2600 March, 1984

Published monthly by 2600 ENTERPRISES, an electronoxary organization. Subscription rates are $10 annually. Write to 2600, Box 752, Middle Island, NY 11953. FSLN 3 VOLUME ONE, NUMBER THREE

THE CONSTITUTION OF A HACKER

With every generation of humans, there are certain types of individuals that emerge. There are (always have been and always will be) leaders, followers, general nuisances, etc. And then there are folks who like to play with things and figure out how they work.

Before technology came along, there really wasn't all that much for these people to play around with. And certainly there was no way for them to pool their resources except through face-to-face communications.

With telephones, of course, all aspects of human life changed. Here was a toy that *anyone* could play with and get virtually unlimited results. But of course, most people didn't (and don't) see it that way—phones are phones and nothing more. You're not supposed to have fun with them. Yet, certain adventuresome types insisted on having fun with their phones anyway. They did all kinds of things they weren't supposed to do, like figure out the way phones work and interconnect. For the first time, these technological enthusiasts posed a "threat" to technology by reaching out and touching it rather than simply using it without asking any questions.

Today there are lots of people still having fun with their phones and making all kinds of technological advancements of their own. But the real focus at the moment is on the newest "threat," people who like to experiment and have fun with computers. Not the kind of fun they're *supposed* to be having with Pacman® and Mr. Do®, but *unauthorized* fun with other people's computers.

Why do they do this? What do these people possibly have to gain by breaking into computer systems and seeing things that don't really concern them or that is of no possible use to them? In the great majority of cases, computer hackers don't gain anything material or financial from their exploration. Add to that the high risk of getting caught and it becomes very hard for the average citizen to understand what motivates these people.

Many computer hobbyists, in fact, are resentful of hackers, considering them immature and troublesome. Quite a few computer bulletin boards prohibit certain topics from being discussed, and when they do, hacking is almost always one of them. There is some justification behind this, since the image of all computer users can be adversely affected by what the hackers do.

There are also the legal people who insist on telling everyone that breaking into a computer by phone is just like physically breaking into a home or office. Fortunately, that logic seems to be shared by very few people.

In spite of all of the threats and criticism, though, the hackers are not "cleaning up their act." And public opinion, particularly among the young, seems to be in their favor, mostly as a result of media coverage.

There's even a weekly TV program about hackers called *The Whiz Kids*. Each week, this group of amazing kids has a new adventure. The scripts are a bit moronic but interesting nonetheless. In one episode, the kids (only one of which is a true hacker) find out about an evil person who happens to be stealing Social Security checks. (They discover this by casually logging into his bank account.) To teach him a lesson, they break into another computer and enter his name as being deceased. In each program, these kids break into at least one new computer. But do they ever get into trouble? Of course not. First of all, they're only children. And second, they're entering these computers for good reasons, even if they are unauthorized.

Now what kind of message is this program conveying? Apparently, it's OK to invade other people's privacy if your intentions are ultimately "good." It sounds like something Reagan would get a kick out of.

A genuine hacker breaks into computers for the challenge. He's not out to save the world, nor to destroy it. He is not out to make a profit out of what he's doing. Therefore, it's not fair to categorize him as a criminal and it's just as wrong to say he's some sort of a savior.

Technological enthusiasts operate with the same motivation that a good mountain climber has. Regardless of what may happen to him, a computer hacker will *always* be interested in playing with computers. It's in his nature. And any laws that are created to "eliminate" hacking simply won't work because of these facts. There will always be people who want to experiment with things and this urge cannot be stifled. Did hacking come to a grinding halt because of the "414" scandal? Or because of the Telemail raids? No. Judging from the proliferation of computer bulletin boards where hacking *is* discussed, it's getting bigger than ever.

The realistic way for the owners of large computer systems to look at this is to regard hackers as *necessary security checks*. That's right. Necessary because if the hackers weren't the ones to break in, who would be? Let's assume that hackers had never even tried to break into the Memorial Sloan-Kettering Cancer Center computer. Someone else would have, because the system was practically wide open. And maybe they would have had a *reason* to get into the system—to do various nasty things. But now, because of what the hackers did, the Sloan-Kettering system is more secure.

One could almost say that a person with hacking abilities has an *obligation* to try and get into as many different systems as he can. Let's get nationalistic for a moment. If you have the number for a top-secret government computer in Ft. George G. Meade, MD, odds are that the Albanians have it also. Now, would it be better for them to break into the system and find out all kinds of nice things or for you to break in and be discovered, forcing the system to become more protected? And, if you do break in, don't you deserve a note of thanks for waking them up?

Keep in mind, though, that a computer hacker is under *no* obligation to turn himself in or warn operators that their system is easily penetrable. It's the job of the sysops to notice when their computers are being tampered with and if they don't detect you, then that's a second security lapse for them.

This is a pragmatic view, however shocking it may seem. In closing, we should point out to the hackers themselves that there is no need to worry or fret if their methods or secrets are eventually discovered. This is only the beginning. Our world is turning into a technological playground.

ALTERNATE LONG DISTANCE

First of a persistent series — how the companies work and a guide to MCI

SWAGIMA. That's the word that National Public Radio uses to describe long distance services. It stands for SBS (or Skyline), Western Union (or Metrofone), Allnet (or Combined Network Services), GTE Sprint, ITT, MCI, and of course AT&T. And there are many more, each of which will eventually be covered in our pages. Right now though, we'd like to give you an idea of what these systems are and how they work.

Except for AT&T, all of the above systems work in a fairly similar manner. (This will be changing very soon and very dramatically under the terms of the Bell divestiture.) Each system has its own series of networks, i.e. land-lines, lines leased from AT&T, microwave relays, satellite links, etc. They each have local city access numbers, although some like Allnet and MCI have special ways of using a "travel" service by dialing a special number, while Sprint uses a "travelcode" to access nodes outside the subscriber's city. On others, like Metrofone, you can use the same authorization code from any of their access points.

A long distance telephone company consists of four major parts: you have your input—that is, a local access number or a toll-free "800" number to access the system. When you do this, a device called a "switch" answers, giving you the familiar "computer dial tone." When you enter your authorization code and destination number, you are routed over their network. The heart of the system is the controlling system, which includes the "switch." This is the computer that checks the authorization code, has provisions for time-of-day restrictions, travelcodes, accounting codes, and the like. They have a few provisions which the long-distance services don't appear to use, such as the infamous "speed number" recording which was a favorite of many phone phreaks (for reasons you'll soon know if you don't already). The system checks to see if the location being dialed is on the network, and acts accordingly. It makes a log of numbers called, the authorization code, and time usage which is stored on a word processing tape and then read by another system for billing. Some companies charge in one minute increments, although the system has the capability to record time usage in 6 second increments.

There are quite a few different systems in use today. A couple of the most common ones are made by Northern Telecommunications, which is based in Dallas, Texas. Another company that sells similar equipment is Rockwell Wescom. MCI allegedly is in the process of buying new switches from them, and they will be installed by Dynacomp Telecommunications, also based in Dallas.

Microwave Links

Most of the low cost services, at one point or another, use microwave antennas to transmit calls. Each microwave station is located about 30 miles from each other to make up for the curvature of the earth since microwaves travel in a straight line. Each of these stations has 4 dishes (at least). One dish is used to receive from a previous station and one is used to transmit to that station. The other two dishes do the same thing to the destination station—one receives and one transmits. So if you make a call 3000 miles away, you may wind up going through 100 different microwave stations, many of which you can see next to major highways.

This is how the alternate long distance companies manage to charge less than AT&T; they use their own systems. But this is also why, in many instances, the sound quality is poorer on the alternate services. Remember, a chain of microwave towers is only as strong as its weakest connection.

A Look at MCI

MCI (Microwave Communications Inc.) was the first new kid on the block, way back in 1967 when the idea of an alternate phone service was almost unheard of and practically illegal. MCI was first used solely by businesses who wanted to communicate between the cities of Chicago and Cleveland. That was it. And even with this amazingly limited system, MCI ran into problems with AT&T, who didn't want *anybody* trying to do what they did. Lawsuits followed, with MCI eventually getting a promise of eventual equal access to the AT&T network. In fact, MCI's legal action is considered one of the motivating factors behind the break-up of the Bell monopoly.

Now MCI is the biggest of the alternate services (they have well over a million subscribers at present, having opened their doors to residential customers a mere 5 years ago) and also one of the hardest to penetrate. The system has 5 digit codes that are entered before the 10 digit phone number, a total of 15 digits. But these codes only work from one location, making it rather unlikely to find one by guesswork. If you want to use the system from another city, you have to sign up for MCI "credit card" service which costs an additional $5 a month (on top of an initial $5 a month charge for the regular service). Here you get a list of 48 phone numbers around the country and a 7 digit code which can be used from any one of them. Most code seekers prefer scanning the "credit card" numbers since more numbers work overall. However, a strong argument can often be heard in favor of the 5 digit numbers that are located in densely populated areas like Los Angeles or New York. Naturally, the odds of finding something increase under those circumstances.

No Proven Method For Finding Codes

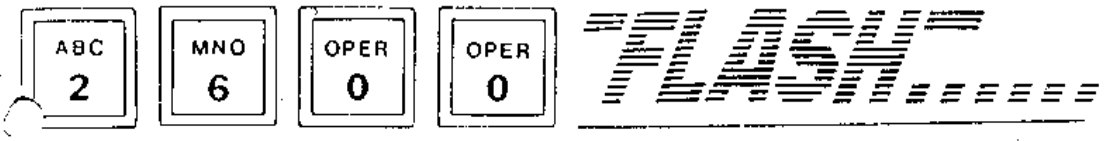
MCI, being the oldest of the companies, has learned quite a bit in that time. Therefore, no major bugs are still crawling around on their system. Hackers have many theories on number patterns, of course. For example, numbers like 22222 or 12345 tend *not* to work. In other words, your guess is as good as ours. As far as what they do when they know a code is being abused, MCI seems to be more interested in changing the code rather than laying a trap, as other companies have been known to do. Of course, this doesn't mean that they're incapable of doing such a thing.

MCI Features

The MCI tone sounds like all the others (a hollowish, medium-pitched, steady tone), but it has its own set of recordings, depending on what you do to it. If you enter an invalid code, you'll hear a mechanical female say: "THEE AUTHORIZATION CODE YOU HAVE DIALED IS INVALID TWO ZERO THREE" and then an ESS reorder that trips over itself (listen to it and you'll understand). If you dial someplace you're not supposed to call (for whatever reasons), you'll hear: "THEE NUMBER YOU HAVE DIALED ISNOT ON THE NETWORK TWO ZERO THREE" and the reorder. Each MCI dialup has its own 3 digit identity code and they tend to be similar the closer together they are.

Many businesses are installing MCI "dedicated lines" in

(continued on page 4)



718 is coming!

The New York Times

The New York State Public Service Commission has voted to begin dividing New York City into two area codes on September 1 to "prevent an impending exhaustion of telephone numbers." At that time, the old 212 area code will begin to reach only Manhattan and the Bronx, whereas a brand new area code, 718, will start to work for Brooklyn, Queens, and Staten Island. The whole system becomes mandatory on January 1, 1985.

Charles Herndon, a New York Telephone spokesman, said that the 718 code was assigned to the city years ago by the North American Dialing Plan, a group that administers area codes in the U.S., Mexico, and Canada.

"Of the numbers available at the time, 718 was the best," he said. "There weren't that many available."

The P.S.C. rejected recommendations by a consultant (Economics and Technology, Inc.) hired by the City Board of Estimates. Those recommendations called for the implementation of the 718 area code, however, instead of using it for people, the consultant suggested using it exclusively for computers, paging systems, and other devices, since they were the main reason for the new area code in the first place.

[*2600* would like to go on record as enthusiastically supporting the idea of an entire area code of machines.]

Supercomputer dialups

Physics Today

Astronomy and astrophysics are gathering so much data by telescope these days, that it cannot be handled by conventional computers, according to Dr. Vincent Icke of the University of Minnesota.

To remedy the problem, Dr. Icke called for the creation of a central supercomputer facility that would be at the disposal of all astronomers and astrophysicists nationwide via telephone lines.

Wiretap City

The New York Times

After an investigation, the New Haven (Connecticut) Board of Police Commissioners, a civilian body that oversees the Police Department, revealed in 1978 that the department had routinely tapped the phones of residents from 1964 to 1971, apparently to monitor radical political activity. This, the board said, was illegal.

In December 1982, after it had been disclosed that the phones of some 3000 residents had been tapped, the Federal District Court in Bridgeport made the case a class action, inviting anyone who felt wronged to become a plaintiff.

So far, 1230 people have become plaintiffs. They include several judges, lawyers, and other prominent political figures and, of course, a great many members of the Yale faculty.

Students Cause Havoc in Computer

Combined News Sources

A group of students at Gompers Secondary School in San Diego tapped into the school's computer system last month, causing all kinds of problems.

"It was funny at first when the kids changed the passwords so the teachers couldn't get into their programs in the system," said Alex Rascon, a school official. "But then they started deleting grades, altering the other kids' homework, and tampering with the teachers' files.

"These kids are whizzes—they're very bright," he went on. "Fortunately we caught it before too much damage was done. At this point it can be easily corrected."

Albert Cook, the assistant San Diego superintendent, took the sorehead approach. "We still haven't decided whether charges will be filed with the San Diego Police Department," he said.

The Person Numbers

The Associated Press

Sweden's Person Number is a 10-digit figure that tells who you are, where and when you were born, and your sex. Every computer file in the country is based on the Person Number, whether it's at a bank, a hospital, an employer, the social welfare office, or the tax authorities.

Person Numbers went into effect on January 1, 1947 and were computerized 20 years later. Recently, a government study suggested the creation of a super-databank (based on the Person Number) that the Central Bureau of Statistics could use freely. By calling up a Person Number on a terminal, the bureau would be able to find out details on everything from a person's illnesses and criminal record to his income and debts.

Critics of the plan see this as an erosion of civil liberties. One said, "The files will collect more information on a person than he can remember himself."

Furthermore...

2600 News Service

- All computers seized by the FBI last October during the Telemail raids have either been returned already or are in the process of being sent back. New developments in the case are expected shortly.
- Telenet now hangs up after 3 connection attempts, whether they're successful or not. This means that last month's article (*Hacking on Telenet*) is already slightly outdated, but only until somebody figures out a way around this latest hurdle.
- Some more signs of the divestiture—this time it's the 950 exchange. This is a universal exchange that is (or will soon be) working *everywhere*. 950-1022 and 950-1088 give alternate long distance dialtones. (The latter belongs to Skyline.) The connection is crystal clear and toll-free. Eventually, the 950 will be dropped and you will dial 10XX to make long distance calls, where XX is the carrier of your choice. You can't access 950's in other area codes.
- Eastern Airlines has changed its mind about allowing portable computers on flights, leaving only American Airlines maintaining the ban.
- 202 and 214 now have automated directory assistance too. Have you checked your area code today?

THE FIRST ATOMIC BOMB

A TRUE TALE

This story was originally related by Laura Fermi, widow of the nuclear physicist Enrico Fermi, who, along with assorted colleagues, participated in the first test bomb in the desert outside Alamogordo, New Mexico in the early morning hours of a summer day in July, 1945.

When the date had been established for the secret test, staff members from the Manhattan Project (as the secret test was known) were invited to bring their spouses to New Mexico to watch the results of the several years of research. Each staff member had been assigned specific tasks to handle while there. Generally, they acted as observers and were stationed in a circle around the perimeter of the bomb site. Enrico and Laura were stationed in an area about twenty miles to the southwest of the bomb site.

The morning came when the bomb was scheduled to be detonated in the test. Laura told it like this...

Enrico and I woke up at 3:00 am, to go to the site. The test was scheduled for 4:30 am that day, which was July 19, 1945. We drove to our post, about twenty miles from the site. It had been arranged that the nearly one hundred of us present would be located in a circle about 100 miles in circumference surrounding the bomb site. We were all to be in communication with each other over telephones, all of which were connected through the exchange in Alamogordo.

We arrived at the site at 4:15 am and almost immediately it began to rain, quite a heavy, very typical torrential downpour during the summer. We waited in our car, and at 4:30 am the time came and went, but the bomb did not go off. Enrico and I assumed it might have been postponed due to the rainstorm, but decided to check with the other staff members to see for sure. For some reason, the telephone there at the site did not seem to work; the operator would not respond. *(Note: At that time, nearly all phones in the United States, and certainly in New Mexico, were manual. No dialing of any sort was possible—you had to use the operator for everything.)*

Finally Enrico decided that we would drive into town and try to contact the others and see what went wrong. So we drove back to town, and got there about 5:15 am. The only place open at that time of night was a hotel, and we stopped in there to use a pay phone. Strangely enough, the pay phone was not working either, or at least the operator never came on the line to ask what we wanted. Enrico was quite curious about all this and decided to investigate. We went outside the hotel, and Enrico found where the telephone wires came off the pole and down into the building. He decided that we would follow the wires, so we walked down the street looking overhead at the wires on the pole as we went along. Finally, we turned down one street and saw a house. The telephone poles and wires from all directions seemed to come down to this house. There must have been hundreds of wires from telephone poles all coming down onto the side of this house and going in through an opening.

We noticed that there was a front porch light which was on. The front door was open, but there was a screen door which was closed. We went up on the front porch and looked into the house. A switchboard was there, and there were a dozen or more lights on the switchboard lit, blinking off and on as people were flashing the switch hooks on their phones trying to raise the operator. The room was just dimly lit, and near the switchboard was a sofa, and a woman was laying on the sofa sound asleep! Enrico pounded very loudly on the screen door, and shouted at the woman. Suddenly she opened her eyes and looked at him, very startled. Then she looked at the switchboard. Immediately she sprang up, dashed over to the board, sat down and began frantically answering the calls...

Without saying any more, Enrico and I left, went back to the hotel where our car was parked, and drove back to our monitoring post twenty miles out into the desert. We had been at our post only about five minutes when the explosion went off, at about 6:30 am, which was two hours behind schedule. Later, we talked to the other staff members and found that there had been some confusion because of the rain. None of them had been able to reach the others because the telephone operator had fallen asleep, and the phones were not getting answered/connected...

We on the staff all had a big laugh out of it, but nothing more was ever said or done, and I doubt to this day that that woman is even aware that the first atomic explosion in the world was delayed two hours because of her.

Amazing, but true. Alamogordo was a tiny town back in the 40's, and it's very doubtful that the night operator had ever seen so much traffic in her life as the hundred or so people all on the line at once that early morning. More than likely, the poor dear had had a very rough day the day before, in the miserable summer heat, had been unable to sleep during the day, and had come to work that night thoroughly exhausted. She probably decided that "it won't hurt just to close my eyes for a minute..." and the rest of the story is already told. After all, experience had taught her that in fact she would not usually get a dozen calls all night on her shift, and she felt relatively safe in stretching out "just for a minute".

Do you have a story about computers or phones? Send it to us! If we print it, you'll get a year's subscription to 2600! The address: 2600, Box 752, Middle Island, NY 11953.

MCI

(continued from page 2)

their offices, which takes away the task of having to dial the MCI access number. In addition, you don't have to enter an authorization code and you don't even have to have touch-tones®. You simply pick up the phone and there's your MCI dialtone! According to MCI, you have to make at least $75 worth of out-of-state calls per month for this system to pay off. Of course, you can't access operators, directory assistance, 800 numbers, and that sort of thing because 1) MCI doesn't support any of those services and 2) they're certainly not going to let you connect to something they can't charge you for. Of course, if you know what you're doing, you can route calls in such a way that numbers that aren't supposed to go through for you will work, and God knows where it finally shows up! This doesn't involve extra codes, blasting the line with tones, or anything overly suspicious. All you need is the right combination of area codes. Now this has been proven to work with MCI dedicated lines; it's rumoured to work on dial-ups as well...

Finally, MCI is starting to offer its own phone booths at airports, which we'll report on as soon as we find one. And of course, there's MCI Mail, an electronic overnight mail service started up last fall which hackers are currently probing. When we get conclusive results on that, we'll pass them along. MCI can be reached at 8006246240.

The following is a list of hosts that are accessible throu ARPANet. ARPANet connects many systems together, allowing them to se electronic mail, transfer files, and be able to work on each other computers. The network is very intricate, containing many subnet including the one below, called "MILNET", short for "Military Network That is, our military. This is a small list, encompassing approximate one twentieth the entire number of systems accessible through ARPANe Notice the PENTAGON-TAC below. This is an access point for people in t government.

Host address:	Host name:	Host type:	Operating system:
26.0.0.3	NOSC-CC	VAX-11/750	UNIX
26.2.0.3	LOGICON	PDP-11/70	UNIX
26.3.0.3	NPRDC	VAX-11/780	UNIX
26.0.0.8	NRL	VAX-11/750	UNIX
26.1.0.8	NRL-AIC	VAX-11/780	UNIX
26.2.0.8	NSWC-WO	VAX-11/750	UNIX
26.3.0.8	NRL-TOPS10	DEC-10	TOPS10
26.6.0.8	NRL-ARCTAN	PDP-11/40	RSX11
26.7.0.8	NRL-CSS	VAX-11/780	UNIX
26.1.0.13	GUNTER-ADAM	DEC-2060	TOPS20
26.3.0.13	ATC-KEES1	BURROUGHS-B/29	BTOX/UNIX
26.0.0.14	CMU-CS-B	DEC-1050	TOPS10
26.6.0.16	RIACS-ICARUS	VAX-11/730	UNIX
26.0.0.17	MITRE	C/70	UNIX
26.0.0.18	RADC-MULTICS	HONEYWELL-DPS-8/70M	MULTICS
26.3.0.18	RADC-TOPS20	DEC-2040T	TOPS20
26.5.0.18	RADC-UNIX	PDP-11/45	UNIX
26.6.0.18	GE-CRD	VAX-11/780	VMS
26.0.0.19	NBS-VMS	VAX-11/780	VMS
26.1.0.19	NBS-SDC	VAX-11/780	VMS
26.2.0.19	NBS-UNIX	VAX-11/750	UNIX
26.3.0.19	NBS-PL	PDP-11/70	UNIX
26.6.0.19	NBS-AMRF	VAX-11/780	VMS
26.7.0.19	NBS-SSI	VAX-11/750	UNIX
26.4.0.20	DCA-EMS	C/70	UNIX
26.0.0.23	USC-ECLB	DEC-1090B	TOPS20
26.3.0.23	USC-ECL	DEC-1090B	TOPS20
26.0.0.24	NADC	VAX-11/780	UNIX
26.1.0.25	DDN1	C/70	UNIX
26.0.0.26	PENTAGON-TAC	C/30	TAC
26.3.0.26	TCACCIS-CSC	VAX-11/750	VMS
26.0.0.29	BRL	PDP-11/70	UNIX
26.1.0.29	APG-1	C/70	UNIX
26.3.0.30	ATC-RAND1	BURROUGHS-B/29	BTOS/UNIX
26.0.0.33	NPS	PLURIBUS	PLI
26.3.0.33	FNOC-SECURE	PLURIBUS	PLI
26.0.0.35	NOSC-SECURE2	PLURIBUS	PLI
26.1.0.35	NOSC-TECR	VAX-11/780	VMS/EUNICE
26.3.0.35	NOSC-SECURE3	PLURIBUS	PLI
26.4.0.35	NOSC-F4	FOONLY-F4	FOONEX
26.0.0.36	COINS-TAS	PLURIBUS	PLI
26.1.0.36	HAWAII-EMH	C/70	UNIX
26.0.0.39	EDWARDS-VAX	VAX-11/782	VMS
26.1.0.39	EDWARDS-2060	DEC-2060T	TOPS20
26.1.0.45	ARDC	VAX-11/780	UNIX
26.3.0.46	OKC-UNIX	PDP-11/70	UNIX
26.1.0.48	AFWL	PDP-11/50	RSX11M
26.0.0.49	BBNB	DEC-10	TENEX

26.0.0.50	DARCOM-TEST	VAX-11/750	UNIX
26.3.0.50	LSSA-DB1	NAS3-5	MVS
26.7.0.50	ETL-AI	VAX-11/780	VMS
26.0.0.53	AFSC-AD	PDP-11/45	RSX11M
26.2.0.53	AFSC-DEV	PDP-11/44	RSX11M
26.4.0.53	NCSC	VAX-11/750	UNIX
26.5.0.53	MARTIN	PDP-11/45	RSX
26.6.0.53	EGLIN-VAX	VAX-11/780	VMS
26.2.0.54	ACC	PDP-11/70	UNIX
26.1.0.55	ANL-MCS	VAX-11/780	UNIX
26.2.0.55	COMPION-VMS	VAX-11/750	VMS
26.0.0.57	TYCHO	PDP-11/70	UNIX
26.2.0.57	MARYLAND	VAX-11/780	UNIX
26.0.0.58	NYU	VAX-11/780	UNIX
26.1.0.58	BNL	PDP-11/44	UNIX
26.3.0.60	CECOM-1	FOONLY-F4	TENEX
26.0.0.61	STL-HOST1	DEC-2040	TOPS20
26.1.0.61	ALMSA-1	VAX-11/750	UNIX
26.1.0.64	MARTIN-B	VAX-11/750	VMS
26.3.0.64	ROBINS-UNIX	PDP-11/45	UNIX
26.0.0.65	AFSC-SD	DEC-2020T	TOPS20
26.2.0.65	AEROSPACE	VAX-11/780	UNIX
26.3.0.65	MARTIN-ED	PDP-11/45	RSX11M
26.1.0.66	AFGL	PDP-11/50	RSX11M
26.3.0.66	MITRE-BEDFORD	VAX-11/780	UNIX
26.0.0.67	AFSC-HQ	DEC-2040T	TOPS20
26.1.0.73	SRI-WARF	PLURIBUS	PLI
26.4.0.73	SRI-F4	FOONLY-F4	TENEX
26.0.0.74	SIMTEL20	DEC-2040T	TOPS20
26.1.0.74	WSMR70A	C/70	UNIX
26.3.0.74	WSMR70B	C/70	UNIX
26.3.0.78	MCCLELLAN	PDP-11/70	UNIX
26.0.0.81	NEMS	VAX-11/750	UNIX
26.1.0.81	NALCON	VAX-11/750	UNIX
26.3.0.81	DTRC	VAX-11/780	UNIX
26.0.0.82	BBNCCT	C/70	UNIX
26.3.0.82	DDN2	C/70	UNIX
26.4.0.82	BBN-RSM	PLURIBUS	PLI
26.9.0.82	TEP1	C/30	
26.0.0.87	SANDIA	DEC-2060T	TOPS20
26.0.0.88	NLM-MCS	VAX-11/780	UNIX
26.0.0.90	LANL	VAX-11/750	UNIX
26.4.0.92	NAVDAF-NEWPORT	UNIVAC-1100	CMS
26.1.0.95	S1-A	FOONLY-F2	WAITS
26.2.0.95	S1-B	VAX-11/750	UNIX
26.3.0.95	S1-C	VAX-11/750	UNIX
26.2.0.97	PAXRV-NES	VAX-11/730	VMS
26.1.0.103	USC-ISIE	DEC-1090T	TOPS20
26.2.0.103	ADA-VAX	VAX-11/780	VMS
26.3.0.103	USC-ISI	DEC-1090T	TOPS20
26.1.0.104	DCEC-LSUS2	IBM-158	MVS/SP
26.4.0.104	DCEC-LSUS	IBM-158	MVS/SP
26.3.0.106	ARPA-PNG11	PDP-11/34	EPOS
26.0.0.112	STL-HOST2	BBN-C/60	UNIX
26.0.0.117	KOREA-EMH	C/70	UNIX