getting caught: hacker's view

Deep down, every hacker wants to get caught. Computer hacking isn't really the same as killing or stealing, after all. You need at least a little brains to be able to hop around on the corporations' DECsystems or to know the ARPANet better than your own PC. So if and when you get caught, you wind up getting a little bit of credit for having some brains. Most people exaggerate and call you a genius! Who can resist this type of an ego boost?

So when the FBI came knocking at my door early this spring, it seemed like the beginning of an adventure. It was me they were after! I had done something to deserve national attention!!

At first I didn't know what it was they wanted. They came to my house before I was awake and showed my mother the search warrant. I'll never forget the tone in her voice when she called me that day. "You'd better come down here right away," she said, sounding very worried and pissed off at the same time. I knew something was up when I heard that.

So then I came downstairs and saw what was happening. I was very calm throughout the whole thing—I even kept my sense of humor. After I figured out which of my many "projects" they were interested in, I showed them where all the good stuff was hidden. "Go tell the world," I said.

I had been hacking for about a year. I seemed to pick up things incredibly fast and before I knew it, I was buried inside the weird world of phones and computers. In this case, I had been running a huge corporation's mainframe for them for a few months. This computer had so much data in it that I could find out (and change) just about anything—paychecks, profit margins, telephone numbers, you name it. I had lots of fun.

My friends used to come over late at night and watch me explore. Nobody knew they had been able to do anything like that and it seemed pretty amazing. Then War Games came out and I turned into a sort of cult figure in my neighborhood. But it was OK—nobody knew exactly what I was doing.

Even my parents didn't seem to mind that much. They'd shake their heads and wonder what kind of mischief I'd get into next. Most people (grown-ups, that is) seemed to act exactly the same. And my friends were all into it as something run and rebellious.

So now that I was caught, I expected the fun to continue. My parents would be outraged that a mischievous kid was being hounded by the feds while murderers and presidents were roaming free. And of course, my friends would stick by me more than ever. We were pretty tight.

For about a day, that's exactly what happened. My name got in all the papers. I was on a few news shows, and nobody really understood anything. I suddenly became popular at school. Everybody seemed to agree that it wasn't fair for them to come to my house and take away my two computers just like that.

Then, after the initial shock, people's moods started to change. My parents were the first. They suddenly got mad at me. "What a stupid thing to do!" I remember those words. "If you don't care about yourself, at least think about what you're doing to your family," and so on. They also said that I never listened when they told me to knock it off, which was totally false, since they never really seemed to care at all.

But all that didn't upset me. After all, parents are supposed to say those kinds of things. I knew they really cared, so it didn't matter what they said.

It wasn't until a few more weeks that the really bad stuff started happening. The feds began calling my friends and tried to scare them into saying incriminating things about me. They told them they'd be in just as much trouble if they didn't say anything. I could tell something was wrong when all of a sudden no one was talking to me. People I used to hang out with suddenly seemed uneasy when I was around.

Then the feuds started calling me. And I could tell from the pointed questions they were asking, that someone I trusted had told them a lot. Much more than they had to. It wasn't like they had just cracked and said, yes, he did this and that. They volunteered information! I tried to figure out why someone would do this—no one I knew had any grudges against me. I didn't really have any enemies. They must have thought that telling everything was for my own good. The feds had probably told them that I was really sick and needed help and that only the truth would set me free. Could that have been it?

It might have been. But there was definitely more than that. When the feds started searching my friends, that was my fault. At least it seemed that way to my friends. A couple of them got so scared that their families hired these big, expensive lawyers. And that was my fault, too—even though I knew they were being ripped off.

So what did I get out of the whole thing? Well, nobody trusts me anymore—people are even afraid to let me use their phone. I've gotten a reputation as someone who doesn't care at all about his friends, otherwise how could I have put them in such a spot? Everyone in town knows that I did something bad to some corporation somewhere, but nobody understands how much of a game the whole thing seemed at the time. The newspapers were never really interested in my side and nobody else seems to be either.

Maybe this is good in a way, because I found out that most people value friendship less than their own safety. As soon as the pressure is applied, they lose all feeling for you. They trick themselves into believing that you were always a bad seed from the start. They do this so they won't feel guilty about the way they shafted you. But there were a couple of others who didn't desert me because they knew who I really was. If it wasn't for them, I might have just jumped off a building one night. That's how bad it makes you feel sometimes.

Yes, I'm through hacking. Let the professionals do it—they can't get hurt like I was.

Name withheld by request.
VITAL INGREDIENTS
SWITCHING CENTERS AND OPERATORS

Every switching office in North America (the NPA system) is assigned an office name and class. There are five classes of offices numbered 1 through 5. Your CO is most likely a class 5 or end office. All Long Distance (Toll) calls are switched by a toll office which can be a class 4, 3, 2, or 1 office. There is also a 4X office called an intermediate point. The 4X office is a digital one that can have an unattended exchange attached to it (known as a Remote Switching Unit—RSU). The following chart will list the office number, name, and how many of those offices existed in North America in 1981.

<table>
<thead>
<tr>
<th>Class</th>
<th>Office Name</th>
<th>Abb.</th>
<th># Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Regional Center</td>
<td>RC</td>
<td>12</td>
</tr>
<tr>
<td>2</td>
<td>Sectional Center</td>
<td>SC</td>
<td>67</td>
</tr>
<tr>
<td>3</td>
<td>Primary Center</td>
<td>PC</td>
<td>230</td>
</tr>
<tr>
<td>4</td>
<td>Toll Center</td>
<td>TC</td>
<td>1,300</td>
</tr>
<tr>
<td>5</td>
<td>Intermediate Point</td>
<td>IP</td>
<td>10,000</td>
</tr>
<tr>
<td>R</td>
<td>RSU</td>
<td>RSU</td>
<td></td>
</tr>
</tbody>
</table>

When connecting a call from one party to another, the switching equipment usually tries to find the shortest route between the two parties. It will then move up to the next highest office for servicing (Class 4). If the Class 4 office cannot handle the call, it will be sent to the next office in the hierarchy (3). The switching equipment then uses the high-usage interoffice trunk groups. If they are busy, it goes to the final trunk groups on the next highest level. If the call cannot be connected then, you will probably get a reorder ([120 IPM (Interruptions Per Minute)]—also known as a fast busy). At this time, the guys at Network Operations are probably going berserk and it will have to go through the process of “social engineering.” It is also interesting to note that 9 connections in tandem is called ring-around-the-rosy and it has never occurred in telephone history. This would cause an endless loop connection (an interesting way to really screw up the Network).

The 10 regional offices in the United States and the 2 in Canada are all interconnected. They form the foundation of the entire telephone network. Since there are only 12 of them, they are listed below:

<table>
<thead>
<tr>
<th>Class Name</th>
<th>Abb.</th>
<th># Existing</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>RC</td>
<td>12</td>
</tr>
<tr>
<td>II</td>
<td>SC</td>
<td>67</td>
</tr>
<tr>
<td>III</td>
<td>PC</td>
<td>230</td>
</tr>
<tr>
<td>IV</td>
<td>TC</td>
<td>1,300</td>
</tr>
<tr>
<td>V</td>
<td>IP</td>
<td>10,000</td>
</tr>
<tr>
<td>A</td>
<td>RSU</td>
<td></td>
</tr>
</tbody>
</table>

They are known as: Step. Crossbar, and ESS. Check past and future issues of 2600 for complete details on how these systems work.

Operators

Another vital ingredient of the Network is the telephone operator. There are many different kinds. What follows is a discussion of some of the more common ones:

- **TSPS Operator.** The TSPS (Traffic Service Position System) operator is probably the bitch (for bastard for the phemal liberationis) that most of us are used to having to deal with.

  Here are her responsibilities:

  1. Obtaining billing information for Calling Card or 3rd number calls.
  2. Identifying called customer on person-to-person calls.
  3. Obtaining acceptance of charges on collect calls.

- **TNIS Operator.** The TNIS (Traffic Number Identification System) operator is not as notorious as the TSPS operator. This is due to the fact that they assume you are a know company employee. The divestiture, though, has resulted in the break-up of a few NOS-PU B #'s and policy changes in TNIS.

- **INTERCEPT Operator.** The intercept operator is the one that you are connected to when there are not enough recordings available or the area is not set up to tell you that the number has been disconnected or changed. They usually say, “What number did you dial?” This is considered to be the lowest operator lifeform since they have no power whatsoever and usually know very little.

- **OTHER Operators.** And there are the: Mobile, Ship-to-Store, Conference, Marine, Verify, “I leave Word and Call Back.” Route and Rate (KIP+300+141+121+51) new number as a result of the break-up, and other special operators who have one purpose or another in the Network.

With an Operator? Ask to speak to their supervisor...or better yet, the Group Chief (who is the highest ranking official in any office), the equivalent of the Madame in a whorehouse (if you will excuse the analogy).

Some CO’s, by the way, have bugs in them that allow you to use a 1 or the 4th digit when dialing. (This happens mostly in crosshairs and it doesn’t work correctly.) This enables a caller to call special operators and other internal telco numbers without having to use a blue box. For example, 415-121-1111 would get you a San Francisco-Oakland INWARD Operator (the above was taken from Basic Telecommunications Part IV, written by BIOC agent 003).
NSA Wants Better Phones

The New York Times

The National Security Agency is proposing that the Government and industry be equipped with as many as 500,000 telephones that can be secured against interception.

The agency is convinced that the Soviet Union and the other nations are obtaining important intelligence from United States telephones.

Although cloaked in secrecy, a program like the one the agency proposes could cost hundreds of millions of dollars.

Under the proposal, production of the secure phones would begin in two years.

The number of secure telephones currently used by Government agencies is classified information. But the Carter Administration said there were 100 such phones in the Government and it planned to buy 150 more. The cost of each phone then was $35,000. The Reagan Administration has bought an unknown number of additional secure phones.

“Anyone making a phone call to the West Coast or Boston from the Washington area has no idea how the conversation will be transmitted,” an NSA spokesperson said. “It might go via fiber optics, conventional cable, microwave towers or one of the 19 domestic satellites. If it is going via satellite you can presume the other guy is listening to it.”

Oh No, Not Again!

Associated Press

The House passed a bill on September 17 by voice vote that would make it a Federal crime to gain unauthorized access to or tamper with computerized medical records.

Victimized by Crime Computers

The New York Times

Police officers went to an apartment in New Orleans looking for a woman named Vera Davis, who was wanted for theft and forgery. Although the woman who answered the door identified herself as Shirley Jones, they arrested her anyway. A police computer listed Shirley Jones as an alias used by the forgery suspect. That was two and a half years ago.

According to her attorney, Mrs. Jones, who was once advised by a sheriff's deputy to change her name to avoid future arrests, is one of a growing number of people in New Orleans who have gotten in trouble with the law because of inaccurate, outdated, or misused information in police computers.

The New Orleans computers are part of a national network. From a local terminal, a computer check can be run through the National Crime Information Center in Washington, operated by the FBI, in less than a minute.

The New Orleans case, said Robert Ellis Smith, publisher of Privacy Journal, a newsletter that reports on privacy cases from Washington, DC, is "symbolic of a larger national problem, an incredibly high rate of inaccuracy" in criminal records and "an inordinate amount of mistaken identity cases in the criminal justice information systems."

Sears Satellite Network

Associated Press

The American Satellite Company has signed a contract with Sears, Roebuck and Company to construct and operate a private communications system linking corporate offices of Sears and its subsidiaries in 26 United States cities. This would be the largest private system ever developed capable of offering full-motion video teleconferencing.

Loopholes Around Wiretap Laws

The New York Times

Senator Patrick J. Leahy, Democrat of Vermont, has said that he will seek legislation to improve protection of privacy by closing gaps in Federal wiretapping laws.

He and several experts said at a Senate Judiciary subcommittee hearing that it was unclear, for example, whether existing laws permitted Government officials or others to intercept electronic mail, or even ordinary telephone calls sent by computer or microwave technology, without a warrant.

"There are tremendous holes in communications privacy today," testified Ronald L. Plesser, a Washington lawyer who has long specialized in information privacy issues.

The experts at this hearing testified that private interception of electronic mail and other messages carried through telephone networks may not violate Federal law.

IBM is Buying Rolm!

The New York Times

IBM has said that it will by the Rolm Corporation, in a move that will heighten the competition between the world's largest computer company and AT&T. The price? $1.25 billion.

"IBM wants it all, it needs it all," said Esther Dyson, editor of Release 1.0, an industry newsletter. "They have a biological urge to grow."

Most analysts, however, said that IBM had realized—perhaps belatedly—that it greatly needs to strengthen its offerings in telecommunications switching equipment.

Rolm, founded in 1969 as a maker of military computers is now a leading maker of private branch exchanges, systems that control both voice and data communications over the telephone.

911 Suspect Hung Up

The New York Times

A notorious hoax caller who has plagued 911 switchboards for three years has been nabbed reporting another bogus crime, police say.

Cops say the suspect—who they have been unable to identify—made more than 500 false reports ranging from strangulations in progress to rapes and shootings of police officers.

He was arrested at a Penn Station pay phone while telling a 911 operator he had just raped and strangled his girlfriend with her pantyhose. That was the fabricated crime he reported most frequently, according to police.

"He called every day of the week at all hours," said Sgt. Stephen McDonald.

"He was causing a lot of problems and the 911 people were really looking for him," said Officer James Lapiedra who collared the hoaxter.

According to McDonald, news of the hoaxter's capture was jubilantly received by 911 operators: "There was a lot of cheering."

In the words of Lapiedra, "He was surprised he was caught."
LETTERS FROM THE OUTSIDE WORLD

Dear 2600:

I am currently involved with the Crystal Palace BBS, formerly OSUNY (hopefully you have heard of it). The system is down now for some software modifications, and many people have tried to persuade me into changing the purpose of the board which is telecommunications and other related fields. The crackdown on this type of BBS is starting to become overwhelming. This is what my inquiry is about. After reading your first copy of a newsletter, I was elated with the quality and content of information it had! Referring to the front page article (July 1984, page 1-37), "Look Out. He's Got a Chip on His Shoulder," I sense that the anti-computer hysteria has gone and is going to go far too! I am interested to know what exactly is an illegal BBS message and what is not. Do I have to monitor the system 24 hours a day, 7 days a week? Am I responsible for every message posted on the board? I know that these are questions that everyone wants answers to and can’t find. As I see it the BBS is just another form of newsletter, so why are they picking on us?? I do, however, realize that some messages are quite illegal like credit card numbers and the like, but the information on how to get those #’s is not illegal (right?). Any information on this subject would be greatly appreciated.

Crystal Palace

Dear CP:

What is a BBS? You know the answer, we do, and a good many of our readers also do. The problem is that the people who go around passing laws and raising hands don’t have the slightest idea what a BBS really is. All they care about is the fact that a computer is involved somewhere along the line. And computers, they say, can do anything in the world. But what’s so ironic in the case of a BBS is the fact that the computer is just storing messages! The exact same effect could be accomplished on a physical bulletin board, inside an auditorium, or in everyday conversation. But you don’t see these things being outlawed because people would never stand for that kind of repression (we hope). Computers are easy targets because the average person doesn’t understand them at all. By making people think that it’s actually illegal to write something down and pass it along to others, the authorities are taking one great step towards total control.

We agree that a BBS is really another form of newsletter. We don’t agree that messages containing credit card numbers are illegal in any sense. (They are boring, though, and practically useless to anyone except fraud investigators.) It’s the actual use of these numbers that constitutes fraud, not the simple act of passing them around. If a cop on the street overheard you giving numbers to a friend, could he arrest you? Let’s hope it hasn’t reached this stage.

We’re currently working on getting some more legal information concerning this subject so that we can address your questions better. In the meantime, though, we hope your board and the many others like it around the world won’t be intimidated by these scare tactics. You can talk about whatever the hell you want. But it’s still illegal to commit the crimes you’re talking about.

If enough of you guys stood up for your rights out in the open, this wouldn’t be such a problem. You might actually wind up saving an important part of democracy for a few more years.

By the way, readers, if you’re running a BBS that talks about these things or knows of one that does, send in the name and phone number for our Hot 100 list which will be published soon. Make sure the BBS you’re sending wants to be publicized and that it includes a reason or two why your BBS is better than most. Check the front page for our addresses.

Dear 2600:

Received your August issue, and enjoyed it. A number of comments...

1) Does anyone know what happened to TAP?
2) There is a newsletter called the Comsec Letter, available for free from Ross Engineering Asso. 7906 Hope Valley Court, Atlanta, GA 30319. Lots of good information, but they want a letter requesting the newsletter on letterhead and identifying your interest in communications security (one can’t be too careful these days!). It’s always interesting to know what’s happening on the other side...
3) What works against an ESS switch? Black boxes are ok, but more modern equipment seems to be coming in rapidly, blowing our older techniques off the air!

The Animal

Dear Animal:

For info on TAP, consult our September issue, page 1-52. We hate repeating ourselves all the time.

Thanks for the sample copy of Comsec Letter. It looks interesting and we’re looking into reprinting some of the good stuff. Readers: feel free to send us anything that looks like it might be interesting to us. It usually is.

ESS switches and black boxes are dealt with extensively on page 1-43 of our August issue, as you probably know. The only thing we can suggest to counter an ESS is ingenuity. There’s always a way to get around anything.

Dear 2600:

I really enjoy your publication! It seems you guys are not a bunch of wimps who are so damn paranoid that the feds are going to catch you. Anyway, what types of back issues do you have? I received my first issue, which is Volume 1, Number 1.

What are the context of the back issues? I’m looking for one having to do with loops, sprinting, hacking out sprint/mci’s, or anything similar. Also, any arpanet/archnet stuff?

kd

Dear kd:

We’ll be publishing a guide to our back issues that should be out right in time for the Christmas rush. Just about all of the topics you mentioned have already been covered and they all will be covered in the future. We accept articles and information from anyone.

You’re quite correct in saying that we’re not paranoid. We have nothing to be paranoid about because we’re not doing anything wrong.

Dear 2600:

Though it may seem like only yesterday that computer crime first caught the nation’s fancy, it has been on the mind of state legislators for quite some time. With the recent passage of computer crime laws in Maryland, Iowa, Connecticut, and Hawaii, the number of states lacking computer crime laws has fallen to seventeen. The laws of the other 33 have been collected in a new reference work published by the National Center for Computer Crime Data, and called The Computer Crime Law Reporter. In the course of compiling the texts of all the state computer crime laws on the books, editor Jay BloomBecker found that a number of states had bills on the books for years without anyone noticing them.

The book, 200 pages plus two updates, is available for $45 from the National Center for Computer Crime Data, 4053 J.F.K. Library, California State University at Los Angeles, 5151 State University Drive, Los Angeles, CA 90032.

In addition, the National Center will begin publishing a newsletter devoted to morals and ethics in computing. Its name is Conscience in Computing.

There are schools teaching computer ethics, no matter how many are not. There are professionals questioning their roles as computer scientists and asking about the social impact of their work. There are computer bulletin boards which support ethics discussion groups.

Conscience in Computing will be a monthly newsletter, subscriptions costing $18 annually. Work exchanges allow readers to become subscribers by convincing others to subscribe, reporting news of conscience in computing, or working out an individual contract with the National Center. Interested people can write to the above address.

The National Center for Computer Crime Data
(The National Center for Computer Crime Data is a nonprofit research organization at California State University at Los Angeles.)

Whoopsee

In our last issue, we forgot to mention that in our August issue, we forgot to mention that the front page story ("But How Does It Work?"") came from the desk of BIOC Agent 003. Better late than never.
CONTACTING THE GESTAPO!

Security
as close as your fingertips

CORPORATE SECURITY
Director Corporate Security
H. L. Young
1-212-295-0505

SECURITY STAFF
Security Supervisor
W. F. McGarly
1-212-295-0528
R. F. Jobson
1-212-295-0552

NEW YORK CITY REGION
Security Manager
W. B. Brem
1-212-295-4156

New York City West
Security Office
1-212-295-0515
R. P. Keenan
1-212-295-0518

New York City East
Security Office
1-212-291-9617
C. J. Hauswirth
1-212-523-9953

STATE REGION
Security Supervisor
H. F. Gallagher
914-699-9949

Suburban
J. J. Ferraro
914-699-9985
H. Zolli
914-699-9985

Mid-State
Long Island
Security Office
516-294-0210
Security Supervisor
R. H. Lamberson
516-294-0722
Security Manager
T. A. Paolucci
518-449-3250

TOLL FRAUD
To query office
212-221-1764
Security Supervisor
212-221-5644
Security Manager
J. S. Whitman
212-295-0507

On weekends, holidays and out of
hours, call the following telephone num­bers to obtain assistance:
Customer Service Bureau
New York City Region
1-212-295-2571
Mid-State
914-390-5600
Long Island
516-742-3030
Security Office
518-449-3250

BUILDING PROTECTION
ORGANIZATION
Guard Coordinators
New York City Region
W. J. Blueme
1-212-394-3400
H. K. Askildsen
914-694-8253
State Region
T. A. Paolucci
518-449-3250
Security Manager
518-449-3250
T. J. Doran
518-449-7224

*NOTE: These telephone numbers
should be called concerning matters of
building protection.
Humm-mm-mm. That's the dial tone—your "go ahead" signal to start dialing. Please wait for it.

Answer Promptly

Don't make a friend wait or miss a call by not answering your telephone at once.

Area codes are used to call from one telephone area to another, but not within the same telephone area.

TRY ONE-PLUS DIALING.

- Telephone cords and water don't mix. A wet cord can put your telephone out of order. So please keep your telephone cord away from sinks, valves, steam and other places where water might get on it.

DIAL CAREFULLY!
Avoid wrong numbers by first checking the number and them
DIAL EACH DIGIT CAREFULLY!

IF YOU'RE NEW IN TOWN...

Party-liners—don't forget the other fellow needs the telephone too.

For better service, don't transfer a call to someone else if you can take care of it yourself.

When you're away from your office— who'll answer your phone?

Shop the Yellow Pages

Party-liners—don't forget the other fellow needs the telephone too.

For better service, don't transfer a call to someone else if you can take care of it yourself.

Save time . . . telephone.

When you're on the go . . . you're as close to home or office as the nearest public telephone booth . . . try it and see.

The wheel that lets you roll around town without leaving home.