed onto the screen by any of the channel members, will automatically result in you kicking them off the channel with the reason that that word is banned. This method is particularly good in channels like #teensex where people are always saying the word sex, male, female, teen, age, etc. All you do is ban these words and watch the kicks begin to fly. Another thing I like to do is moderate the channel. What this does with the /mode +m command is to make it such that nobody on the channel can speak. This is a particularly good thing to do when many of the channel members are getting out of hand and you want to make some sort of statement without anybody interrupting you. Yes, all eyes will be trained on you. If you want to be really mean, when you are finished hacking the channel, you can leave it moderated in which case nobody will be able to speak and the channel is effectively shut down. Another thing to do which is nasty as well is to kick everybody out of the channel and make it invite only, effectively shutting it down as well. Think of your own creative things to do.



- Buffalo News (Ups
- Jamestown Post Journal (Upst
- Rochester Democrat (Upstate)
- Syracuse Post Standard (Upstate)

An additional ad was placed in the New York Times to an advertisement containing the complete listing of Downst appear that day. nounce ate unclaimed prop

The advertisements list the mailing address and tele phone number of the Abandoned Property Reporting Area for customers wishing to inquire about an item listed.

A non refundable advertising fee will be assessed and deducted from the customer's current principal.

■ WOW96 Downstate ■ WOW96 Upstate ■ NY WOW

PIN Change for Customers Picking up Temporary Cards after Reporting PIN Lost or Stolen to ServiceLine

Due to a systems problem, you must change a customer's PIN when issuing a *Temporary Card* to a customer who previously notified ServiceLine that his or her PIN was lost, stolen, or compromised along with the ATM card.

To ensure the customer makes this request, ServiceLine will advise a customer to request a PIN change when going to a branch to pick up a *Temporary Card*.

IMPORTANT> *If the ATM PIN is not changed, the ATM card reported lost or stolen will continue to work.*

You will be notified when this problem is corrected.

582997-J.DOC

Confidential: For Internal Use Only

Page 1 of 1

HOW TO DESTROY SENSITIVE INFORMATION. Always tear confidential memos into two or three pieces before placing them in the trash. This ensures that nobody will be able to read them. We only wish we knew what company this was so we could congratulate them publicly.

Brute Forcing The World

by ChezeHead

One university I know of uses an old Burroughs mainframe for their registration computer and allows, with a username and a four number pin code, access to a person's grades, the ability to add and drop classes, financial aid information, and a student directory. They also implemented a campus-wide pop mail server with the default passwords, changeable only through a program like Eudora, of a static four letter combination and the pin code, allowing a brute force attack that takes ten minutes maximum against the majority of accounts, and then complete access to the student directory to find more usernames!

Welcome to the ancient art of brute force hacking, the way into systems with no gaping wide backdoors such as PHF or sendmail's finer remote hacks. A world in which infamous internet attacks such as the Great Worm were able to enter thousands of systems. The concept of brute force hacking hasn't changed much although in recent years different forms of attack have sprung up; at one time telnet and ftp attacks were common and they are still around, but it gets really annoying when after three tries you are disconnected, and system logs can show huge attacks against usernames.

Enter the latest greatest system for delivering email, the Post Office Protocol aka popmail. There are many systems out there yet that don't log pop attempts, and many popmail servers don't kick you off, so you can start a script and let it go, being almost assured of eventually gaining entrance to a system. ISP systems, as they are usually extremely lax in required passwords in an attempt to keep their customers happy, can be very easy marks.

Popmail is a very simple protocol to play with. Just like ftp you login with user <username> and pass <password> and, unless an encryption scheme such as apop is used, the passwords are just sent in the clear. Popmail servers reside normally on port 110 for the pop3 protocol, the current standard.

I won't include a script for this as that would be too easy, but it shouldn't take more than 15 minutes to write and debug a working brute force script for popmail, and the results can be incredible.

WRITE FOR 2600!

Apart from helping to get the hacker perspective out to the populace and educating your fellow hackers, you stand to benefit in the following ways:

A year of 2600 for every article we print (this can be used toward back issues as well)
A 2600 t-shirt for every article we print
A voice mail account for regular writers (two or more articles)
An account on 2600.com for regular writers (2600.com uses encryption for both login sessions and files so that your privacy is greatly increased)

PLEASE NOTE THAT LETTERS TO THE EDITOR ARE NOT ARTICLES

Send your articles to:

2600 Editorial Dept.
PO Box 99
Middle Island, NY 11953-0099

Hack The Vote

by A Non-Candidate

The Voting Rights Act of 1965 and the more recent "Motor Voter" laws (officially known as the National Voter Registration Act -circa 1995) allow the wily hacker - or the zealous political extremist - the opportunity to over-influence the political process in the United States with a very positive risk-reward ratio: vote early, vote often, vote with very little chance of getting caught.

"Motor Voter" is less useful, so we will discuss it first. All it does is present voter registration material at almost every contact an individual has with government, either federal, state or local. It is named from the practice of actually attaching a voter registration form to various motor vehicle department forms, notably driver's license applications and the like. Its only effect is to enlarge the electorate, allegedly favoring Democrats. However, it is interesting to note that the previous act enlarging the electorate (the lowering of the voting age from 21 to 18), though predicted to favor Democrats, has actually favored Republicans in most elections since this has been in effect (1972).

The Voting Rights Act is the tool, the camouflaged loaded gun waiting to be seized by hackers - or by Hitlers.

The act states that if a geopolitical area (a state, such as Mississippi, a county, or a city such as New York City) has a minority election turnout which is less than that minority's percentage of the general population, then that area is subject to the Voting Rights Act, which liberalizes the election laws.

In other words, if NYC has a population which is 35% black and 30% Latino/Hispanic, then at least 35% of voters at the polls must be black, and 30% must be Hispanic/Latino. Otherwise the NVRA kicks in.

This raises many interesting questions. What if you're a very dark skinned Hispanic? What if you're a dark skinned Latino libertarian and refuse to declare your ethnic background? What if David Dinkins (a black man) runs against Fernando Ferrar (a Hispanic man) for mayor of New York, and almost no whites vote - are the white people's rights violated, and should the NVRA then apply?

Enough of that. No one philosophizes over rlogin, they just use it. How can we use the Voting Rights Act of 1965?

The main applications of the NVRA are the permitting of voter registration by mail and the elimination of identification requirements.

Mail applications can be found at most public (governmental) buildings: Department of Motor Vehicles and Post Offices. Notarization or witnessing of these forms is not required; the prospective voter simply fills out the form, signs a name, and mails it. At this point, there are a few dangers to a "hacker" - first, the registration *must* be mailed from within the state (a rule set up to combat fraud); second, in most states, a voter ID card - usually with nothing more than the name, congressional district, and election district for the given address - is sent to the address provided on the registration form in a "DO NOT FORWARD" envelope. If this envelope is returned, most Election Boards will remove the name so recently added to the voter rolls.

A criminal can get around this second danger in either of two ways: he can register at the last possible moment (this differs state by state, but is usually 30, 60, or 90 days before the election he wishes to vote in. Of course, a few days must be added for mail delivery. This works well *only* in states with the 30 day deadline, such as New York!) or he can use a name similar to one found in a phone book. John Jacob Astor might not think much about getting a voter registration card in the name of Jon Jacob Aster or John Jacoby Astor.

The "voter" must decide if he will visit the various polling places himself and vote manually or if he should risk using absentee ballots. If using absentee ballots, in most states the decision must be made when registering to vote. (The New York State form has a space for this purpose.) In some states, these ballots may be sent to a third-party address, i.e., an address other than the voter's.

In most states, the absentee ballot must be sent out by the voter - and postmarked - roughly two weeks before Election Day!

While dozens or hundreds of absentee ballots sent to Hacker Travel, Incorporated may seem suspicious to some election boards, this is fairly easy to cover up with a database of personal information (name, address, date of birth, party registration) for the phantom voters, as well as latex gloves, mass market pens (such as Bic or Pilot), no-lick postage stamps, and a sponge to seal the ballot envelopes.

Though our multi-threaded voter may be an energetic marathoner, some danger lurks at the polls. He may run into the same person (a police officer, election official, or reporter) at multiple polling places. Even though the Voting Rights Act prohibits requiring possession of your voter registration card, and the "Motor Voter" law and various immigration laws from 1995 prevent election officials from examining other ID and even asking if you are a US citizen, indications of apparent fraud should probably be avoided.

In addition, no matter how speedy our constituent, lines of people waiting to vote do occur and will slow him down. Examination of his database in public will be difficult and suspicious; practicing alternate signatures (even in his own handwriting) impossible.

In short, to vote often, vote by mail.

The E-ZPass System

by Big Brother

I am responding to the comments in the Summer 1997 issue (on page 55) about the New York State Thruway's E-ZPass system and its ability to identify a particular vehicle for violation enforcement by using "secret detectors."

These "secret detectors" are probably nothing more that conventional radar units, wired to a central location for recording data. If the "secret detector units" are state-of-the-art, they are video cameras feeding a video unit with software that allows individual vehicle speed determination and recording. The use of E-ZPass to cite speed violators is cumbersome and can only "average" the vehicle's speed over a known distance, as I will explain below. Radar units, RF or laser, or video systems are much easier to use for the actual speed determination.

What is a "toll pass?" There are many types of "toll passes" in use. E-ZPass is only one. To alleviate the paranoia concerning toll passes, let's understand how the system works and with this understanding will come realization and, perhaps, "relief" that the "authorities" sometimes really do try and make things easier for the motoring public without always hiding some "Big Brother" device among the "goodies."

Transponders (aka "toll passes" or "tags") are used to identify the location of a particular vehicle. By passing a particular location, a motorist's location, time, and date will be recorded. Not the speed. It takes two stationary installations to determine a vehicle's speed. The vehicle's "average" speed is then calculated between these two known locations. There are many ways to easily determine a vehicle's speed without trying to adopt the E-ZPass type system to this use but, if they have enough stationary locations, it can certainly be done. This is not rocket science. Let me explain (without, hopefully, writing a booklet). The technical types might find this interesting.

Toll pass systems use microwave frequencies, usually in the 900-928 MHz. or 2.8 GHz, or (soon) 5.8 GHz bands to communicate between the stationary transmitter/receiver and the vehicle transponder. Can you jam these frequencies? Sure. If you do, and the system uses gated access, you will not be granted access. So what good have you done?

Could you cause a signal to be transponded that would indicate a lower charge than you should be paying? Some systems only query the transponder for its unique identifier number. The central computer keeps the rest of the data for the billing occurrence. This would seem to me to be impossible to "hack" at the transponder end. Other systems record the entry time, location, etc. into the transponder. Then, when the transponder is queried upon exiting, both the "entry" and "exit" data are sent to the stationary receiver. There is potential here for hacking. It is also federally illegal (two years and $ 10,000 per occurrence) and not recommended. (Hey guys, there ain't no free ride. Somebody has to pay for the road. Let the users pay or all of you nonusers will wind up paying for the roadway via higher income taxes, fuel taxes, and so forth.)

900-928 MHz is the most common frequency spectrum presently in use. Want to hear what the transmissions from the vehicle transponder sound like when "they" are using a 900 MHz system? Place a cellular telephone near the transponder and depress the "SND" key. The transponder will usually react to the nearby cellular frequency and think it is being queried, hence causing a transpond. You will hear the transpond as a burst of data in your cellular telephone's handset earpiece. Record this for analysis. It is not encrypted and usually consists of a simple multiple digit code. Depending upon the system being used, this transpond will always contain the transponder's unique identifier code, and it may also include the date, time, location of last time it was queried, and other administrative information.

One commonly used toll pass system uses "backscatter modulation" to activate their vehicle transponders. From a stationary transmitter, with the antenna mounted over the roadway, microwaves are caused to impinge upon the vehicle mounted transponder, causing the transponder to power up, use some of the absorbed microwave energy, and reflect ("backscatter transpond") back to a nearby stationary receiving antenna, on another nearby frequency, with the transponder's identifying code number (usually about eight digits). A central computer records the identification number, location, time and date, and performs the desired action. This is all that is required for "entry verification" to a parking lot, etc. More normally, this initial information will be the entry point to a controlled access Tollway.

Intelligent Vehicle Highway Systems ("IVHS") use a second occurrence of the proceeding action, occurring at a second location, usually where the vehicle exits the Tollway. The central computer will then access the "billed to" account and record this data for end-of-month processing into an invoice.

As you may have deduced, backscatter modulation is imperfect as a speed determining medium. Within a distance of many meters there is no relatively accurate method to determine just when the transponding action will occur. As an aside, if the vehicle has one of the "metallic" impregnated windshields used to reduce ultraviolet ray transmission into the vehicle, the normally "inside the windshield" mounted transponder will have to be mounted on the outside - usually in the area of the front bumper - so it is unshielded. But I digress. Different stationary microwave transmitter/receiver combinations can cause the distance-to-vehicle measurement to vary. Multiple vehicles being almost simultaneously measured are another cause for error. At highway speeds the inaccuracy of the distance determination is enough to potentially flaw any attempt at speed measurement at a given location.

This same argument applies for battery operated vehicle transponders. However I do believe they would be inherently more accurate than backscatter types, even though I would not believe their accuracy would be sufficient for speed measurements over short distances. A counterpoint can be made that, if the distances between the two stationary transmitter/receivers is great enough, and I am not going to bother with the calculations but a quarter mile or so would certainly do it, the distance inaccuracy in reading the transponder would be rendered inconsequential and speed could be determined with sufficient legal accuracy.

So why not measure speed this way? Each stationary installation will cost many thousands of dollars ($30,000 each is a good estimate). And it takes two such installations. Why complicate life when it is unnecessary? It is much easier and vastly less expensive to perform the speed determination with radar and a camera. Or with a video system. Especially with a video system. Betcha this is what the New York State Thruway is using!

If you want to join the modern age in speed enforcement you would use a pure video system. Forget the radar; this system is undetectable. There are no emissions and, consequently, nothing to detect.

Fully automatic video enforcement is not yet legal in all states (aren't you lucky!) However, the laws of some states do allow ticketing speed violators via this method. Imagine a scene being photographed with the frame rate of the camera being known. Therefore a vehicle moving between two known points on the video picture can have its speed easily calculated. There are several systems that can do this. You do not even need an actual known point of reference.

Some systems allow you to "draw" two lines on the screen of your video monitor like the sportscasters do during a football game. When the vehicle crosses the first line a clock timer begins. Crossing the second line stops the counter and, bingo, your speed can be calculated very accurately.

When the calculated speed is above an arbitrarily set threshold a "freeze frame" will be captured and held. And, just to terrify you more, up to 26 lines can be drawn on one video screen, meaning that up to 13 simultaneous vehicles can be tracked. (You have to have one entry line and one exit line for each "detection block.")

Lines can define detection blocks for each lane, located adjacent to each other, or they can be located in the same lane, perhaps a quarter mile apart, subject to the video resolution possible. Different timing thresholds can be set for each detection block. And the camera does not need to be near the site in question, just have a clear field of view. However, since bad weather would limit the system's ability to "see" vehicles, the camera(s) will usually be mounted near the site in question.

Using near infrared technology cameras that are quite inexpensive, and near infrared "illuminators" which are really just floodlights operating in the near infrared spectrum, the entire site can be flooded with light for the camera to use, light that your eyes cannot detect... it will look dark to you and they can still see you!

With a line drawn for height detection and a side mounted camera, "over height vehicles," usually trucks, can be detected and someone alerted to stop them. If there are different speed limits for trucks and cars, this is how they can be differentiated.

The resultant "freeze frame" will be automatically processed to produce a printed picture of your vehicle from the rear, showing your license plate, and then imprint the image with your vehicle's speed, the date, and time. AT&T is above 95 percent accuracy in doing optical character recognition on your license plate and automatically entering the plate number into the computer system. Imagine how easy those European license plates must be for OCR. Now if we could just "standardize" the print and colors used on U.S. plates....

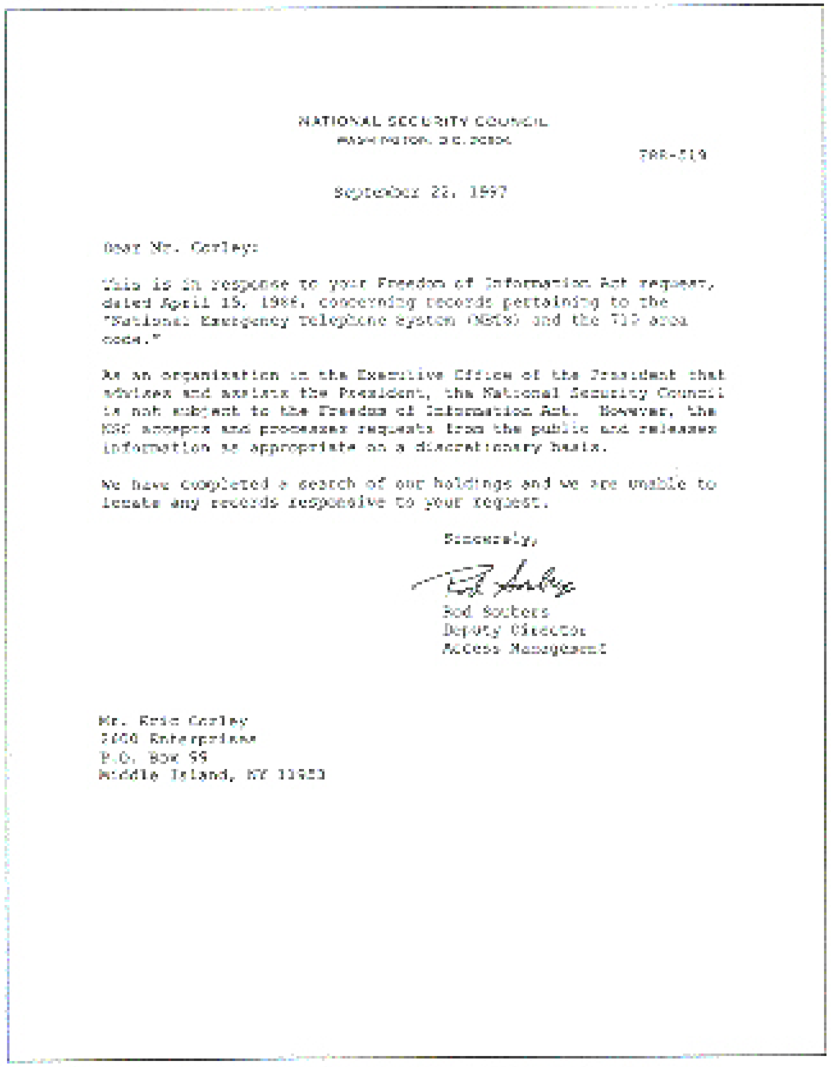
Not uncommonly, a second camera will simultaneously take a photo of the driver. Look around when you see one camera and see if you can find the second one. It can be mounted more than a block away from the site in question. Again, location is determined by the ability of the camera to take a good picture in adverse weather conditions. All of this results in a citation, including copies of any photographs taken, being mailed to the address shown on the vehicle's registration. Pay up or "see you in court."

As another aside, in some states the use of the second camera to photograph the driver has been considered an invasion of privacy and may not be allowed by that particular state, hence they do not know who is driving the vehicle. It is possible that the vehicle's owner may be held liable for the operation of the vehicle. One case comes to mind where the citation, including the driver's photograph and that of the incident passenger next to him, arrived at his house and was opened by the driver's wife. Needless to say, as revealed in the ensuing divorce proceedings, the driver had been thought by his wife to be elsewhere and not in the company of the lady next to him! I believe this case was sufficient to obtain the elimination of the "driver's camera" in that state and hence prevent future incidents such as this from occurring.

I am somewhat sure, but not absolutely positive, that the New York State Thruway is not issuing speeding citations solely via the use of the E-ZPass system. Perhaps a reader is with that fine agency?

In closing, do not lose the convenience of the E-ZPass system because of paranoia about speeding violation enforcement. If they want you they will get you with much easier and more efficient incontestable methods!

And, no, I do not work for the New York State Thruway. But I would use their E-ZPass system if I lived there.



NATIONAL SECURITY COUNCIL
WASHINGTON, D.C. 20506

788-519

September 22, 1997

Dear Mr. Corley:

This is in response to your Freedom of Information Act request, dated April 15, 1988, concerning records pertaining to the "National Emergency Telephone System (NETS) and the 710 area code."

As an organization in the Executive Office of the President that advises and assists the President, the National Security Council is not subject to the Freedom of Information Act. However, the NSC accepts and processes requests from the public and releases information as appropriate on a discretionary basis.

We have completed a search of our holdings and we are unable to locate any records responsive to your request.

Sincerely,

Rod Soubers
Deputy Director
Access Management

Mr. Eric Corley
2600 Enterprises
P.O. Box 99
Middle Island, NY 11953

Now THIS is what we call a diligent search. For nine and a half YEARS, the National Security Council has been searching for the information we were looking for. Three presidents have occupied the White House since we filed this request! Now that we have our answer, we can move to Plan B.

WE PRINTED YOUR LETTER!

True Hacking

Dear 2600:

I just read the article in Volume 14, Number 1 about hacking LED signs. A few years ago, a friend of mine and I were war dialing and, among other things, came across a modem number for True Value, a local hardware store. The login read something like "Type login I.D. or press ENTER for backdoor" so I hit enter and it asked for a password. I hit enter again and we were in. No password. While toying around to see what could be done we noticed the programming for the LED sign in front of their store could be done from here. But, being too paranoid, I logged off, and when I tried back several weeks later a password had been added. After reading your article, I plan to get back on there and have a little fun. I may even send a picture later. But, for now, I encourage *anyone* with a True Value local to them to start war dialing now.

bonaker

Fun At Barnes & Noble

Dear 2600:

My Barnes and Noble store uses four AT&T PCs for looking up books. If the ISBN number X50 is entered (Author COFFEE, J; Title COFFEE), all coffee sales for the past year are shown. I haven't tried X(1-49) yet, but I thought you'd like to know.

Black Jaguar

Anyone who can manage to publish a book with that title and author name stands to make a pretty penny.

Dear 2600:

/dev/thug had some interesting things to say about the Barnes & Noble computer systems (pressing alt+both shifts to open a config screen on any terminal) but he doesn't know the coolest thing.

First a brief run-down. The cash registers and dummy terminals at any Barnes & Noble store are run from two nodes in the back, typically one in the receiving room and one in the manager's office. They alternate, which means the odd number registers run from node 1 and the even numbered registers run from node 2 (it has happened that one node has crashed allowing the employees to still run the store from the remaining node).

In addition to the two nodes and dummy terminals, there is what is called an ISP (In Store Processor). These machines send sales data to the home office in New York. They were also recycled out of the old B. Dalton and Software Etc. stores when they upgraded their systems.

On the nodes in the back room you can press ALT+2 to change to a UNIX prompt and ALT+1 to change back to the Wings (their custom software) menu. (It may be Shift or Control + the number key, I haven't worked for B&N in a number of years.)

Now here is the cool bit. When the ISP logs on to the nodes to get sales data for transfer to New York *it doesn't log off*. So if the store manager gets lazy and runs the ISP routine at 8 or 9 pm (I've seen them do it as early as 5) then all you have to do is get access to one of the nodes (easy if you work there, harder if you don't), get to the UNIX prompt using the above method, and you have complete system access at the root level all because the people who set up the ISP were too dumb to log it off.

I saw this first hand at four Barnes & Noble stores and I repeatedly warned them about it as a security hole. If they haven't fixed it by now then they deserve what they get.

anonymous

Dear 2600:

After reading /dev/thug's letter to you in Volume 14, Number 1, we had to send in a reply. We at the Barnes & Noble's Support desk would like to thank him for the wonderful laugh.

In his letter he wants to dispel some misinformation about the store. He failed miserably. First off, the system is not proprietary. B&N likes using standard hardware and configurations because it makes supporting the system easier. As for the Operating System, our friend must not be familiar with UNIX or DOS because that's what runs most of our stores. Only a few stores at this time are running Windows NT and I hope he knows how to recognize that!

/dev/thug must have picked up a computer dictionary somewhere and neglected to read the definitions of the big words he was trying to use to impress your publication. Not all our stores use a "Star Topology." A lot depends on the number of registers and nodes. The star topology is used in very small stores. Another thing: the main server does not "run blind." It has a monitor and keyboard. This is where the store runs the openings, closings, and other managerial functions.

The operating system he talks about is not called Wings. The operating system is QNX, a version of UNIX used for point of sales applications. Wings is just a label given to the system. As for the "secret configuration" screen of the DT's, it's not a secret. Anyone with any kind of computer knowledge knows that DT's and PC's have CMOS screens and that's all this is. There isn't much fun in playing around with these settings because almost any change made will either freeze the screen or make it go to a blinking cursor. This can be reset by hitting "D" to reset the defaults, "S" to save them, and "F9" to exit. There is no "E" command as /dev/thug stated in his letter. He must be out of the info chain as far as development goes because the idea of putting Book In Print onto the store system was scrapped over a year ago. Instead B&N has chosen to create their own Title database that will be incorporated into the new system. And the best part... the ISP (In Store Processor) is a glorified word processor. The ISP has only two real functions: one is to keep track of the store's magazine inventory and the other is to let the store manager read their administrative messages (a cheesy form of email). It's not even a backup to the nodes. There are no modems connected to it even though sometimes one of the store modems is labeled "ISP modem." If the wiring is traced it goes nowhere near the ISP. There is no "fone/phax bridge" - it's two modems on the node. One is for polling and the other is for the store to shop vendors.

If /dev/thug had taken a few minutes to call us at Westbury, we would have gladly answered any technical questions he may have had. We don't mind taking time and going over the system. Having people in the stores who are educated on the system makes our job easier.

Barnes & Noble Financial Center
Westbury, NY

You may be getting a lot more educated people in your stores than you can imagine. Thanks for the info. We've now published letters from three different Barnes and Noble employees, all of whom are cool enough to share info rather than restrict it. Surely such people exist at other large chains...

Righteous Hacking

Dear 2600:

I read the article "Sharp Cash Trix" in the Spring 96 issue. Mr. Fiery gives info on the Sharp ER-3100 cash register. The ER-3100, according to Fiery, makes no noise when the drawer is opened by hand. The Sharp ER-3231, which looks very much like the 3100, makes a loud ding (similar to the ding elevators make) when opened by hand. I do hope some asshole who wrongly considers himself a hacker tries to abuse the info by trying to open what he thinks is a 3100 in order to steal money. Then, to his dismay, the register, which is really a 3231, makes a loud ding that gives him away. Every wannabe who makes hackers look bad by abusing our information should get caught that easily.

Bomber Chick

Dear 2600:

I would like to ask a huge favor of you. I have a 14 year old son who, regretfully, I do not have custody of. He is very bright and computer literate. Unfortunately he has steered his creative energy in the wrong direction lately, such as hacking into the school computer, letting a few viruses loose, and getting caught. I would love to get him a subscription to 2600, but alas, my parents, who have custody, would go ballistic. Could someone there please drop him a little note, via snail mail, and tell him a little bit about "hacker ethics?" Coming from 2600 I am sure it would have much more influence than anything I could write or say. It would mean very much to me as well as him.

Katfish

We're not able to send out individual replies (and in this case getting an unsolicited personal note from a strange magazine may cause way more harm than good) but you can clip this reply and mail it to him, anonymously if necessary. Hopefully others will heed this too: it's easy to screw things up with knowledge. That leads simpletons to the conclusion that certain knowledge is bad. They will never experience the thrill of hacking and the rush you get from discovery. They are rule followers who don't want to ever rock the boat. And then there are those the rule followers need - the rule breakers who cause mayhem for no real reason, just because they can. You have knowledge and ability and a good chance of avoiding the dead end lives of the above. Understand why you either follow or break the rules and use that knowledge to change things. And, above all else, don't hide behind hacking as a reason to do things you would never do in real life. What you do behind a keyboard should be a reflection of the values you believe in already.

Replies

Dear 2600:

This is my little response to Mr. "I'm gonna bust your balls" from 14:1. Professional... ha! Can't even formulate a decent argument. I'm not writing just because of the content of his letter but the overall tone of it. It was spiteful. And what's sad is that what he thinks is what the majority of people think. He's completely taken in by the media stereotype and doesn't seem to exercise much thought of his own. And it's the little things in his letter that tell me this.

First, if he actually read 2600 or knew anything about us, the first thing he would realize is that we aren't crooks. Case-in-point: the numerous letters you received regarding "How to Steal Things." Theft is not the driving force behind what we do.

Second, handles are not something that we hide behind. It does not display any cowardice. We use handles to create identities. There's a lot you can learn from a handle - favorite bands, favorite authors, attitude, etc. Would he consider Orwell a coward for hiding behind a pen name?

I would imagine that this gentleman (and I use the term loosely) knows nothing about what he appears to hate so adamantly. They say that hackers do what they do because of some innate immaturity. Read his letter. Which side is being immature? Not the Professional. He says he laughs at punks like us. His letter wasn't very jovial. And I'm the one who fell off the sofa laughing when I read it.

"Hack me and I'll bust your balls." Whatever.

Imran Ahmed a.k.a. Eric Blair

Dear 2600:

This is in response to billsf's letter (Summer 1997) regarding my "Red Box Detection Circuit" (Spring 1997). My article and design was silly, but not an April Fool's joke like billsf had mentioned. Many people had displayed interest in seeing such a circuit, so I went ahead with it. The article was meant to show people what can be done with electronics and was to be used as a building block and learning tool. With any design, be it hardware, software, artwork, etc., there are many different ways to get to the final goal.

billsf seems convinced that the mentioned circuit will not work, but he did not take the time to build a prototype of my circuit before criticizing it. I have prototyped and tested the circuit multiple times, and it works flawlessly.

In response to his claims:

1) "Using a LM386 as a preamplifier is simply not a good choice and powering it from nine volts to drive a five volt chip is looking at a blown IC!" The circuit I used for the audio pre-amp is the standard example circuit for an amplifier with a gain of 200 as described in the National LM386 data sheet. I happen to like the LM386 Audio Amplifier because of its ease-of-use and easy availability. The limits of Vcc to this chip range from 4V to 12V, and 9V is very much within this range.

2) "The 510k to -5V is also mysterious." The 510k resistor used to power the condenser mic was chosen after brief experimentation. The value seems to work perfectly with my microphone, so why change the design? As with any electronic circuit published in a magazine, the values should not be set in stone, because of differences in components and tolerances. Your microphone may require a different value, but it works fine with mine.

3) "The MX105A is a very poor choice for the detector, as it requires adjustment." I thought this feature of the MX105A was very attractive because the circuit can be "fine tuned" for frequency detection of your own specifications, and you aren't stuck to the standard frequency tolerances of the 8870 DTMF decoder. I chose the MX105A because it was an interesting IC and I wanted to experiment with it. In an email correspondence, billsf explained to me a different circuit with the same result using the 8870 DTMF decoder (described in his letter). Although I respect billsf's knowledge of electronics, he must realize that there is not only one correct solution to the design.

4) "Anyone who would attempt to build this should know that the LED will go on and off at every other pulse." By only looking at the schematic, this may appear to be the case. The one thing that cannot be seen in the schematic, but only by comparing the component values to the MX105A data sheet are the lock and detection times. Since the five pulses of the "quarter tone" are so close together, we can choose values to make the IC detect the entire string of tones, instead of each of the five tones. This way, the Detect Out pin of the MX105A will toggle high and low for each quarter, not each nickel as billsf claims.

As an aside, I noticed a mistake in the published schematic of my article. All of the components connected to the right side of U2 (MX105A) should not only be connected to each other (as shown in the schematic), but pulled to ground as well.

kingpin
L0pht Heavy Industries

Dear 2600:

It's good to see some crypto-related articles in *2600* (Seraf's "Fortezza: The Next Clipper?" in v14 n2). But *please* encourage the authors to do their research before discussing the subject. There's plenty of available texts, papers, source code (online and in the bookstore), and even mailing lists and newsgroups regarding cryptography.

Some comments and nitpicking:

(1) The NSA didn't force DES on anyone. By the early seventies, a lot of corporations needed a standard that was publicly known and deemed secure. As suspect as the NSA was and is, there were few other people or organizations at the time with the skill to evaluate algorithms.

(2) As to whether DES was purposely designed by the NSA to be easily cracked: what is meant by "cracked"? Very likely there's no subtle mathematical magic keys that can easily decrypt the algorithm. Despite the religious view many paranoids hold, the NSA is not so many light years ahead of the rest of the world mathematically that (even if crash test dummies from Roswell help them out) such a ruse could be pulled off. If ever such a thing were discovered, the NSA would lose all trust from large corporations that have used DES. It *might* be that DES was designed to allow special key searching algorithms combined with some forms of cryptanalysis to work more efficiently, but this is still brute force cracking and anyone with the resources (a large corporation, other foreign governments, or a group of people on the internet) can do this. Unlike Skipjack, DES has been public knowledge for over 20 years and anyone who wants to can and has (and will be for some time) scrutinizing and tearing it to pieces. And keep in mind that a purposeful weakness made in DES by the NSA could have been discovered by, say, their Soviet counterparts, who would have enjoyed being able to decrypt Western capitalist financial transfers.

(3) As for the Digital Signature Algorithm (DSA) and companion Secure Hash Standard (SHA-1 algorithm), these are also public and open to scrutiny. They were designed to be used for signatures (which the NSA would have little interest and use in being able to forge - the only use for a weakness or crack in a digital signature algorithm). Which is not to say DES, DSA, or SHA-1 are perfectly secure algorithms. They have their weaknesses when used in certain circumstances. All crypto algorithms do.

Fortezza and Skipjack may not matter in the long run: there are plenty of non-NSA and non-US, publicly available algorithms, plenty of widely available (often free) crypto software (with the source code if you're really paranoid) using non-Skipjack standards out there.

I'd be more interested in seeing an article about hacking Fortezza, and figuring out more about how the Skipjack algorithm works or to find flaws and weaknesses in how the card operates.

Deranged Mutant

Seraf replies:

"The NSA did not force DES on the public in its early days, but it didn't need to - America was so happy to finally standardize on a single cryptosystem that it embraced DES. Does the Agency force the algorithm on companies today? Let's just say that they won't license any company producing truly secure crypto goods as a Fortezza manufacturer.

"Regarding your scrutiny of my allegation that DES is 'trap-doored,' this is now a well-known fact. The S-boxes, along with their 'magic numbers' (which were changed from LUCIFER, on which DES was largely based, for no publicly-stated reason), are specifically designed to make the algorithm weak in government hands. So, in those 20 years you speak about, DES HAS been torn to shreds, to some degree.

"Moving on to SHA-1, I never said that it was weak/weakened - not sure where you got that one from. DSA, however, has NOT been extensively peer reviewed, and it would certainly be in the NSA's best interest to have it backdoored. Unfortunately, however, I cannot give evidence for this hypothesis as compelling as the evidence that DES is trapdoored. It's just something to keep in mind, as a possibility.

"Finally, you proclaim the availability of REALLY strong crypto as a damper on Fortezza's significance. For those of us who understand these technologies, Fortezza is indeed something we can brush off our collective shoulders. However, to an uninformed public, and to many of the people who make security decisions for American businesses, Fortezza can be very inviting - just as DES was inviting in the 1970's. The difference is that we have options now - everyone just has to see them."

A Challenge

Dear 2600:

My (real) name is Clive. I'm 46 years old. I've spent the last 20 years collecting incriminating information on people and businesses I don't like. I do this by whatever means I deem necessary. I can do things that you can't do. All the information you need to find me is printed on this page. There's nothing secret or sneaky or hidden - the words are all that matter (you could read this over the phone and get the information you need). There are no fingerprints. There's no saliva on the envelope. It was printed on a laser printer at a local service bureau. Anonymous remailing isn't limited to e-mail - this letter was remailed at least twice (I don't live in Colorado or California - probably where the postmark is from). Here's my challenge.

If you can find me, I will give you documentation on the technologies listed below, how to use them, whom to use them against, and how to get to those people easily. If there's anything you want to know, ask me and I'll tell you if I can.

If you find my e-mail address, send a message saying you found me, and include a secret word and number combination, and a newsgroup that you want me to post information to. I'll post using your word as my userID, with information about where to go to get what I've promised. You'll use your number to retrieve the information. If you don't care about anonymity, say so and I'll just e-mail the information directly to you.

If you find me by telephone, figure out how you want me to give you the information, and I will do it that way (or by one of my own methods).

If you find my home address, pick a communication method, or pick a newspaper and we can communicate through classified ads (remember to include an identity for me to use).

If you can find my web site and hack it, there are some cryptic links to this information buried in there.

If you find me at work, bring me a sombrero. I'll give you what you want, and then I'll be on the next plane to Mexico.

If you're with a law-enforcement agency and find me, be sure you have the paperwork for search and seizure, but don't confiscate anything (nothing is on my hard drive, all data is on self-destructing non-electronic media - if you don't know how to get it, it's gone). Just ask for it and I'll give you everything. When I go down, a lot of assholes come with me.

What I'm offering:

Cellular information: how to listen to, and make calls from any known phone (free, not stolen and cloned numbers - that exist "between the cracks"). This includes analog cell, all types of digital cell, PCS/GSM, and satellite. This includes information on cloning digital and how to make or change "smart cards".

Computer hacks: how to get into and use "supers," and access to government, insurance, bank, and credit company (among others) computers. This lets you view and change driving records, credit records, etc.

Telephone information: how to access and manipulate digital switch controls remotely. Anything the telephone system can do is done through these switches.

That covers your basic interests. There is also other information about a number of electronic devices, as well as source information included. A lot of this information concerns things that people are told are impossible to do (like cloning digital phones, for example). Most of my information can be gotten from publications you could find in a public library - if you know how to use it and what it applied to. I doubt most of you could figure out what you want to know unless it was given to you.

What you need to know to find me:

TL/GSCV156330098-74

My name is Clive

That's all. If you know what it refers to, it's really easy. A lot of people who probably aren't hackers could see that and find me in about a minute - it's a common sequence of a public number. The simpler something is, the harder it can be to figure out.

I made this offer so more people could help to make a difference. There is responsibility involved. I hope that the clever ones of you who get there can handle it. If you weren't mostly irresponsible punk assholes, I'd just give it away freely. If you really care about changing the system, this has been a good way to do it.

Clive

Of course this could be bullshit but if it isn't we're certain someone will take up the offer and figure this out. Your days of anonymity may be numbered. We hope to hear the results.

Questions

Dear 2600:

While I was waiting for the school secretary to get off her fat ass and give me my schedule I amused myself by reading the back of her monitor. As I read I grew confused. Here's what it said:

FCC ID: L5ACPD100SF

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

Why would the Federal Government ensure that one's computer could be interfered with?

SILSD2000

This is one instance where it's not a plot by the government. Electronic devices are subject to interference from other more powerful devices - radio transmitters, etc. When this happens, you have no legal recourse or moral right to prevent this interference. It's up to the manufacturer to ensure that neither of these two things occurs.

Dear 2600:

Does the Editor-In-Chief, Emmanuel Goldstein have anything to do with the Emmanuel Goldstein (Serial Killer) in the movie *Hackers*?

Phracture

Consider it an inside joke. That's really the extent of it. And, no, nobody here got paid for that.

Dear 2600:

In order to solve a argument between me and some friends, do you pronounce 2600 as: "two-thousand six hundred" or "twenty-six hundred" or "two six zero zero?" It would solve a little conflict if you could please answer this message.

scott

In the States and most other places it's pronounced "twenty-six hundred" but in England for some reason it's more common to say "two-thousand six hundred." We honestly have no idea why.

Dear 2600:

Is it true that if you record the tones coming from the receiver of a phone when five dollars worth of quarters is put in then, going to another phone playing the tape then pressing the coin return lever and you get five bucks?

CP

Those little beeps indicate the presence of money. You can't use them to create actual money. If that were true, phone companies might actually be in danger of losing money.

The End?

Dear 2600:

In August, I found three NYNEX phones that are no longer accepting red box tones. Red box tones played into the mouthpiece are not heard through the earpiece, although touch tones played through the mouthpiece come through loud and clear. At one of them, I saw a NYNEX repairman installing a beige rectangular module measuring approximately 2" x 1.25" x 0.5". The module marked "FRAUD PIN DEVICE" was installed in the phone and wired in series with the handset wires. This module effectively filters out the red box frequencies. Red box, RIP.

Ripped Off by NYNEX

Many phones now mute out the mouthpiece while money is being accepted. We'd like more info on this "fraud pin device" you saw.

Critics' Corner

Dear 2600:

I enjoy reading your mag but WTF is this with the Special Spoofing issue written on the front of your mag? Is it hidden somewhere in the mag and I didn't see it? This brings to mind the "red box issue." Why do you keep writing shit on the cover if you don't include it in your mag? I don't see any point in this other than trying to get people to buy your mag that normally wouldn't.

sTs

No, we do it just to annoy you.
Alternate answer: buy a dictionary.

Dear 2600:

In the letters to the editor section of the Summer 1997 issue, readers called into question your judgment on a couple of things that make me believe 2600 does not hold itself to a standard so high as I thought.

First, your response to a reader questioning your printing of "Credit Card Numbers Via Calculators" as a show of support for credit card fraud. Your defense that it is only an exercise in algorithms and calculator programming is bullshit. This sounds like something a lawyer would say. I suppose you believe head shops sell pipes that are not intended to be used in any illegal activities. Printing information for knowledge is quite different than printing information that could be used in the commission of a crime against innocent people. I sense you are losing the ability to tell the difference.

Second, the Mitnick thing. What is wrong with you people? You act like Mitnick is some kind of God and that he is being persecuted by the powers that be. The truth is Mitnick is a punk. If he shouldn't be in jail because "there are a great number of holes in the accusations hurled at Kevin" then he should be in jail because he is stupid. Anyone who continues to do what he did after being in trouble for the same thing needs to be punished. What does it take to get through Mitnick's head to stop hacking? If he is such a genius, why doesn't he realize this? He's lucky he never broke into any shit of mine. I wouldn't have been as merciful as Shimomura. Instead of spending the last two and a half years in jail the SOB would have spent the last two and a half years recovering at a local hospital.

Technically, Mitnick is not great at all. After all, he did get caught. And most of the techniques he used were obtained from more clever and skillful hackers. Anybody can use the social engineering techniques used by Mitnick. You just have to be willing to lie like a dog (which I'm sure is OK by 2600 standards). His greatest social engineering feat has been convincing 2600 that he is a victim.

Has Mitnick ever contributed anything to society? Isn't it about time for him to grow up and get a job and go on with life contributing something of value to society?

Orion

You obviously can think of only one use for studying credit card algorithms which makes you just as pathetic as the idiots who commit credit card fraud. That's your problem.

But your views on Mitnick are truly disturbing. In the interests of space, we'll skip over the childish posturing and focus on your apparent belief that his imprisonment is justified. How can you honestly say that so many years in prison (his trial at press time is being scheduled for April 1998, more than three years after his imprisonment) is a suitable punishment for someone who has never committed a violent crime or profited in any way from his actions? Just how much vengeance do you want and exactly what is it that you think you're avenging? Your loss of privacy and security? You lost that a long time ago. And the people who've locked Mitnick away have no interest in giving it back to you. Mitnick didn't expose your life for all to see. It's the fact that he could have or really that anybody could have that has you so bent out of shape.

Who is the real victim here? You? Us? Corporate America? Not at all. The real suffering has been going on behind bars the whole time. And the real problem is simplistic idiots who go around thinking that violence and imprisonment are the only ways of dealing with things. This method of thinking has transformed our society into the short-sighted reactionary wasteland of paranoia that plagues us daily. And that will make victims of every last one of us. We'll see you there.

Dear 2600:

This letter is in response to your reply from my letter you printed in the Summer 1997 issue.

I feel your publication is misleading your readers into thinking that Kevin Mitnick has been mistreated by being imprisoned for two and a half years without trial or bond. Tell me if I am wrong or not, but I do not believe you have told your readers that in July 1995, Kevin had plead guilty for one charge of cellular fraud while in Raleigh and received an eight month sentence. A trial is for determining guilt or innocence. Since he plead guilty, no trial. Since he already has been shown to be a flight risk and shown to be a habitual criminal in their eyes, you can understand why he has not been allowed to bond out of jail, even though he has already served his original eight month sentence. As for the problem with his probation, he was being investigated for probation violation, but since he fled the area, it is more than quite obvious that he violated probation.

Don't get me wrong, I believe that the justice system is as corrupt as most of the politicians in office, and racking up convictions seems to be more important, and the penalties for hacking, phreaking, etc. are outrageous. But most people do not want this happening and if the maximum penalty for running up someone's phone bill a few thousand dollars was only 10 to 30 days in jail, then quite a few people would be doing it all the time.

So now you can see where I am doubting his mistreatment, or maybe I am just missing something.

TC
Fort Leavenworth, KS

You are. This case is not about making free phone calls. People who steal don't get treated this badly. This case is about sending a message to the rest of us. You can bet every hacker who gets prosecuted in the future will be made aware of the Mitnick prosecution and how it is indeed possible to spend large amounts of time in prison for doing little more than evading capture. Prosecutors will have little trouble making deals with almost anyone as long as they have this to point to.

Mitnick Fallout

Dear 2600:

I was absolutely shocked after reading your article about Kevin Mitnick, "The Neverending Story." No matter what he did, nobody deserves to have their rights taken away like that! Rapists, murderers, and child molesters get off easier than this. Technology is growing and advancing at such a fast rate that things like computers, cell fones, and pagers are unbelievably common and part of our everyday life. And these are all things that they want to keep Kevin and others from using! And I can't think of the last time that I walked into someone's workplace and didn't see a computer. What do the authorities expect him to do about a job? Would he be allowed to use the computer behind the McDonald's counter? They are basically throwing him onto the street with nothing.

Like you said, it is the complete lack of understanding of technology that makes the authorities come up with this complete bullshit. People like Kevin who possess such an unbelievable amount of knowledge should be hired to catch the real criminals.

Phip-C

Dear 2600:

We read the latest issue of 2600 and we were startled, to say the least. The conditions of Mitnick's release were unbelievable. What's he going to do now, be a farmer? I mean really, they are affording him practically no options to earn a living in today's society.

DM & NightShadow

Perhaps that's why they're showing no indication of ever releasing him back into that society. Maybe they think prison is more merciful.

Dear 2600:

I've seen many letters in your magazine about how the education system can't stand the mention of back-crypbreakers, and are quick to blame them for any problems related to data loss or phone misuse. So I decided to test the waters at my local high school. I let my Government teacher read "The Neverending Story" article in the Summer 1997 issue, being that she is a firm believer in the Constitution. She was outraged at the circumstances of Kevin Mitnick and the restrictions he faces after his release. She agreed that this is a total violation of his rights under the First Amendment. I feel sorry for my fellow

Generation X'ers who are under persecution by their schools, and I encourage them to press on in the fight for freedom of information.

fiNred
Montgomery, AL

Thanks for helping to open some eyes.

Circuitry

Dear 2600:

The Red Box detection circuit Kingpin showed how to create in the Spring '97 issue can also be used as a remote activation system. Wire it up to whatever you want it to activate, and place it next to your answering machine. Call home on a payphone, and just put a quarter (or nickel or dime) in the slot. It will activate the detector, and you'll get it back when you hang up. Oh, this won't work on COCOTs.

In Volume 14 Number 1, DETHMaster submitted an excellent TI-82 progie to generate credit card numbers. However, I found that the program had a rather glaring bug: It was unable to generate Discover credit card numbers. Discover uses the prefix 6011, which caused the program to fall into an endless loop. This modification should solve that error: Immediately preceding the line 0->S, insert:

```
:If [A](1,2)=0
:Then
:1->F
:Else
:0->F
```

And the line that reads:

```
:[A](2,P)+S->S
```

Should be changed to:

```
:[A](2,P)+S+F->S
```

I hope this solves any problems!

Crumpet

Suggestions

Dear 2600:

I was thinking about the millennium bug (computers supposedly will not be able to tell the difference between 2000 and 1900 due to an error in coding, and they might interpret the change of 00 at the end of the date as 1900 instead of 2000 which will in turn cause a majority of systems to shut down) when I realized a quick fix to this might be a Morris worm program to correct the problem on a widespread basis. Anyhow if the hacking community presents this even as a workable solution at the very least it might improve the public perception of us, especially for something we took so much shit over in the first place.

Steven

Sending worms out all over the net to fix software is probably not the best way to make friends.

Dear 2600:

I'd like to comment on the issue of free speech on the net. Recently on a certain site, I saw copies of the *Anarchist's Cookbook* and other documents which explicitly show how to create bombs, poisons, and things that could be used to murder hundreds of people at once. My position is that sites like this are the reason that bullshit like the CDA exists in the first place. Freedom to exchange information means freedom to exchange it responsibly. If you give a baboon a gun, and the baboon shoots someone, do you point the finger at the baboon? Just because it is probably not against the law to give firearms to primates does not mean we should all do it. Giving step-by-step instructions on murder to lunatics is equal to giving guns to baboons. If information is to remain free, we must act in an adultlike responsible manner when distributing it.

On a lighter note, I submitted a Unix backdooring article. Willing to give ten to one odds that a "How to Red Box" article was published in its place.

sh

And just who would you be willing to trust to decide what information should be given to whom? People need to be responsible with the information they obtain. That's where the burden rests. Once you start deciding who has the right to read what, any semblance of a free society goes down the drain. You'd better start boycotting libraries and bookstores too since the Anarchist's Cookbook was in those decades ago. And our last "How to Red Box" article was Autumn 1994.

Problems

Dear 2600:

My name is [obliterated] and I am hoping you can help me with a problem I have been having for 2 1/2 years. I saw an article in *Newsday* on Sunday, June 8, about hackers. At the end of the article, a women called the radio show about someone billing calls to her calling card to Bangladesh. We are having the same problems.

About two and a half years ago, our phone bill contained over 300 calls to adult sex lines and it hasn't stopped. The account is in my husband's name. Our phone number at the time was [obliterated]. We blocked access to these numbers but more things came up. We were billed for international, long distance, calling card, collect calls, all to our bill. Companies like Pilgrim Telephone, Telemedia Billing, and others showed that we called long distance using these carriers. We called all the companies, NYNEX, AT&T, to tell them we did not make these calls. They all said they were directly dialed from our home. Our children are small, we had no one home for many calls, but they practically called us liars and my husband a pervert. We have gotten NYNEX's recourse department to take off the calls which eventually were over $700 and sent them back to the independent companies for billing. We are now being pursued by collection agencies. By the way, in August 1996 we moved from our home and had our number changed to an unlisted number in an effort to stop this. We had the lines checked, we have blocked everything possible to block but to no avail.

Since reading the article on hackers, I am convinced that a hacker is somehow getting these calls billed to our account. I am begging you to help us solve this problem. We cannot call long distance anymore, use a calling card, or call collect. We are at our wits' end to solve this. Please, please help us, or get the word out to your fellow hackers to please leave us alone and go on to someone

else. The article stated that hackers usually do this to reveal the flaws in computer systems, but this person, or persons are illegally billing these calls to us. NYNEX will not admit a problem. Also, calls were being charged to our credit cards. I have canceled one card, and changed the number on the other but it is still happening. *Help!!!!!*

[Name Obliterated]

First off, let's clear something up. Whoever is doing this to you is not acting as a hacker. Just because someone has the ability and is capable of figuring something out does not mean that they are the culprit. Now, concerning your problem, it seems relatively clear that you are known to the perpetrator. Otherwise, this wouldn't follow you to another location, another number, and a credit card. It's up to you to figure out why. As for how, that's pretty easy. There are bugs in many of the major long distance companies and almost all of the smaller ones that allow people to bill all kinds of things to other numbers and make it appear as if those other numbers made the calls. We've seen cases where sleazy companies just ignore third number billing blocks and collect call blocks and bill using those methods anyway. It's possible to make weird things happen by dialing into an 800 number using an operator who has gotten an ANI failure - the number you tell the operator then follows you around on whatever calls you make through that 800 number. We're certain there are an almost unlimited number of ways of doing this. If the phone company is serious about tracking this down, they should put a pen register on your line so they can see this happening live. Yes, they can be used to help customers as well as spy on them. Demand it. And don't be afraid to launch a criminal investigation. This kind of thing does none of us any good.

Dear 2600:

Every day when I am on my phone, it will make a pulse dialing like sound through the phone. It doesn't usually bother me when I am talking on the phone, even though it is rather loud, but when I am on my modem, it messes up everything, and I have to log off of whatever I am doing. Sometimes I also pick up other people's conversations as well, even when I am not on my cordless phone. Do you have any ideas what in the world this is?

MaRTiAn

It's just a wild guess but we'd say you've got a crosstalk problem. Report it to your local company each and every time it happens. If they don't fix the problem, odds are they'll move your line to another cable pair to shut you up. You can also track down the one cranky old-fashioned person in the neighborhood who's still using a pulse phone and have a little talk.

Dear 2600:

Ok, I give it to you short and simple. I was up one night and somehow got my parents' password for the internet. They found out I knew so they changed it. I want to get it again. Do you have any ideas for me how to get it?

sryob

Well, you could "somehow" do it again the same way you did it the first time or you could monitor them somehow whenever they log on. A keyboard sniffer on your local machine could do the job if they actually type it in. We doubt they've put it in a script since you could just run that without ever knowing what the password is. Since you're probably going to be spending another decade or two living with these people, it might be wise to ask yourself why they don't want you using their account and what will happen to you when you're repeatedly caught.

Improvements

Dear 2600:

First off, I'd like to say I've been an avid reader of *2600* for a number of years and enjoy the consistently good issues which cover important topics that most people would otherwise fail to hear about. While reading the article entitled "How to Generate Credit Card Numbers On a Calculator" in the Spring issue of *2600* I found a series of mistakes (most likely typographical) in the code.

The idea of generating CC numbers on a TI-82 to learn about the Luhn algorithm is a great idea and it's a shame that a small mistake might ruin that chance for the curious reader. The problem is where the code assigns numbers to the second matrix (it starts at the bottom of the first column). The part where it says:

```
[A](1,1) * 2 -> [A](2,1)
[A](1,2) -> [A](2,2)
[A](1,1) * 2 -> [A](2,3)
[A](1,2) -> [A](2,4)
```

etc. should read:

```
[A](1,1) * 2 -> [A](2,1)
[A](1,2) -> [A](2,2)
[A](1,3) * 2 -> [A](2,3)
[A](1,4) -> [A](2,4)
```

etc. and, of course, the first matrix should keep incrementing with the second. After this small correction is applied, the program works perfectly.

Matter

Numbers

Dear 2600:

Wading through and checking up on some old printouts of dialups and other assorted numbers I've accumulated over the years, I came across a number I recognized as a service which, per some magazine ad, was supposed to offer free PPP service: (217) 792-2PPP. I called it up and got a series of weird tones which I've not yet taken the time to attempt decoding or anything, then some mechanical, automated voice: "Dial 9-1-1 from your calling area. Hang up, and dial 9-1-1." After that, if you stay on, those same tones can be heard faded in the background. Any ideas?

Ydeologi

Those are old fashioned MF tones before the recording. We don't know what purpose this serves. After around five minutes, we get a recording saying the party isn't answering so a connection isn't actually being made. Since this is in-band signalling, it may still be possible to blue box off this exchange.

Dear 2600:

While attempting to get tech support from Microsoft, I incorrectly wrote their 800 support number as 1-800-426-9200. When I dial it, an automated voice reads the numbers 21 7 1 1 4 0 5 0. I am guessing the 405 part is the (my) area code. The results are identical if I call from a PBX or a COCOT.

DJinOK

It's not your area code since we get the same thing. Incidentally, those touch tones you hear translate to 02142047114050305.

Dear 2600:

305-625-3335, produces loud cycles of noise when called. I'm stumped.

A.

This is a sweep tone, used by phone companies to test frequency response, used by hackers to annoy and confuse.

Dear 2600:

A couple of issues ago you gave two different ANI's. One was in English, the other was in Spanish. English 1-800-MY-ANI-IS. Spanish 1-800-235-0900. Well, as you all know, the English one no longer works, but if you call the Spanish one and listen to the lady talk for like 10 seconds it gives you the option of choosing your ANI in English or Spanish. To get it in English you have to press 2. I hope I have helped some of you.

Spillage
Orange, CT

You certainly have. We never thought to stay on the line ourselves.

Dear 2600:

Here is another toll free ANI: 1-888-324-8686. It uses the Bulletproof Voice Mail service, the same as 1-800-611-8791 which was posted in Vol. 14 #2, so therefore it works only twice from the same number (maybe once by the time you try it out).

Mwaaah

This new number does indeed work twice in 24 hours and no more.

Dear 2600:

In case nobody's heard yet, Southern New England Telephone's information operators will now do reverse lookups. Granted, you can only give them Connecticut numbers, and unlisted numbers are listed as such. Payphones are not in their listings at all.

Jonny Deth

Uh Oh

Dear 2600:

I'm ashamed of you. How could you people call yourselves hackers? You've overlooked one of the simplest security holes. I fingered 2600.com and it told me all the people logged on. That is half (and possibly all since root was running) of what I need to break in.

Josmo

Come and get us.

Fixing Juno

Dear 2600:

Hacking around on the computer one day, I whipped up a handy batch file which can be used to remove those stupid ads from Juno automatically upon execution. This allows you to enjoy all of the benefits of Juno without the advertisements, finally making the email service truly free. Begin by finding the location of certain files within \juno (or whatever you named the juno subdirectory). Look for a directory named \juno\ads and especially for directories starting with 0; these are the ones which contain ad files that need to be deleted. Use a command such as deltree /y 0* to delete all the files within this subdirectory. Next go to the \juno\ads\logs directory and delete all the user logs (such as user0000.log) by using del user*.log. Return to \juno\bin and run juno.exe as usual. Below is a template for using the above in a batch file.

```
@echo off
c:
cd\juno\ads
deltree /y 0*
cd logs
del user*.log
cd\juno\bin
juno
```

The above file will remove the unwanted junk ads and will make Juno truly free.

BuPhoo

Dear 2600:

I have found a new way to make the Juno email service a little more interesting by altering the startup bitmaps and running Juno through a batch file (remember those?). This allows you to select which image is to be displayed, runs Juno with the new image, and changes the image back when you exit Juno. I did this all in version 1.15, so it might not apply to some of you running the newer version. First of all, make a new directory for your images. Let's call this new directory IMGS. Now, go ahead and open up JUNOLOGO.BMP in the \JUNO\LIB directory. This bitmap is 342 x 397, and 256 colors by default. Go ahead and fuck with this image all you want. Save each new image under a different name in the IMGS directory. Name them like JUNOx.BMP, where x is 0-9 or A-Z. Make sure they are all still *.bmp format. Now, you must make the batch file. It goes something like this:

```
@ECHO OFF
DEL JUNOLOGO.BAK
REN JUNOLOGO.BMP JUNOLOGO.BAK
COPY JUNO%1.BMP JUNOLOGO.BMP
CD..
CD BIN
JUNO
CD ..
CD IMGS
DEL JUNOLOGO.BMP
REN JUNOLOGO.BAK JUNOLOGO.BMP
```

Name the batch file JUNOBAT.BAT or something and place it in your IMGS directory. Also, copy the JUNOLOGO.BMP file out of the \JUNO\LIB directory to the IMGS directory. You must now alter the properties of the batch file to make the whole thing work. In Win95, right click on the batch file with your mouse, and select properties. Go to the Program tab and add a question mark at the end of the line where it says Cmd line. Now click OK and you're done. Now just run the batch file, and a dialog box will appear that says parameters. Type in the number or letter of the image you want displayed. Like 1 for JUNO1.BMP or A for JUNOA.BMP or whatever. Click OK and Juno should launch with your new image. There, now don't you feel proud!

cap.n_crack

Offended

Dear 2600:

Hackers and anarchists have at least one thing in common: Both groups are being demonized in mainstream media and are represented as disturbed individuals bent on meaningless destruction. That our corporate media spread lies and distortions should surprise no one. I am surprised, however, when I find the same misinformation in the pages of 2600. In the spring issue of 2600, an invitation to "Summercon" states that: "If you are a criminal, if you are an anarchist, if you are interested in pulling fire alarms or breaking things, don't come to this con; we don't want you here and you wouldn't like us anyhow."

I hereby challenge the organizers of "Summercon" to explain in detail why us anarchists should not feel welcome to your gathering. I would also like you to expand on whether it is only anarchists that should be dissuaded from attending hacker events, or if this should also apply to adherents to other unpopular ideologies; say for instance communists or monarchists. I hope 2600 will provide space for a lengthy reply on these questions, as I am sure it will provide for an entertaining read.

Absinthia Vibrato

We'll print the reply if and when it comes. And we really hope we don't piss off the monarchists.

Notes From The Military

Dear 2600:

First off, I am a member of the US Army. Specifically, a high ranking member. I'd rather not get too specific. I read your magazine for the thoughts/concepts and opinions. I agree that lots of information should be free. We live (and the US military defends) a democracy in which you enjoy your rights.

In response to the Social Engineering article you published: I haven't heard the "go to the Marines or go to jail" line since the 1970's. It's a load. The US military doesn't want people who are in question with the law. It wants bright, forward-thinking people who are motivated to succeed. If you don't want to be a part of the military community, then all you have to possess is the desire to leave. Pick up a copy of the *Army Times* - thousands of soldiers are being eliminated because of drawdowns. Do you think the military wants you if you don't want to be there? Certainly if you start talking about suicide, you're going to get a response. But this whole "social engineering" thing is BS.

Second: There is a stereotype among the hacker community that the military is anti free speech and anti hacker. You would be amazed that the bulk of the military shares your views on "big government" and rights infringement, that "information should be free." On the other hand, no one wants to see federal and military computers invaded or electronically defaced. Whenever I see questions like: "I think this is an Army computer, if anyone can get in please tell me how," it scares the crap out of me. Think about your motivations next time you decide to invade these areas - is it for fun and exploration? Okay - it's still illegal. If your methods work, what's to say someone of unscrupulous motives won't hesitate to do the same thing, out of malice? Yes, it's necessary to bring information to the masses - but at a cost to national security? Next time you want to go muck about fedworld, think about the rights and freedoms the government provides. Is it really worth messing up your life to explore these areas? I'd think not. There are other ways to find truth, to free information, than to invade privacy and security of the US government.

Finally, 2600 is an outstanding publication, and it constantly points out the reason "hackers" seek out new knowledge is not for personal profit, but for general knowledge. Let's keep it that way.

Jungle Bob

Thanks for the kind words. But it's doubtful that the hacker spirit can be trained to only explore computers that are not "federal interest." The bigger the target, the more the challenge. All the threats in the world won't dissuade a determined individual, particularly if that individual has yet to experience a lifetime of media training and fear. The best we can hope for is for hackers to "do the right thing" once they've discovered something. For instance, if a hacker were to find a wide open computer that turned out to belong to a hospital and it contained patient records, we believe the vast majority would contact the hospital to get it fixed and, if that didn't work, alert the media (hopefully avoiding getting held accountable for the flaws by blame-seeking "reporters"). If the military and the government are respected, they can expect to be helped in the same manner. But you folks need to remember that this respect will never be achieved through fear and intimidation, regardless of how many guilty pleas are tallied.

For The Record

Dear 2600:

I think that your magazine kicks ass and I would love to be a part of it. I find it a great source of information as well as entertainment. I was shocked recently when I read a letter in the Spring 97 issue (page 34-35) where someone called themself NeoCzar. I have had that tag for years and have been using it for just as long. Since I am in the process of becoming a well known part of the hacking

continued on page 48

continued from page 13

Your first classification is done by the Region Designator at BOP Regional Headquarters. As a computer hacker you will most likely be placed in a camp or a low FCI. This is assuming you weren't pulling bank jobs on the side. *If* you do wind up in an FCI, you should make it to a camp after six months. This is assuming you behave yourself.

Another thing the Region Designator will do is to place a "Computer No" on your file. This means you will not be allowed to operate a computer at your prison work assignment. In my case I wasn't allowed to be within 10 feet of one. It was explained to me that they didn't even want me to know the types of software they were running. Incidentally, the BOP uses PC/Server based LANs with NetWare 4.1 running on Fiber 10baseT Ethernet connections to Cabletron switches and hubs. PC based gateways reside at every prison. The connection to the IBM mainframe (Sentry) is done through leased lines via Sprintnet's Frame Relay service with 3270 emulation software/hardware resident on the local servers. Sentry resides in Washington, D.C. with SNA type network concentrators at the regional offices. And I picked all of this up without even trying to. Needless to say, BOP computer security is very lax. Many of their publicly available "Program Statements" contain specific information on how to use Sentry and what it's designed to do. They have other networks as well, but this is not a tutorial on how to hack the BOP. I'll save that for if they ever really piss me off. (humor)

Not surprisingly, the BOP is very paranoid about computer hackers. I went out of my way not to be interested in their systems nor to receive computer security related mail. Nevertheless, they tried restricting my mail on numerous occasions. After I filed numerous grievances and had a meeting with the warden, they decided I was probably going to behave myself. My 20 or so magazine subscriptions were permitted to come in - after a special screening. Despite all of that I still had occasional problems, usually when I received something esoteric in nature. It's my understanding, however, that many hackers at other prisons were not as fortunate as I was.

D. Ignorant Inmates

You will meet some of the stupidest people on the planet in prison. I suppose that is why they are there, too dumb to do anything except crime. And for some strange reason these uneducated low class common thieves think they deserve your respect. In fact they will often demand it. These are the same people who condemn everyone who cooperated, while at the same time feel it is fine to break into your house or rob a store at gunpoint. These are the types of inmates you will be incarcerated with, and occasionally these inmates will try to get over on you. They will do this for no reason other than the fact you are an easy mark.

There are a few tricks hackers can use to protect themselves in prison. The key to your success is acting before the problem escalates. It is also important to have someone outside (preferably another hacker) who can do some social engineering for you. The objective is simply to have your problem inmate moved to another institution. I don't want to give away my methods but if staff believes that an inmate is going to cause trouble, or if they believe his life is in danger, they will move him or lock him away in segregation. Social engineered letters (official looking) or phone calls from the right source to the right department will often evoke brisk action. It's also quite simple to make an inmate's life quite miserable. If the BOP has reason to believe that an inmate is an escape risk, a suicide threat, or has pending charges, they will handle them much differently. Tacking these labels on an inmate would be a real nasty trick. I have a saying: "Hackers usually have the last word in arguments." Indeed.

Chances are you won't have many troubles in prison. This especially applies if you go to a camp: mind your own business, and watch your mouth. Nevertheless, I've covered all of this in the event you find yourself caught up in the ignorant behavior of inmates whose lives revolve around prison. And one last piece of advice. Don't make threats. Truly stupid people are too stupid to fear anything, particularly an intelligent man. Just do it.

E. Population

The distribution of blacks, whites, and Hispanics varies from institution to institution. Overall it works out to roughly 30% white, 30% Hispanic, and 30% black. The remaining 10% are various other races. Some joints have a high percentage of blacks and vice versa. I'm not necessarily a prejudiced person, but prisons where blacks are in the majority are a nightmare. Acting loud, disrespectful, and trying to run the place is par for the course.

In terms of crimes, 60% of the Federal inmate population are incarcerated for drug related crimes. The next most common would be bank robbery (usually for quick drug money), then various white collar crimes. The Federal prison population has changed over the years. It used to be a place for the criminal elite. The tough drug laws have changed all of that.

Just to quell the rumors, I'm going to cover the topic of prison rape. Quite simply, in medium and low security level Federal prisons it is unheard of. In the highs it rarely happens. When it does happen, one could argue that the victim was asking for it. I heard an inmate say once, "You can't make no inmate suck cock that don't wanna." Indeed. In my 41 months of incarceration, I never felt in any danger. I would occasionally have inmates that would subtly ask me questions to see where my preferences lie, but once I made it clear that I didn't swing that way I would be left alone. Hell, I got hit on more often when I was hanging out in Hollywood!

On the other hand, state prisons can be a hostile environment for rape and fighting in general. Many of us heard how Bernie S. got beat up over use of the phone. Indeed, I had to get busy a couple of times. Most prison arguments occur over three simple things: the phone, the TV, and money/drugs. If you want to stay out of trouble in a state prison, or Federal for that matter, don't use the phone too long, don't change the channel, and don't get involved in gambling or drugs. As far as rape goes, pick your friends carefully and stick with them. And always, always, be respectful. Even if the guy is a fucking idiot (and most inmates are), say excuse me.

My final piece of prison etiquette advice would be to never take your inmate problems to "the man" (prison staff). Despite the fact that most everyone in prison snitched on their co-defendants at trial, there is no excuse for being a prison rat. The rules are set by the prisoners themselves. If someone steps out of line there will likely be another inmate who will be happy to knock him back. In some prisons inmates are so afraid of being labeled a rat that they refuse to be seen talking alone with a prison staff member. I should close this paragraph by stating that this bit of etiquette is routinely ignored as other inmates will snitch on you for any reason whatsoever. Prison is a strange environment.

F. Doing Time

You can make what you want to out of prison. Some people sit around and do dope all day. Others immerse themselves in a routine of work and exercise. I studied technology and music. Regardless, prisons are no longer a place of rehabilitation. They serve only to punish and conditions are only going to worsen. The effect is that angry, uneducated, and unproductive inmates are being released back into society.

While I was incarcerated in 95/96, the prison band program was still in operation. I played drums for two different prison bands. It really helped pass the time and when I get out I will continue with my career in music. Now the program has been canceled, all because some senator wanted to be seen as being tough on crime. Bills were passed in Congress. The cable TV is gone, pornography mags are no longer permitted, and the weight piles are being removed. All this means is that prisoners will have more spare time on their hands, and so more guards will have to be hired to watch the prisoners. I don't want to get started on this subject. Essentially what I'm saying is make something out of your time. Study, get in to a routine and before you know you'll be going home, and a better person on top of it.

G. Disciplinary Actions

What fun is it if you go to prison and don't get into some mischief? Well, I'm happy to say the only "shots" (violations) I ever received were for having a friend place a call with his three-way calling for me (you can't call everyone collect), and drinking homemade wine. The prison occasionally monitors your phone calls and on the seven or eight hundredth time I made a three-way I got caught. My punishment was ten hours of extra duty (cleaning up). Other punishments for shots include loss of phone use, loss of commissary, loss of visits, and getting thrown in the hole. Shots can also increase your security level and can get you transferred to a higher level institution. If you find yourself having trouble in this area you may want to pick up the book, "How to win prison disciplinary hearings" by Alan Parmelee, (206) 328-2875.

H. Administrative Remedy

If you have a disagreement with the way staff is handling your case (and you will) or another complaint, there is an administrative remedy procedure. First you must try to resolve it informally. Then you can file a form BP-9. The BP-9 goes to the warden. After that you can file a BP-10 which goes to the region. Finally, a BP-11 goes to the National BOP Headquarters (Central Office). The whole procedure is a joke and takes about six months to complete. Delay and conquer is the BOP motto. After you complete the remedy process to no avail, you may file your action in a civil court. In some extreme cases you may take your case directly to the courts without exhausting the remedy process. Again, the *Prisoner's Self-Help Litigation Manual* covers this quite well.

My best advice with this remedy nonsense is to keep your request brief, clear, concise, and only ask for one specific thing per form. Usually if you "got it coming" you will get it. If you don't, or if the BOP can find any reason to deny your request, they will.

For this reason I often took my problems outside the prison from the start. If it was a substantial enough issue I would inform the media, the director of the BOP, all three of my attorneys, my judge, and the ACLU. Often this worked. It always pissed them off. But alas, I'm a man of principle and if you deprive me of my rights I'm going to raise hell. In the past I might have resorted to hacker tactics, like disrupting the BOP's entire communication system bringing it crashing down! But... I'm rehabilitated now. Incidentally, most BOP officials and inmates have no concept of the kind of havoc a hacker can wield on an individual's life. So until some hacker shows the BOP which end is up you will have to accept the fact most everyone you meet in prison will have only nominal respect for you. Deal with it, you're not in cyberspace anymore.

I. Prison Officials

There are two types, dumb and dumber. I've had respect for several but I've never met one that impressed me as being particularly talented in a way other than following orders. Typically you will find staff that are either just doing their job, or staff that are determined to advance their career. The latter take their jobs and themselves way too seriously. They don't get anywhere by being nice to inmates so they are often quite curt. Ex-military and law enforcement wannabes are commonplace. All in all they're a pain in the ass but easy to deal with. Anyone who has ever been down (incarcerated) for awhile knows it's best to keep a low profile. If they don't know you by name you're in good shape.

One of the problems that computer hackers will encounter with prison staff is fear and/or resentment. If you are a pretentious articulate educated white boy like myself you would be wise to act a little stupid. These people don't want to respect you and some of them will hate everything that you stand for. Many dislike all inmates to begin with. And the concept of you someday having a great job and being successful bothers them. It's all a rather bizarre environment where everyone seems to hate their jobs. I guess I've led a sheltered life.

Before I move on, sometimes there will be certain staff members, like your Case Manager, who will have a substantial amount of control over your situation. The best way to deal with the person is to stay out of their way. Be polite, don't file grievances against them, and hope that they will take care of you when it comes time. If this doesn't seem to work, then you need to be a total pain in the ass and ride them with every possible request you can muster. It's especially helpful if you have outside people willing to make calls. Strong media attention will usually, at the very least, make the prison do what they are supposed to do. If you have received a lot of bad press, this could be a disadvantage. If your care continues to be a problem, the prison will transfer you to another facility where you are more likely to get a break. All in all how you choose to deal with staff is often a difficult decision. My advice is that unless you are really getting screwed over or really hate the prison you are in, don't rock the boat.

J. The Hole

Segregation sucks, but chances are you will find yourself there at some point and usually for the most ridiculous of reasons. Sometimes you will wind up there because of what someone else did. The hole is a 6' x 10' concrete room with a steel bed and steel toilet. Your privileges will vary, but at first you get nothing but a shower every couple of days. Naturally they feed you but, it's never enough, and it's often cold. With no snacks you often find yourself quite hungry inbetween meals. There is nothing to do there except read and hopefully some guard has been kind enough to throw you some old novel.

Disciplinary actions will land you in the hole for typically a week or two. In some cases you might get stuck there for a month or three. It depends on the shot and on the Lieutenant that sent you there. Sometimes people never leave the hole.

K. Good Time

You get 54 days per year off of your sentence for good behavior. If anyone tells you that a bill is going to be passed to give 108 days, they are lying. 54 days a year works out to 15% and you have to do something significant to justify getting that taken away. The BOP has come up with the most complicated and ridiculous way to calculate how much good time you have earned. They have a book about three inches thick that discusses how to calculate your exact release date. I studied the book intensely and came to the conclusion that the only purpose it serves is to covertly steal a few days of good time from you. Go figure.

L. Halfway House

All "eligible" inmates are to serve the last 10% of their sentence (not to exceed six months) in a Community Corrections Center (CCC). At the CCC, which is nothing more than a large house in a bad part of town, you are to find a job in the community and spend your evenings and nights at the CCC. You have to give 25% of the gross amount of your check to the CCC to pay for all of your expenses, unless you are a rare Federal prisoner sentenced to serve all of your time at the CCC in which case it is 10%. They will breathalyse and urinanalyse you routinely to make sure you are not having too much fun. If you're a good little hacker you'll get a weekend pass so you can stay out all night. Most CCCs will transfer you to home confinement status after a few weeks. This means you can move into your own place (if they approve it), but still have to be in for the evenings. They check up on you by phone. And no, you are not allowed call forwarding, silly rabbit.

M. Supervised Release

Just when you think the fun is all over, after you are released from prison or the CCC, you will be required to report to a Probation Officer. For the next three to five years you will be on Supervised Release. The government abolished parole, thereby preventing convicts from getting out of prison early. Despite this they still want to keep tabs on you for awhile.

Supervised Release, in my opinion, is nothing more than extended punishment. You are not a free man able to travel and work as you please. All of your activities will have to be presented to your Probation Officer (P.O.). And probation is essentially what Supervised Release is. Your P.O. can violate you for any technical violations and send you back to prison for several months, or over a year. If you have *any* history of drug use you will be required to submit to random (weekly) urinalyses. If you come up dirty it's back to the joint.

As a hacker you may find that your access to work with, or possession of, computer equipment may be restricted. While this may sound pragmatic to the public, in practice it serves no other purpose than to punish and limit a former hacker's ability to support himself. With computers at libraries, copy shops, schools, and virtually everywhere, it's much like restricting someone who used a car to get to and from a bank robbery to not ever drive again. If a hacker is predisposed to hacking he's going to be able to do it with or without restrictions. In reality many hackers don't even need a computer to achieve their goals. As you probably know, a phone and a little social engineering go a long way.

But with any luck you will be assigned a reasonable P.O. and you will stay out of trouble. If you give your P.O. no cause to keep an eye on you, you may find the reins loosening up. You may also be able to have your Supervised Release terminated early by the court. After a year or so, with good cause, and all of your government debts paid, it might be plausible. Hire an attorney, file a motion.

For many convicts Supervised Release is simply too much like being in prison. For those people, it is best to violate and go back to prison for a few months, and hope the judge terminates their Supervised Release. Although the judge may continue your supervision, he/she typically will not.

Part III - Healthy Hacking

A. How to Avoid Detection

Now that you know what kind of trouble you are facing I'll go back to the beginning. If what I've just covered doesn't make you want to stop hacking then you had better learn how to protect yourself. Many hackers feel they have some god given constitutional right to hack. Many don't believe it should be illegal. Well, neurosis and personality disorders work in strange ways. Regardless, I'll cover the topic of stealth. Please note that I in no way advocate or encourage hacking. This technical information is being provided for educational purposes only. And as I mentioned you may feel you have a perfectly legitimate reason for avoiding detection. Simply trying to stay clear of other hackers would be an acceptable reason. This article (I'm sure) will also serve to educate law enforcement officials on the methods currently being deployed by hackers to avoid detection.

Avoiding being identified while hacking is in actuality a rather simple feat, assuming you follow a few basic rules. Unfortunately, very few people bother with them, due typically to arrogance and ego. I have noticed that this seems to be a trait which is a prerequisite to being a successful hacker. I've never met a hacker who didn't think he was the shit. And when it gets right down to it, that was the reason that Mitnick got caught. I'll examine this incident a little later.

I will list here a few of the basic rules I used, and then I'll expound upon them a little later.

- Most important of all, I would never tell another hacker who I was, where I lived, or give out my home phone number. (OK, I screwed up on that one.)
- I didn't set up network access accounts in my real name or use my real address.
- I didn't set up phone numbers in my real name.
- I would never dial directly into anything I was hacking.
- I would set up some kind of notification system that would let me know if someone was trying to figure out where I was connecting from.
- I didn't transmit personal data on systems I had hacked into.
- When I used a network or computer for work or social objectives, I tried to keep it separate from my hacking.
- I never assumed that just by connecting through a bunch of different networks or using cellular phones that I was safe. Even though most cellular networks do not have triangulation equipment installed they still have the ability to narrow a transmitting location down to a square mile of even a few blocks, even well after you have disconnected.
- The minute I got into a system I would examine and edit all of the logs. I would also look for email daemons on admin or admin associated accounts that sent out copies of the system security logs.
- When setting up accounts on systems, I would use different login ID's.
- I never went to hacker cons (until I worked with the FBI).
- I would change network access dial up accounts and dial up numbers every so often. I would also change living locations every 8-12 months.
- I would keep in mind that the numbers I dialed on my phone could eventually be used to track me again. For example, if I called my girlfriend frequently, after I changed numbers and location I might still be calling that number. The telcos now have toll record database software that can cross reference and track this type of thing.
- I rarely used IRC until I worked with the FBI. If you must, change your handle frequently, remain in invisible mode, and if you're leet enough, spoof your IP. Remember that you should never trust other hackers. Many times association with them will cause you as much trouble as a run-in with the Feds.

And yes the FBI logs all of the IRC channels and searches them for key words when they are looking for information on someone or some breech. There is a secret logging program running on a special irc.server that doesn't accept port 6667 connections, etc. Doesn't show up as a link either. Hmm.

Following all of these rules would be tough. The fact of the matter is if you generate enough interest and piss off the right people, they will come after you. However, the FBI routinely passes over low level hackers. When I worked with the Bureau I was instructed that only the most malicious and aggressive hackers were to be investigated. Fine with me, wasn't my goal in life to put a bunch of little hacker dorks in jail. It's not real easy to catch an accomplished hacker but it can be done. It's really just a matter of contacting all of the right people and putting a little time into it. Typically hackers get caught because someone snitched. Thus the importance of my first rule - I never told anyone who I really was. The other primary reason for getting caught is arrogance or underestimating the abilities of the authorities. Poulsen didn't believe an investigator would sit outside of a grocery store for a week on the off chance he might show up. Poulsen had used the

payphones at that store a few times, which was determined by a toll record search. Mitnick didn't think someone would go through the trouble of doing toll searches on cell phone records then radio frequency triangulating his location

Poulsen and I went through some rather elaborate anti-detection procedures. Since I had physical access to my local telco central office I would activate, connect, and wire all of my own phone services. There was essentially no record of my phone number or cable and pair data. In addition, I ran the wires going into my apartment through a trash chute, over the roof covered by tar, and down a vent pipe into my bathroom. The connection to the bridging terminal (F2) was through a hole drilled into the back of the junction box. Examination of the telephone box in the basement of my building revealed no connections - you would have had to take the box apart to see it. And if that wasn't enough, over at the C.O. I tapped onto the output channel (SCI, which was the feed to SCCS) of the 1AESS telephone switch and ran it up to my apartment. There I had an old PC-XT with a Bell 202 modem watching the 1AESS output. Poulsen wrote a small basic program that looked for call traces and any other suspicious activity. The XT would start beeping and print out any of those output messages. Elaborate indeed.

B. The Stealth Box

But a truly good anti-detection system would notify you absolutely if someone was attempting to trace your connection. In addition, it would terminate the connection before it allowed someone to see where it was going. What I am suggesting is some type of dial in/dial out mechanism. For example, two modems connected back to back, with their 232 ports connected. They would then be placed in a generic wall mounted box in an anonymous phone closet somewhere. In addition, a stun gun would be wired to give the modems a death shock if the box was opened by an unauthorized person. A password would be set on the modem for dial out and the phone lines feeding the two modems would have to be set up under separate accounts. This would require anyone investigating to come out and take a gander at this device to determine that it's not the location of the hacker, and that yet another call trace is in order to see who is dialing in. However, having opened the box the investigator has disabled the device and when you dial in you'll know that something is up. Even if they attempt to replace the device, they could never know the original password, or even if there was one. It would be further advisable to disguise the telephone lines feeding the device, making it necessary to open the box to identify them.

Well, that's just an idea for the design of an anti-detection device. It's obviously a bit complex, but you get the idea. My point is that avoiding detection is not a simple task. If someone wants you they can get you. There really isn't such a thing as a secure connection; virtually everything can be traced, short of a highly directional data burst satellite uplink. At that point the Air Force National Reconnaissance Office (NRO) or the NSA would have to get involved. Big bucks.

Aside from setting up physical hardware another idea would be to find a sysadmin who will let you use his system to connect through. If you trust him to tell you if there has been an inquiry regarding your connection, then you might be OK. It would also be wise to set up background processes that monitor finger and other related probes of your account. Watch them watch you.

As I mentioned earlier, if you fall under surveillance there will be two-way radio traffic in your vicinity. Using the OptoElectronics Explorer will detect this and you can further investigate to see who it may be. Good physical surveillance is difficult to detect. Bad physical surveillance is comical.

C. More Protection

I covered encryption earlier and as I mentioned it really is not safe to assume that it will protect you from someone who takes possession of your computer. The only truly safe encryption would be a military spec hardware/software implementation. When people talk about secure encryption they are not taking into account that all the power of a government might be trying to crack it, and that they will have physical access to the encryption device: your computer! This leaves us with one other method: destroying the data. Now this in and of itself can be construed as obstruction of justice. However, should you feel the need to instantly destroy all of the data on your hard drive, for oh... let's say educational purposes, I would suggest mounting a bulk magnetic tape eraser next to your hard drive. You can pick one up at Radio Hack, err Shack. One flip of the panic switch, thus powering up the eraser while the drive is turning, and zap! Mount a switch next to your bed.

This may or may not destroy all of the data on your drive. If the drive disk is removed and placed on a special reader some data may still be recovered. This is a science in itself. DOD spec requires that a hard drive be written to with O's 7 times before it is considered erased. Simply erasing a file, formatting, or defragging will not suffice. Look for a shareware utility named "BCwipe". This will erase to military spec. You may also want to install some type of program that auto erases under certain conditions. Regardless, computer specialists who work with computer crime are trained to look for this.

There are still a lot of issues that could be covered with respect to avoiding detection and keeping clear of hackers. In fact I could fill a book, and in retrospect I probably should have. But I told a lot of people I would write this article and make it public. I hope you found it of some assistance.

Closure

What a long strange trip it's been. I have a great deal of mixed emotions about my whole ordeal. I can however, say that I *have* benefitted from my incarceration. However, it certainly was not because of how I was handled by the government. No, despite their efforts to kick me when I was down, use me, turn their backs after I had assisted them, and, in general, just violate my rights, I was still able to emerge better educated than when I went in. But frankly, my release from prison was just in the nick of time. The long-term effects of incarceration and stress were creeping up on me, and I could see prison conditions were worsening. It's hard to express the poignancy of the situation but the majority of those incarcerated feel that if drastic changes are not made America is due for some serious turmoil, perhaps even a civil war. Yes, the criminal justice system is that screwed up. The nation's thirst for vengeance on criminals is leading us into a vicious feedback loop of crime and punishment, and once again crime. Quite simply, the system is not working. My purpose in writing this article was not to send any kind of message. I'm not telling you how not to get caught and I'm not telling you to stop hacking. I wrote this simply because I feel like I owe it to whoever might get use of it. For some strange reason I am oddly compelled to tell you what happened to me. Perhaps this is some kind of therapy, perhaps it's just my ego, perhaps I just want to help some poor 18 year old hacker who really doesn't know what he is getting himself into. Whatever the reason, I just sat down one day and started writing.

If there is a central theme to this article it would be how ugly your world can become. Once you get grabbed by the law, sucked into their vacuum, and they shine the spotlight on you, there will be little you can do to protect yourself. The vultures and predators will try to pick what they can off of you. It's open season for the U.S. Attorneys, your attorney, other inmates, and prison officials. You become fair game. Defending yourself from all of these forces will require all of your wits, all of your resources, and occasionally your fists.

Furthering the humiliation, the press, as a general rule, will not be concerned with presenting the truth. They will print what suits them and often omit many relevant facts. If you have read any of the five books I am covered in you will no doubt have a rather jaded opinion of me. Let me assure you that if you met me today you would quickly see that I am quite likable and not the villain many (especially Jon Littman) have made me out to be. You may not agree with how I lived my life, but you wouldn't have any trouble understanding why I chose to live it that way. Granted, I've made my mistakes - growing up has been a long road for me. Nevertheless, I have no shortage of good friends. Friends that I am immensely loyal to. But if you believed everything you read, you'd have the impression that Mitnick is a vindictive loser, Poulsen a furtive stalker, and I a two-faced rat. All of these assessments would be incorrect.

So much for first impressions. I just hope I was able to enlighten you and in some way to help you make the right choice. Whether it's protecting yourself from what could be a traumatic life altering experience, or compelling you to focus your computer skills on other avenues, it's important for you to know the program, the language, and the rules.

See you in the movies.

Special thanks to Netta Gilboa and Evian S. Sim.

continued from page 39

community, I would greatly appreciate if you would no longer allow articles or letters to be published unless they arrive from one of the addresses below. If this is too much of a hassle I understand, but it would be *greatly* appreciated.

The "REAL" NeoCzar

You've just gotten a lot more well known.

Meeting Problems

Dear *2600*:

First I want to say that it was your excellent mag that got me into the scene and for that many thanks. Now I wanted to share something that happened at our most recent *2600* meeting that was at the least unusual. At our meetings we usually get at least one new face a month and we always welcome the new talent. This month we got three who stayed and were fine. Another, however, showed up in a suspicious manner and left very shortly afterwards. He came to the middle of the group and started asking if this was the meeting and what we were doing and if anything was happening that night. No name or handle given, just way too many questions. We all were very calm and responded with no real info other than yes this is the meeting. He left for about ten minutes and then returned very pissed off and cussing at us and saying things like "I would have never expected that from this group." He obviously felt discriminated against or something. At any rate, he left again and did not return. The main thing that comes to mind now is that I am surprised that someone would come to a meeting of this nature and not realize that some tact and discretion are in order as far as introductions are concerned. In fact, when most of the people show for the first time they tend to hang out and watch from a distance, then work their way in and talk to people one at a time until they are at least familiar with and to the group. I just thought this might be a good thing to read for people who have not yet gone to a meeting but are considering it. As far as the discrimination goes, we don't at all. In fact one of the newbies who showed was 13 and dragging his mother with him, not a problem at all. We are lucky to have the wide variety of people in our group that we have and we definitely benefit from the unique talents of each.

CW Extreme

Not everyone knows the "proper" way of joining a new group. Your rules don't necessarily apply to others. People can be very sensitive in this situation, especially if they're already somewhat insecure. But these can wind up being the smartest people in the group. Unless someone is abrasive and obnoxious, it's worth it to go the extra length to see that they're comfortable the first time they show up. It's good that this situation got you to think about this.

Dear *2600*:

I have recently become interested in learning all about hacking and the like. I found that there was a meeting listed in my area and I anticipated it greatly. I thought for sure that there would be people there to meet and that I might be able to find more information and maybe make a new friend or two.

At the meeting I saw only one "group" of people and couldn't be sure so I sat and waited for another possible gathering so as not to disturb just anybody. I eventually concluded that this was the only "group" and decided to just ask them if they were *2600*. I have to say that this was the last group of people I expected to be a superficial, stereotypical, prejudiced bunch of elitist fucks. But that is exactly what they showed themselves to be. I was very uncomfortable and walked away after they refused to look me in the face while spouting some bizarre rhetoric about being from another nebula and not taking calls at this time. But after walking a hundred feet or so I turned around and told them, one of them specifically, exactly what I said above. At this point I was offered a chair. All I could say was "You have got to be fucking kidding me" and walked away.

Sorry to take so long to get to the point. But since you advertise the meetings on your website and hold them in public places I just assumed that anybody was welcome. I felt that since these people are representing what it is you are all about, that you should know how they receive newcomers who are interested in the same thing.

Unfortunately this particular group is filled with "untouchables" as I did not show up in the required uniform of Marilyn Manson t shirts, fucked up hair, and a skateboard. Some people have to move on after high school and I guess I was a casualty of Big Brother and his working class machine.

Flipsquid

It seems likely that you are the very same person referenced in the previous letter. So read what we said to the other person and apply it to yourself. You should never be judged on first impressions which, unfortunately, both of you did. We hope you give it another try.

Dear *2600*:

This is a message to everyone who attends the New York City *2600* meetings: I've learned recently from a friend who did an article a while ago on us for a magazine called *Computer Sweden*, that the FBI watches us quite a bit more than most of you may think. Apparently he interviewed Tim Foley (I think he's the head of the Computer Crime Division). Mr. Foley informed the reporter that the FBI has a room on the seventh floor of the Citicorp building. From a window on the inside (overlooking the large open courtyard in the middle of the building), they have an office that they watch us from.

Keep in mind that I have no way of verifying this information; just something to think about.

PS. HOPE kicked ass!

Checkmate

We always operate under the assumption that we're being watched. It's kind of foolish to go to so much trouble to spy on people who are meeting in an open space.

Beyond Hope Aftermath

Dear *2600*:

I have just left the Puck Building in New York City, site of the Beyond Hope computer enthusiast conference. The con was well organized and of excellent quality. The Puck building was classic, interesting, and, most importantly, big enough to comfortably hold everybody. I was impressed with both the large conference room and the hack room. The conference room was big enough to hold everyone, and the sound and video were excellent. I appreciated the live video on the screen behind the panelists. It allowed everyone to see who was speaking from even the farthest corner of the room. The audio link to a telephone was awesome, as well as the demonstrations this link allowed. K-mart never had a chance! The transfer to the shoe department was a special touch. (OK, you had nothing to do with this, but I liked it so I will attribute it to you as the prank enabler.) The hack room had enough tables, chairs, and power outlets, and food for everyone.

The best feature of the con was the bandwidth to the Internet. I was expecting T1 speeds, but this seemed even faster. I heard rumors that we were using more than just T1 bandwidth, but whatever it was, it rocked. I found it extraordinary how fast I could download and how responsive the WWW was. I was able to try a bunch of technologies that frankly don't work very well at 28.8Kbps. It was great to envision what our future will be like when this bandwidth capability will be in every home in the world. The only problem I saw with the network was that on Saturday the beyond hope net box did not want to stay up. Special thanks to the DHP guys for the public terminals, both graphical and ASCII. It looked to me that they were constantly used though the whole con. A great source of information for those who were not able to, or chose not to bring computers.

I loved the baggage check areas as well as the convenience of having food on-site. It would have been nice to have accommodations on-site as well, but in retrospect I didn't see many people complaining.

Because of the Beyond Hope conference I was able to experience what it is like to speak with equals, people who have an understanding of the technology, and who hold similar views on how it can change the world. It was so nice not having to preface every communication with a short course in TCP/IP or UNIX technology. It is for this experience I thank you and everyone who was a part of this conference.

mattj

Your experience was echoed by many, both technical and non-technical. Thanks for being there. We like to think the Hope conferences show the true hacker spirit in action.

Dear *2600*:

The Hope conference at the Puck building was great! When will your guide to the area around the Puck building be finished on the Hope page?

D.

Oh be quiet.

IRC Woe

Dear *2600*:

I tried to get on #2600 on EFNET the other day and was slammed with an error. "Channel is invite only". Invite only??? That's when I began to think. Why would a hacker channel, a channel that is created for the free exchange of information, be invite only? This isn't the first time this has happened to me and I want to know why. Hacking should not be exclusive to those who have alot of friends on IRC.

havok

It's just the nature of IRC for idiots to somehow gain control and lock everyone else out. Any channel that closes itself off from unknowns has no hope of knowledge advancement. So if you find yourself locked out of #2600, go to #2601 until #2600 is liberated. If that one gets taken over, keep going up. Free speech will always prevail.

USA Still #1

Dear *2600*:

In your *Summer 97* issue you stated on the "News Items" page the story about the German Compuserve chief being charged for distributing child pornography and violent computer games and complained about Germany being even worse than the U.S. in treating free speech. As a German exchange student living in the U.S. for a year I totally have to disagree for various reasons:

1. When the charge was presented, there was a huge cryout which went through all of Germany, and many more left-oriented politicians in Parliament complained about restrictive laws letting Germany fall way behind other countries. Experts claim that the charge was a mistake and has no chance of succeeding. This charge is an insult for every democracy.

2. You stated, too, that you're punished for distributing violent games in Germany. You took Quake as an example. This is simply not correct. Too violent games are restricted in a way hardcore porn is here in the U.S.; only minors can't access them.

3. We don't have an SS-like organization like the Secret Service.

4. Something like being sentenced not to use computers anymore would in no way be possible in Germany, and it seems to be quite legal here. I'm not trying to say that Germany is free-man's paradise, but it is in no way treating free speech worse than the U.S.

elw00d

Gee Whiz

Dear *2600*:

Well, I use AOL and am in a warez group called kryp-. My leader and I found out a nifty way to get free calls using 1-800 COLLECT. Here's how to do it: Okay, at a toll phone, dial 10, 222, 0, and then the area code, and then the number. It will ask for your CC#, punch [real credit card number omitted]. It will ask for the expiration date, and that's when you punch in 298. Finally, it will ask for the zip code: you dial 00000 (5 zeros). "Thank you for using 1-800-COLLECT!"

Does this qualify me for a free subscription, and a teeshirt, and all the other cool crap??

Adam768L and Da Violator

You qualify for the Fool of the Month, that's for certain. How you ever got the idea that credit card fraud has anything to do with hacking or requires any brain power whatsoever is beyond us. We could dismiss you as just another AOL lamer but the truth is that AOL didn't make you into this. And only you can make you into something better. Please get to work.

Singapore Connection

Dear 2600:

I'm a 17 year old male teenage hacker apprentice from Singapore who is a great fan of your magazine. I just downloaded the Real Audio file from your website. That was the show from the Beyond Hope conference you held on August 9th, 1997 which is of course the National Day of my stooopid country Singapore. Yeah, Emmanuel Goldstein was right - you can't chew gum, you can't litter, you can't vandalize, technology reigns supreme, and we are ruled by some boneheaded square conservatives. (So what's new?) Anyway, I found it real funny that you guys wanted to use my country's national colors. I find it real cool that you guys tried to make the Empire State Building light up blue and white. Did it turn out successful in the end?

Anyway, you guys in NYC are trying to hack the Metrocard, right? Well, Singapore also has their own version of this. We call it the Transitlink card. This card can be used on the MRT (Singaporean version of the subway) and on the bus. It works like this. First, you have to go to this ticketing booth to buy this card. Then you have to choose how much you want to put into that card. This ranges from $5 to $50. There are three flavors to choose from: child, adult, or senior. When the credit runs out, you go back to this place to top it up again. You can also use your ATM card and top it up using this machine they have and you can also have this cool GIRO card. This card basically deducts a certain amount from your bank account and tops the card up whenever your card runs low on credit. However, you have to take the subway for this to work; it doesn't work on buses. So firstly, when you go to the MRT station, you will see this big metal box with two red colored plastic gates. You insert your Transitlink card into the slot. Some amount is deducted from your card and the remaining value is shown on a display on top of the box. Real Simple. I have seen a Supervisor card however that only the people at Transitlink have. It basically gives you unlimited access to the system and can be used for a couple of functions.

Joe a.k.a. DaemonX

We attempted to light up the Empire State Building with the official Hope colors of blue and white but were told that this could only be done for national holidays. So we discovered that Singapore's national holiday was right smack in the middle of our conference. Trouble was their official colors were red and white. We were stuck until we realized that we too could become revisionists. So we simply changed Singapore's history a bit to make their official colors blue and white and created the Singapore Cultural Center, complete with a phone book listing. But in the end, the Empire State people said that technical problems wouldn't permit them to make the change. It was a valiant effort.

Free Video Games

Dear 2600:

I really enjoy the open forum of information that you present in 2600. To continue a discussion from Vol. 14 #2 on standalone commercial video games, in the distant past (say, about 1976 +/-) some fellow science and engineering undergrads found that the residence hall's Atari Tank coin-op could be activated via static discharge. Inadvertently someone shuffled up to it one day, quarter in hand, and the cheap carpet's static buildup started the game. Careful scientific investigation revealed that the most effective way was to jump in the air before touching the joystick's metal ring around the fire button. This was basically like inserting a quarter.

The machine was moved off of the carpet, presumably by the service tech who may have found that the counter (if any was kept electronically) didn't match the coin box. However, if one leapt from the carpet area across the five feet of tile and managed to discharge into the correct spot, it would still work.

I have occasionally tried this trick on games since then, but either the carpet was not effective or the game's external pieces are adequately buffered.

A mention was made of a "gun" which could activate some games. The Zerostat gun, made by Discwasher, was intended for the reduction of static charges on vinyl record albums, and also has some uses in the electronics and microscopy industries. Its trigger emits a small stream of ions, charged one way on pull and the other way on release. This might provide enough charge to trigger a logic state change in some electronics, and might also be capable of destroying some static sensitive components.

PaulT

The thought of all these college students flying through the air towards the video game of their choice is truly awe-inspiring.

Clarification

Dear 2600:

On the back cover of the new issue, are you sure that the payphone that says "Georgia" isn't Soviet Georgia? Cuz the writing above it doesn't seem to be English. And that style payphone was never a Western Electric brand... Look closer...

Ether Bunny

Well gee. We were certain they used Cyrillic letters in the Deep South. We'll investigate further.

Dear 2600:

My copy of your Summer issue arrived a few days ago and I am rather disgusted with VaxBuster's article on "Fast Food Phun." First, it was unresearched and the only real information he managed to give were the frequencies broadcasted on. Second, I would like to know what type of person would actually waste his time modifying a ham radio so they can mess up fast food orders. The people who work in fast food have a hard enough time without some childish junior high student fucking up orders and causing more customer complaints.

TheRich

You didn't really point out any information that was wrong. As for mischief, we find that it often provides that little interruption in the daily mundane lives of drones which almost makes living worthwhile. Plus, laughing your head off can be very therapeutic for the rest of us.

PCS Mystery

Dear 2600:

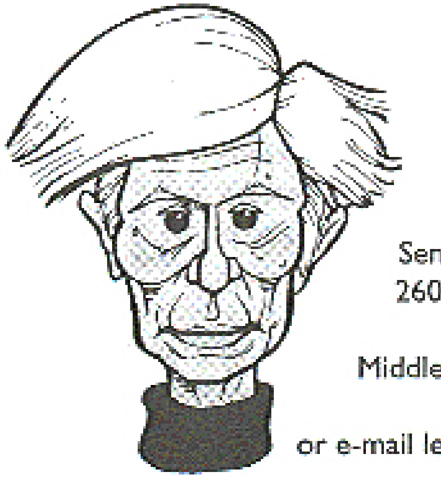
I am a recent subscriber to AT&T's digital PCS system using a Nokia phone. I have been experiencing the strangest occurrence and wondered if anyone at your organization has had similar experiences. My account has been set up to receive alpha and numeric paging. On weekends, I receive several pages with seemingly random four digit numbers. I know that who or whatever is sending the data is not dialing my cell number because my phone doesn't ring. This means that data is being sent via the web or perhaps a telephone number set up to send numeric only pages. I think the weirdest part of this is that it only occurs on weekends and that the data is always a four digit code. I called AT&T and asked them if they could explain it or had any other people reporting similar problems and of course they told me that I was the first and that probably someone was just fooling around. Any ideas of what could be going on here?

Matt D.

Barring the possibility that someone is indeed messing around who only has time to do this on the weekends, it's possible that this is some sort of an automated process that's malfunctioning. You should keep notes of exactly when each instance occurs and what gets sent and then compare them. AT&T should be able to tell you how the page was sent and maybe even from where.

☎

Everyone gets to be famous for fifteen minutes. Now is your chance.



Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, New York
11953-0099
or e-mail letters@2600.com

Marketplace

☎ ☎ ☎ ☎ ☎ ☎ For Sale ☎ ☎ ☎ ☎ ☎ ☎

UNDETECTABLE VIRUSES. Offering six viruses/viri which can automatically knock down DOS and Windows (3.1) operating systems at the victim's command to open Windows. Easily loaded, recurrently destructive and undetectable via all virus detection and cleansing programs with which I am familiar. Well-tested, relatively simple and designed with stealth and victim behavior in mind. Well written instructions, documentation, and antidote programs are included. $5.00 even - TOTAL! Cash, money orders, and checks accepted. Sorry, no foreign orders. Provided on seven 1.44 MB, 3.5" floppy disks which can be freely copied. They make great gifts! Orders are promptly mailed out "priority" (USPO). Satisfaction guaranteed or you have a bad attitude! The Omega Man, 8102 Furness Cove, Austin, TX 78753, omegaman4@juno.com

2600 POSTERS! 2600 van crashing into NYNEX payphone from the Winter 95-96 cover. 20" x 30". Quality coated stock. Shipped in tube. $15. Send money order (no checks) payable to Kiratoy Inc., c/o Shawn West, PO Box 86, New York, NY 10272. Allow 4-6 weeks for delivery. Visit www.kiratoy.com/poster for more info.

ATTENTION PHREAKERS AND HACKERS. For a catalog of plans, kits, and assembled electronic "tools" including the red box, radar jammer, surveillance, ATM & slot machine manipulators, cable descramblers, and many other hard-to-find equipment at low prices, send $1.00 to M. Smith-03, 1616 Shipyard Blvd., Suite #257, Wilmington, N.C. 28412 or check out my web page at www.hackershomepage.com.

TWO NEW DSS SMART CARD DEVICES. 1) Smart card emulator computer interface. 2) Smart card programmer (works with new generation access cards). These devices are the same ones used in the satellite, banking, and medical industries and the ISO7816 standards. Software and any updates are available on the Internet. Send for new brochure - you won't be disappointed! Also, cable TV converters for all systems. Send me the brand and model number of the converter used in your system. Ray Burgess, PO Box 99865086, Pontiac, IL 61764-0099.

TOP SECRET CONSUMERTRONICS, exciting hacking, phreaking, and weird products since 1971. Go to www.tsc-global.com or send $3 for catalog to: Box 23097, ABQ, NM 87192.

6.5536 MHZ CRYSTALS available in these quantities ONLY: 5 for $20, 10 for only $35, 25 for $75, 50 for $125, 100 for $220, 200 for only $400 ($2 each). Crystals are POSTPAID. All orders from outside U.S. add $12 per order in U.S. funds. For larger quantities, include phone number and needs. E. Newman, 215-40 23rd Road, Bayside, NY 11360.

DISAPPEARING INK FORMULAS! Safely write the ultimate love letter or nasty note. Great gag item. Signed documents and memos will completely and undetectably disappear in 1 day to 4 weeks depending on formula used. $5 postpaid. Pete Haas, PO Box 702, Kent, Ohio 44240-0013

TAP BACK ISSUES, complete set Vol. 1-91 of QUALITY copies from originals. Includes schematics and indexes. $100 postpaid via UPS or first class mail. Copy of 1971 *Esquire* article "The Secrets of the Little Blue Box" $5 & large SASE w/52 cents of stamps. Pete G., PO Box 463, Mt. Laurel, NJ 08054. We are the original!

INFORMATION IS POWER! Our catalog is available with informational manuals, programs, files, books, and video. Get the information from the experts in hacking, phreaking, cracking, electronics, viruses, anarchy techniques, and the internet here. Legit and recognized world-wide, our information will elevate you to a higher plane of consciousness. Join today! Send $1 for our catalog to: SotMESC, Box 573, Long Beach, MS 39560.

CAP'N CRUNCH WHISTLES. Brand new, only a few left. THE ORIGINAL WHISTLE in mint condition, never used. Join the elite few who own this treasure! Once they are gone, that is it - there are no more! Keychain hole for keyring. Identify yourself at meetings, etc. as a 2600 member by dangling your keychain and saying nothing. Cover one hole and get exactly 2600 hz, cover the other hole and get another frequency. Use both holes to call your dog or dolphin. Also, ideal for telephone remote control devices. Price includes mailing. $99.95. Not only a collector's item but a VERY USEFUL device to carry at all times. Cash or money order only. Mail to: WHISTLE, P.O. Box 11562-ST, Clt, Missouri 63105

☎ ☎ ☎ ☎ ☎ Help Wanted ☎ ☎ ☎ ☎ ☎

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

HELP! I need someone with more brains than I have. Credit record needs serious surgery. Smith, 3167 San Mateo NE, Ste. 101, Albuquerque, NM 87110.

I WILL PAY TOP DOLLAR FOR A NEW IDENTITY. Birth, social, and driver's license, any state. Not looking for "altered" documents, need ones that will pass law enforcement/government scrutiny. Call me now, name your price! Leave private message. Mark, (714) 354-3771

☎ ☎ ☎ ☎ ☎ ☎ Services ☎ ☎ ☎ ☎ ☎

HELP WITH CREDIT. How to get a clean credit data. 280 Union Ave., Apt. 10, Irvington, NJ 07111.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Jr., Attorney at Law, at (334) 265-6602 or cyberlaw@mont.mindspring.com. Extensive computer and legal background.

☎ ☎ ☎ ☎ ☎ ☎ Personal ☎ ☎ ☎ ☎ ☎ ☎

BOYCOTT BRAZIL. Please review my web sites and help me inform the WORLD as to my torture, denial of due process, and forced brain implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, P.O. Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct.

DESPERATELY SEEKING OTHER HACKER/PHREAK in Binghamton, NY area. Please write me at Matt Westfall, 138 Clifton Blvd., Binghamton, NY 13903.

I AM 28, degreed, and presently paying for the mistake of wasting my intelligence. I am looking for anyone who is creative, intelligent, sincere, and truly with a finger on the pulse of the world of true cyberpunk/technopunk culture to share correspondence with. Please respond to: Emilie A. Ramsey, P.O. Box Y-170678, Victoria, VA 23974.

IF YOU KNOW OF ANY UNDERGROUND BBS'S or elite hacking groups in Tampa, FL please contact me ASAP. Send mail to: GRECO, 2001 Riverside Dr., Gainesville, GA 30501-1227.

☎ ☎ ☎ ☎ Bulletin Boards ☎ ☎ ☎ ☎

ANARCHY ONLINE. A computer bulletin board resource for anarchists, survivalists, adventurers, investigators, researchers, computer hackers, and phone phreaks. Scheduled hacker chat meetings. Encrypted e-mail/file exchange. WWW - http://anarchy-online.com. Telnet: anarchy-online.com. Modem: (214) 289-8328.

FLUID BBS is a bulletin board system created for conversation. One line. Call and post messages, download QWK packets, etc. No files, no doors (olg's) and no stupid renegade mods. A simple board that you call up to talk to each other and log off. HPAVC related, somewhat. (303) 460-9632.

MONTREAL'S H/P BBS and home of Hackknowledge zine. Last Territory (514) 565-9754.

THE DEF CON VOICE BBS SYSTEM (801) 855-3326 will be moving! The new location will feature NO phantom voice bridges, just 24 lines, and the same Voice BBS, VMBs, and voice bridge structure. When the change happens the old number will refer you to the new one.

THE ANSWER IS NO! You CANNOT take out a classified ad in 2600 if you don't subscribe! You cannot pay us any amount of money to advertise either here or elsewhere in the magazine. So please don't ask - you probably won't even get a reply. If you do subscribe, you are entitled to a free ad in the Marketplace as space and standards permit. Send your ad to: 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Winter Issue: 12/31/97.

The payphone ripoff continues with the blessing of the Federal Communications Commission. It's expected that payphone rates will soar thanks to the new FCC ruling which deregulates them. In logic that we cannot grasp, the FCC ruled that long distance companies must immediately give payphone companies 28.4 cents for every call to an 800 number, as well as calling card and 950 calls. This stupidity will result in all kinds of surcharges for basic services as well as increased rates for local and long distance payphone calls. Some companies, such as Sprint, plan on blocking certain 800 calls from payphones. It's a known fact that greed tends to screw up telecommunications. It's a real shame to see the FCC help it along.

Greed was apparently the motivation behind Sprint's recent rate change (it predated the FCC action). They had been offering a 25 cents a minute phone card with no surcharge. After snagging a bunch of customers who were fed up with paying extra surcharges for making a simple phone call, they quietly changed their pricing to 30 cents a minute *and* and a 30 cent surcharge per call! They'll probably be about as quiet when it comes to telling everyone how many customers they wound up losing.

It shouldn't come as a surprise to anyone wanting to put up a controversial web page that America Online is not the place to do it. Serial killers may no longer put up pages according to AOL spokeswoman Tricia Primrose, nor will any user be allowed to link to such pages. "We believe in a person's right to speak," she explains, "but we don't believe individuals have a right to force us to associate with that speech."

Wandering around on www.govtech.net you can really get a sense as to how the other side thinks. Check out these excerpts from *Computer Evidence Processing* by Michael R. Anderson. This document is a how-to for law enforcement involved in raiding houses and seizing computers. One section is entitled "Assume That Every Computer Has Been Rigged To Destroy Evidence." Raiders are advised not to operate a suspect's computer until a full backup is made. "Normal computer backups won't do - a full bit stream backup is necessary." Also, it's advised that everything always be taken since vital evidence may be tied to "special" hardware. "Encrypted files can cause you serious grief, and finding a password scrawled on a desk or on a calendar can help make your case." In the case of actually turning off the system when seizing it, all kinds of concerns are raised. "To preserve the image on the screen, a quick photograph of the screen display may be appropriate. Then a decision has to be made as to whether or not the computer will be unplugged from the wall or shut down systematically based on the requirements of the operating system.... Usually, networked computers should be shut down following normal shutdown procedures as dictated by the operating system involved. Usually, stand-alone computers can be unplugged as long as background processes are not active, e.g. disk defragmentation." Probably the most fascinating part of this document is the concern over destroying evidence. Investigators are warned not to run any programs on the computer since temporary files could be created that could overwrite evidence. Even using the keyboard can be dangerous since "one wrong press of a key can trigger destructive memory resident programs that may have been planted on the computer." It is suggested that pictures be taken of the exact configuration of the computer system from all different angles, wires clearly marked so they get plugged back into the right places, and the computer clearly marked as evidence so other employees don't screw the whole thing up by playing around with it. Apparently that's been a problem. "A destructive process can be initiated in a heartbeat and the results can be disastrous," the document warns. "Consider using a subterfuge to remove the operator from the computer to eliminate the possibility of them destroying potential evidence. Raid planning is very important, and this is especially true if the probability of destructive processes exist. Watch out for 'burn boxes' at the raid site which might be rigged to incinerate floppy diskettes and zip disks." Now *there's* a cool thing to pick up at CompUSA. Finally, a couple of handy tips for those law enforcement people determined to screw up: "Avoid storing the computer components near the police car radio. The magnetic field created by the operating radio may be strong enough to destroy evidence. A word to the wise - don't transport the seized computer in the trunk on top of the radio transmitter."

Get ready for more confusion. The new seven digit carrier access codes we've been warning you about are set to become mandatory in January. 10XXX becomes 101XXXX (initially 1010XXX). This oughta be fun.

As reported in our last issue, one has to be careful when calling Omnipoint GSM phone exchanges since *67 is ignored on all calls that go to voicemail. As reported in an article in this issue, this is not because of ANI but Caller ID. So how can you protect yourself? For starters, here is a current list of Omnipoint exchanges throughout the country - calling them could reveal your number even if you've blocked it: 201-349, 201-486, 201-757, 201-873, 215-715, 215-820, 215-939, 302-898, 316-990, 516-312, 609-334, 609-505, 609-510, 610-202, 610-203, 610-504, 717-604, 908-338, 914-316, 914-320, 917-251, 917-257, 917-770, 917-774, 917-815, 917-915, and 917-945. But this info is pretty useless if someone forwards a regular phone line to one of these exchanges. There is no way you would ever know you were going to an Omnipoint exchange in that case. One possible protection is to recognize the voice mail system that Omnipoint uses. Here are some distinguishing characteristics: if you don't speak after the beep, the recording will say "Your message is too short." Hitting 1 during the outgoing message will allow you to send a numeric page, 2 a text page through an operator, 3 will send a "callback number," 7 will say "Please begin recording at the tone," 8 will allow you to send a fax, and 0 will either transfer you to a referral extension or get an Omnipoint recording. Hitting * allows you to enter a password, hitting # skips the outgoing message. (All new Omnipoint accounts have no password initially. The voice mail system itself can be accessed at XXX-XXX-MAIL in all Omnipoint exchanges.) We've also noticed that dialing *67 or *82 before dialing one of the MAIL numbers *within* the same state always gets you a reorder as if those commands were somehow confusing the Omnipoint switch. If this is somehow related to the capturing of Caller ID, it's possible that blocked calls are only captured if they come from the same state.

Sprint PCS uses CDMA technology as opposed to GSM. We don't have a whole lot of info on them right now but we do know that they aren't capturing blocked numbers. We also know that they too use the MAIL suffix on their voicemail system and that the default password that many subscribers don't change is, you guessed it, SPRINT. Two of their exchanges are 917-701 and 917-805.

There's a fair amount of 2600-related mischief in the air recently. Pager traffic from none other than the White House was leaked to us and, in response to draconian laws and proposals to make listening to certain frequencies illegal, we decided to release this to the mainstream media. The purpose was to demonstrate how absurd and unenforceable such laws are. The real way to protect privacy is through encryption, something law enforcement wants kept quiet since they would still be allowed to listen to the "illegal" frequenci s to gather information easily. It's time we started fighting back.

Some other anonymous sort went and changed a sign in the subway to read like our one of our covers. According to the Associated Press, "electronic signs telling subway riders to 'Watch Your Step' and 'Have a Great Day' were flashing the message 'The Hacker Quarterly' and 'Volume Fourteen, Number Three' instead" during a recent morning rush hour. Apparently word is getting out that we're short on cover ideas....

And add to this the various mischief caused by Beyond Hope. Just ask the Empire State Building, Singapore, and K-Mart for starters. And, of course, there were those Beyond Hope stickers that looked just like the NYNEX signs on payphones. We're told that was the final straw that made Bell Atlantic decide to take over NYNEX. That's unconfirmed.

SECRETS OF WAL-MART

by Pirho

Have you ever walked into a store like Caldor or Target and seen one of the employees on the phone? Ever wonder what it would be like to phreak the phone system in one of those stores? Well, wonder no further. In this article I will attempt to explain to you how the phones at your local Wal-Mart work and hope to answer any questions that you might have.

First off, it's important to know the type of phone that you'll be dealing with. Most Wal-Mart's use a Lucent Technologies or AT&T model MLX-100 or 8102. For those of you who might happen to see a Bell Labs phone, don't panic. Bell Labs is the same as Lucent.

Let's start with the AT&T 8102. This is your standard non-display type phone with a series of 10 buttons arranged in pairs of two's. These are your programmable buttons. They usually contain three outside lines, and the rest are usually just different departments, or if you're really lucky one of them is for the paging system. (I'll explain more about that in a minute.)

The three lines that are for outside calls on these phones are for incoming only. Most of them have a block on the lines that won't allow you to get an outside dial tone but will allow you to pick up an outside call. But you can dial 911 just by picking up and hitting 9 for a dial tone, then 911.

The next set of buttons you'll see are three in a straight line. These are your flash, redial, and hold. Keep in mind that the flash button does not give you enough time to truly flash the receiver, so almost always this has to be done manually.

After your hold button row is a normal numeric touch tone pad for you to dial the different extensions on. All the extensions in every Wal-Mart are the same no matter where you go, some of which are as follows:

105: electronics.
123: men's.
129: fitting room.
150: front courtesy desk.
181: layaway.
0: Operator.

Which brings me to my next point. The Operator. She is located in the ladies fitting room; she has the best phone in the whole store, so if you want to phreak the system you have to get through her.

Inter-store communication is possible simply by picking up any house phone and dialing one of the following numbers:

9-1-700-701-xxxx
9-1-700-707-xxxx

xxxx stands for the store's number that you are calling. This is the number of the store in the order of when it was built, not the phone number. Example: store 2046 was built before store 2155 so if you wanted to call store 2155 then xxxx would be 2155. (Get it?) Anyway, the next step will be the store code - you must enter this to complete the call. This is, in most cases, the store number that you are calling from. Example: if you dial 1-700-707-2355, it will ask you to enter your code. If the store you are calling from is store number 0042, then 0042 is the code you would enter to complete the call.

That just about covers the model 8102. Now on to the good stuff: model MLX-100. MLX-100 has all the same features but it looks totally different. The first noticeable thing you'll see is that it has a display screen. Watch out for this type of phone, it will display whoever is calling and where they are calling from.

Directly under the screen you will see four buttons (black). Directly below each of them are another set of four buttons, home, inspect, menu, and more. Each of these buttons does a different specialized function which is of no relevance to this article. Below them you will see a set of 10 black buttons - this is the good stuff.

There are as follows: (left side) paging, privacy, blank, intercom voice, and intercom ring. The right side has pick up line one, pick up line two, pick up line three, followed by two blank buttons. Let's start with the paging button. This button is preprogrammed by the store to dial #96. This is the extension on the phones that is used to notify other employees or customers of what's going on. But please note this is not an extension. Unlike K-Mart, whose paging system is simply an extension on the phones like a department, Wal-Mart's is not. It uses the # for a reason, so as not to be confused with any other department that has a 96 in it. This is the only way to page on any of the phones. If the phone you have doesn't have a paging button, then you must manually dial #96 to activate the PA.

"Privacy" is used to keep your calls private and not have anyone pick up the line you're using and listen in on your calls. If the Privacy light is not on, you do not have a secure call.

"Blank" - these are the non-programmed buttons. Pressing these will do nothing. However, try your luck anyway. Some of them are programmed with different departments or other stores.

"Intercom voice" allows you to speak to a person in another room (they must also have an MLX-100) using the speakerphone.

"Intercom ring" is the same as intercom voice, but used as a prequel to it to see if they are available.

"Pickup line's 1-3" are pretty much self explanatory. If you are receiving an outside call you must pick up one of the three that the call is on.

Now on some of the MLX-100's there is no way to get an outside line without putting in a 3-digit code. The code is usually Feature 8xx, then you must pick up a free line. This is the only way on the "non-essential" phones to get an outside line. But in some cases the only type of line you can get is an inter-store line no matter what. Some of the phones (if you're lucky enough to get into the back of the store) don't even need a code to get an outside line. Just simply pick up the phone, choose an outside line, and dial away.

Ok, so now that I've covered most of the buttons on this type of phone, we will move on to the final group of buttons. They are: feature, HFAI, mutes, speaker, transfer, conference, drop, and hold.

Let's start with "feature". This in conjunction with the code 8xx allows you to pick up an outside line. The xx can be any set of numbers that your heart desires. Each one is supposed to be assigned to a different department head to keep track of who is making what calls and to where.

"HFAI" - I have no idea what this does and I can't seem to figure out what purpose it serves, so we will disregard it for now.

"Mute", "speaker", and "hold" are all self-explanatory.

"Transfer" allows you to obviously transfer calls to other areas of the store, simply by hitting transfer and then dialing the department number.

"Conference" allows you to make conference calls (similar to that of a party line).

"Drop" hangs up a call once it's placed on hold.

One last thing before I go: 800 numbers. Most of them are OK to dial on this type of phone, but some of them won't go through. I can only speculate that the 800 number is one that allows return billing for services (such as some tech supports and phone sex lines). 900 numbers are strictly forbidden and won't work so don't even try.

So wrapping everything up now, we see the ins and outs of the Wal-Mart phone system. So next time you're in a Wal-Mart and a new employee is having trouble with the phones, simply pull out this article and you'll be able to get the job done. Happy Hacking!

NORTH AMERICA

Akron, OH
Coffee Cartographers on the corner of East Exchange and Union near Akron University.

Albuquerque, NM
Winrock Mall Food Court, near payphones on the lower level between the fountain and arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

Anchorage, AK
Diamond Center Food Court, smoking section, near payphones.

Ann Arbor, MI
Galleria on South University.

Atlanta
Lenox Mall Food Court.

Austin, TX
Dobie Mall food court.

Baltimore
Baltimore Inner Harbor, Harborplace Food Court, Second Floor, across from the Newscenter. Payphone: (410) 547-9361.

Baton Rouge, LA
In the LSU Union Building, between the Tiger Pause and Swensen's Ice Cream, next to the payphones. Payphone numbers: (504) 387-9520, 9538, 9618, 9722, 9733, 9735.

Bloomington, MN
Mall of America, north side food court, across from Burger King and the bank of payphones that don't take incoming calls.

Boise, ID
Cyberplayce at 1019 Overland Rd.

Boston
Prudential Center Plaza, Terrace Food Court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Buffalo
Eastern Hills Mall (Clarence) by lockers near food court.

Charlotte, NC
South Park Mall, raised area of the food court.

Cincinnati
Kenwood Town Center, food court.

Cleveland
Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus, OH
Convention Center, lower level near the payphones.

Dallas
Mama's Pizza, northeast corner of Campbell Rd. and Preston Rd. in North Dallas, first floor of the two story strip section. 7 pm. Payphone: (972) 931-3850.

Ft. Meyers, FL
At the cafe in Barnes and Noble.

Helena, MT
Lewis & Clark County Library, near the walking mall.

Houston
Food court under the stairs in Galleria 2, next to McDonalds.

Kansas City
Food Court at the Oak Park Mall in Overland Park, Kansas.

Los Angeles
Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520, 625-9923, 9924.

Madison, WI
Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Mexico City, DF (Mexico)
Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones and the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

Miami
Dadeland Shopping Center in front of the Coffee Beanery by Victoria Station restaurant.

Milwaukee
Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

Nashville
Bean Central Cafe, intersection of West End Ave. and 29th Ave. S. three blocks west of Vanderbilt campus.

New Orleans
Food Court of Lakeside Shopping Center by Cafe du Monde. Payphones: (504) 835-8769, 8778, and 8833 - good luck getting around the carrier.

New York City
Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Northampton, MA
Javaline Cafe at 241 Main Street.

Orlando, FL
Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648, 896-9708, 895-6044, 6055.

Ottawa, ONT (Canada)
Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Pensacola, FL
Cordova Mall, food court, tables near AT&T. 6:30 pm.

Philadelphia
30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

Phoenix
Peter Piper Pizza at Metro Center.

Pittsburgh
Carnegie Mellon University student center in the lobby.

Portland, ME
Maine Mall by the bench at the food court door.

Portland, OR
Pioneer Place Mall (not Pioneer Square), food court.

Raleigh, NC
Crabtree Valley Mall, food court.

Reno, NV
Meadow Wood Mall, Palms Food Court by Sbarro, 3-9 pm.

Rochester, NY
Marketplace Mall food court, 6 pm.

St. Louis
Galleria, Highway 40 and Brentwood, lower level, food court area, by the theaters.

Sacramento
Downtown Plaza food court, upstairs by the theatre. Payphones: (916) 442-9543, 9644 - bypass the carrier.

San Antonio
North Star Mall food court.

San Francisco
4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

Seattle
Washington State Convention Center, first floor.

Sioux Falls, SD
Empire Mall, by Burger King.

Toronto, ONT
Harvey's on Queen St., across from MuchMusic. 8 pm.

Vancouver, BC (Canada)
Pacific Centre Food Fair, one level down from street level by payphones. 4 pm to 9 pm.

Washington DC
Pentagon City Mall in the food court.

AUSTRALIA, EUROPE, ASIA, SOUTH AMERICA, AFRICA

Aberdeen, Scotland
Outside Marks & Spencers, next to the Grampian Transport kiosk.

Adelaide, Australia
Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell and Pulteney Streets.

Antwerp, Belgium
At the Groenplaats at the payphones closest to the cathedral.

Belo Horizonte, Brazil
Pelego's Bar at Assufeng, near the payphone. 6 pm.

Buenos Aires, Argentina
In the bar at San Jose 05.

Bristol, England
By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Cape Town, South Africa
At the "Mississippi Detour".

Granada, Spain
Cafeteria Granada in Pza. Einstein near the Campus de Fuentenueva.

Graz, Austria
Cafe Haltestelle on Jakominiplatz.

Halmstad, Sweden
At the end of the town square (Stora Torget), to the right of the bakery (Tre Hjartan). At the payphones.

Hull, England
In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds, England
Leeds City train station outside John Menzies. 6 pm.

London, England
Trocadero Shopping Center (near Picadilly Circus) next to VR machines. 7 pm.

Manchester, England
Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

Melbourne, Australia
Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

Milan, Italy
Piazza Loreto in front of McDonalds.

Moscow, Russia
Burger Queen cafe near ITAR/TASS (Telegraph Agency of Russia/Telegraph Agency of Soviet Union) - also known as Nikitskie Vorota.

Munich, Germany
Hauptbahnhof (Central Station), First Floor, by Burger King and the payphones. (One stop on the S-Bahn from Hackerbruecke - Hackerbridge!) Birthplace of Hacker-Pschorr beer. Payphones: +49-89-591-835, +49-89-558-541, 542, 543, 544, 545.

New Delhi, India
Priya Cinema Complex, near the Allen Solly Showroom.

Paris, France
Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

Rio de Janeiro, Brazil
Rio Sul Shopping Center, Fun Club Night Club.

Tokyo, Japan
Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message and phone number at (516) 751-2600 or send email to meetings@2600.com.

Special Offers

2600 Shirts

The new 2600 shirts have arrived! And the NSA loves them!

Version 1 (see photo below) has a nifty hacker dateline on the back and the latest headlines from the hacker world on the front. Black lettering on white. $15, 2 for $26

Version 2 (see photo below right) is only for those of you into cryptology. Others are prohibited from owning this shirt. Do not wear this around children or senators. White lettering on black.
$15, 2 for $26

All shirts are printed on high quality 100% cotton. Available in L, XL, and XXL. (XL fits most nearly everyone.) $15 each or two for $26.

We also have navy blue Beyond Hope shirts left over from the conference! You can now lie to your friends and say you were there even if you weren't! $12 each or pay $30 total when ordered with any two other shirts - that's ten bucks a shirt! Limited availability - XL and XXL only.

Caps

Stand out in the crowd of people wearing caps. Yes, 2600 caps, suitable for raving, are finally out. Despite the wide disparity of heads, we're assured that this one can be adjusted to fit. Those of you who went on a different evolutionary route may have problems.
$10

Off The Hook CD ROMS

After many years, we've finally gotten off our asses and put together a collection of the hacker radio show "Off The Hook" so that people outside the New York metro area can join the fun! And we're doing it at a price that is almost as cheap as turning on your radio. Each cd-rom holds nearly 100 hours of audio. All you need is a computer with a cd-rom drive and browser software (available for free on the net) and a realaudio player (also available for free from www.realaudio.com).

You do NOT need net access to play these files! And you can still download our shows one by one off our web site for free!
10/88-12/91 $20
01/92-12/93 $20
01/94-09/95 $20
10/95-06/97 $20

Hope Videos

Another project we took our time doing. From the first HOPE conference back in 1994, the following is available:

The HOPE intro & Robert Steele's speech. 60 minutes ($15)
A guide to Metrocard from a mystery transit worker. 80 minutes ($15)
The LINUX people discuss their OS and Bernie S. talks about TDD's. 100 minutes ($20)
TAP Magazine with Cheshire Catalyst/Dave Banisar on Digital Telephony and the Clipper chip. 105 minutes ($20)
The 2600 panel featuring Emmanuel Goldstein, David Ruderman, Scott Skinner, and Ben Sherman. 60 minutes ($15)
Encryption and beyond with Bob Stratton, Eric Hughes, Matt Blaze, and Bernie S. 120 minutes ($20)
The National ID Card with Judi Clark, Bob Stratton, and Dave Banisar / the famous Social Engineering panel. 100 minutes ($20)
Hacker authors featuring Julian Dibell, Paul Tough, Winn Schwartau, Rafael Moreau, and some of the production staff for "Hackers." 75 minutes ($15)
Cellular Phones with Jason Hillyard, Bernie S., and Mark. 120 minutes ($20)
European Hackers featuring the Chaos Computer Club. 65 minutes ($15)
The Art of Boxing with Billsf and Kevin Crow - Phiber Optik phones in from prison. 105 minutes ($20)
Closing ceremonies. 40 minutes ($15)
Order the complete set for only $150!

To Order

Send a list of what you want (be specific!), your address, and your money to:

2600
PO Box 752
Middle Island, NY
11953