==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 10 of 13

```
PWN ^*^ PWN ^*^ PWN { CyberView '91 } PWN ^*^ PWN ^*^ PWN
^*^                                                   ^*^
PWN         P h r a c k   W o r l d   N e w s         PWN
^*^         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~         ^*^
PWN            Special Edition Issue Four             PWN
^*^                                                   ^*^
PWN      "The Hackers Who Came In From The Cold"      PWN
^*^                                                   ^*^
PWN                 June 21-23, 1991                  PWN
^*^                                                   ^*^
PWN             Written by Bruce Sterling             PWN
^*^                                                   ^*^
PWN ^*^ PWN ^*^ PWN { CyberView '91 } PWN ^*^ PWN ^*^ PWN
```

The Hackers Who Came In From The Cold

"Millionaries and vandals met at the computer-underground convention to discuss free information. What they found was free love."

by Bruce Sterling : bruces @ well.sf.ca.us

- -

** A slightly shorter version of this article appears in Details Magazine (October 1991, pages 94-97, 134). The Details article includes photographs of Knight Lightning, Erik Bloodaxe, Mitch Kapor, and Doc Holiday.

- -

They called it "CyberView '91." Actually, it was another "SummerCon" -- the traditional summer gathering of the American hacker underground. The organizer, 21 year old "Knight Lightning," had recently beaten a Computer Fraud and Abuse rap that might have put him in jail for thirty years. A little discretion seemed in order.

The convention hotel, a seedy but accommodating motor-inn outside the airport in St Louis, had hosted SummerCons before. Changing the name had been a good idea. If the staff were alert, and actually recognized that these were the same kids back again, things might get hairy.

The SummerCon '88 hotel was definitely out of bounds. The US Secret Service had set up shop in an informant's room that year, and videotaped the drunken antics of the now globally notorious "Legion of Doom" through a one-way mirror. The running of SummerCon '88 had constituted a major count of criminal conspiracy against young Knight Lightning, during his 1990 federal trial.

That hotel inspired sour memories. Besides, people already got plenty nervous playing "hunt the fed" at SummerCon gigs. SummerCons generally featured at least one active federal informant. Hackers and phone phreaks like to talk a lot. They talk about phones and computers -- and about each other.

For insiders, the world of computer hacking is a lot like Mexico. There's no middle class. There's a million little kids screwing around with their modems, trying to snitch long-distance phone-codes, trying to swipe pirated software -- the "kodez kidz" and "warez doodz." They're peons, "rodents." Then there's a few earnest wannabes, up-and-comers, pupils. Not many. Less of 'em every year, lately.

And then there's the heavy dudes. The players. The Legion of Doom are definitely heavy. Germany's Chaos Computer Club are very heavy, and already back out on parole after their dire flirtation with the KGB. The Masters of Destruction in New York are a pain in the ass to their rivals in the underground, but ya gotta admit they are heavy. MoD's "Phiber Optik" has almost completed his public-service sentence, too... "Phoenix" and his crowd

down in Australia used to be heavy, but nobody's heard much out of "Nom" and "Electron" since the Australian heat came down on them.

The people in Holland are very active, but somehow the Dutch hackers don't quite qualify as "heavy." Probably because computer-hacking is legal in Holland, and therefore nobody ever gets busted for it. The Dutch lack the proper bad attitude, somehow.

America's answer to the Dutch menace began arriving in a steady confusion of airport shuttle buses and college-kid decaying junkers. A software pirate, one of the more prosperous attendees, flaunted a radar-detecting black muscle-car. In some dim era before the jet age, this section of St Louis had been a mellow, fertile Samuel Clemens landscape. Waist-high summer weeds still flourished beside the four-lane highway and the airport feeder roads.

The graceless CyberView hotel had been slammed down onto this landscape as if dropped from a B-52. A small office-tower loomed in one corner beside a large parking garage. The rest was a rambling mess of long, narrow, dimly lit corridors, with a small swimming pool, a glass-fronted souvenir shop and a cheerless dining room. The hotel was clean enough, and the staff, despite provocation, proved adept at minding their own business. For their part, the hackers seemed quite fond of the place.

The term "hacker" has had a spotted history. Real "hackers," traditional "hackers," like to write software programs. They like to "grind code," plunging into its densest abstractions until the world outside the computer terminal bleaches away. Hackers tend to be portly white techies with thick fuzzy beards who talk entirely in jargon, stare into space a lot, and laugh briefly for no apparent reason. The CyberView crowd, though they call themselves "hackers," are better identified as computer intruders. They don't look, talk or act like 60s M.I.T.-style hackers.

Computer intruders of the 90s aren't stone pocket-protector techies. They're young white suburban males, and look harmless enough, but sneaky. They're much the kind of kid you might find skinny-dipping at 2AM in a backyard suburban swimming pool. The kind of kid who would freeze in the glare of the homeowner's flashlight, then frantically grab his pants and leap over the fence, leaving behind a half-empty bottle of tequila, a Metallica T-shirt, and, probably, his wallet.

One might wonder why, in the second decade of the personal-computer revolution, most computer intruders are still suburban teenage white whiz-kids. Hacking-as-computer-intrusion has been around long enough to have bred an entire generation of serious, heavy-duty adult computer-criminals. Basically, this simply hasn't occurred. Almost all computer intruders simply quit after age 22. They get bored with it, frankly. Sneaking around in other people's swimming pools simply loses its appeal. They get out of school. They get married. They buy their own swimming pools. They have to find some replica of a real life.

The Legion of Doom -- or rather, the Texas wing of LoD -- had hit Saint Louis in high style, this weekend of June 22. The Legion of Doom has been characterized as "a high-tech street gang" by the Secret Service, but this is surely one of the leakiest, goofiest and best-publicized criminal conspiracies in American history.

Not much has been heard from Legion founder "Lex Luthor" in recent years. The Legion's Atlanta wing; "Prophet," "Leftist," and "Urvile," are just now getting out of various prisons and into Georgia halfway-houses. "Mentor" got married and writes science fiction games for a living.

But "Erik Bloodaxe," "Doc Holiday," and "Malefactor" were here -- in person, and in the current issues of TIME and NEWSWEEK. CyberView offered a swell opportunity for the Texan Doomsters to announce the formation of their latest high-tech, uhm, organization, "Comsec Data Security Corporation."

Comsec boasts a corporate office in Houston, and a marketing analyst, and a full-scale corporate computer-auditing program. The Legion boys are now digital guns for hire. If you're a well-heeled company, and you can cough up per diem and air-fare, the most notorious computer-hackers in America will show

right up on your doorstep and put your digital house in order -- guaranteed.

Bloodaxe, a limber, strikingly handsome young Texan with shoulder-length blond hair, mirrored sunglasses, a tie, and a formidable gift of gab, did the talking. Before some thirty of his former peers, gathered upstairs over styrofoam coffee and canned Coke in the hotel's Mark Twain Suite, Bloodaxe sternly announced some home truths of modern computer security.

Most so-called "computer security experts" -- (Comsec's competitors) -- are overpriced con artists! They charge gullible corporations thousands of dollars a day, just to advise that management lock its doors at night and use paper shredders. Comsec Corp, on the other hand (with occasional consultant work from Messrs. "Pain Hertz" and "Prime Suspect") boasts America's most formidable pool of genuine expertise at actually breaking into computers.

Comsec, Bloodaxe continued smoothly, was not in the business of turning-in any former hacking compatriots. Just in case anybody here was, you know, worrying... On the other hand, any fool rash enough to challenge a Comsec-secured system had better be prepared for a serious hacker-to-hacker dust-up.

"Why would any company trust you?" someone asked languidly.

Malefactor, a muscular young Texan with close-cropped hair and the build of a linebacker, pointed out that, once hired, Comsec would be allowed inside the employer's computer system, and would have no reason at all to "break in." Besides, Comsec agents were to be licensed and bonded.

Bloodaxe insisted passionately that LoD were through with hacking for good. There was simply no future in it. The time had come for LoD to move on, and corporate consultation was their new frontier. (The career options of committed computer intruders are, when you come right down to it, remarkably slim.) "We don't want to be flippin' burgers or sellin' life insurance when we're thirty," Bloodaxe drawled. "And wonderin' when Tim Foley is gonna come kickin' in the door!" (Special Agent Timothy M. Foley of the US Secret Service has fully earned his reputation as the most formidable anti-hacker cop in America.)

Bloodaxe sighed wistfully. "When I look back at my life... I can see I've essentially been in school for eleven years, teaching myself to be a computer security consultant."

After a bit more grilling, Bloodaxe finally got to the core of matters. Did anybody here hate them now? he asked, almost timidly. Did people think the Legion had sold out? Nobody offered this opinion. The hackers shook their heads, they looked down at their sneakers, they had another slug of Coke. They didn't seem to see how it would make much difference, really. Not at this point.

Over half the attendees of CyberView publicly claimed to be out of the hacking game now. At least one hacker present -- (who had shown up, for some reason known only to himself, wearing a blond wig and a dime-store tiara, and was now catching flung Cheetos in his styrofoam cup) -- already made his living "consulting" for private investigators.

Almost everybody at CyberView had been busted, had their computers seized, or, had, at least, been interrogated -- and when federal police put the squeeze on a teenage hacker, he generally spills his guts.

By '87, a mere year or so after they plunged seriously into anti-hacker \033OBenforcement, the Secret Service had workable dossiers on everybody that really
mattered. By '89, they had files on practically every last soul in the American digital underground. The problem for law enforcement has never been finding out who the hackers are. The problem has been figuring out what the hell they're really up to, and, harder yet, trying to convince the public that it's actually important and dangerous to public safety.

From the point of view of hackers, the cops have been acting wacky lately. The cops, and their patrons in the telephone companies, just don't understand

the modern world of computers, and they're scared. "They think there are masterminds running spy-rings who employ us," a hacker told me. "They don't understand that we don't do this for money, we do it for power and knowledge." Telephone security people who reach out to the underground are accused of divided loyalties and fired by panicked employers. A young Missourian coolly psychoanalyzed the opposition. "They're overdependent on things they don't understand. They've surrendered their lives to computers."

"Power and knowledge" may seem odd motivations. "Money" is a lot easier to understand. There are growing armies of professional thieves who rip-off phone service for money. Hackers, though, are into, well, power and knowledge. This has made them easier to catch than the street-hustlers who steal access codes at airports. It also makes them a lot scarier.

Take the increasingly dicey problems posed by "Bulletin Board Systems." "Boards" are home computers tied to home telephone lines, that can store and transmit data over the phone -- written texts, software programs, computer games, electronic mail. Boards were invented in the late 70s, and, while the vast majority of boards are utterly harmless, some few piratical boards swiftly became the very backbone of the 80s digital underground. Over half the attendees of CyberView ran their own boards. "Knight Lightning" had run an electronic magazine, "Phrack," that appeared on many underground boards across America.

Boards are mysterious. Boards are conspiratorial. Boards have been accused of harboring: Satanists, anarchists, thieves, child pornographers, Aryan nazis, religious cultists, drug dealers -- and, of course, software pirates, phone phreaks, and hackers. Underground hacker boards were scarcely reassuring, since they often sported terrifying sci-fi heavy-metal names, like "Speed Demon Elite," "Demon Roach Underground," and "Black Ice." (Modern hacker boards tend to feature defiant titles like "Uncensored BBS," "Free Speech," and "Fifth Amendment.")

Underground boards carry stuff as vile and scary as, say, 60s-era underground newspapers -- from the time when Yippies hit Chicago and ROLLING STONE gave away free roach-clips to subscribers. "Anarchy files" are popular features on outlaw boards, detailing how to build pipe-bombs, how to make Molotovs, how to brew methedrine and LSD, how to break and enter buildings, how to blow up bridges, the easiest ways to kill someone with a single blow of a blunt object -- and these boards bug straight people a lot. Never mind that all this data is publicly available in public libraries where it is protected by the First Amendment. There is something about its being on a computer -- where any teenage geek with a modem and keyboard can read it, and print it out, and spread it around, free as air -- there is something about that, that is creepy.

"Brad" is a New Age pagan from Saint Louis who runs a service known as "WEIRDBASE," available on an international network of boards called "FidoNet." Brad was mired in an interminable scandal when his readers formed a spontaneous underground railroad to help a New Age warlock smuggle his teenage daughter out of Texas, away from his fundamentalist Christian in-laws, who were utterly convinced that he had murdered his wife and intended to sacrifice his daughter to -- Satan! The scandal made local TV in Saint Louis. Cops came around and grilled Brad. The patchouli stench of Aleister Crowley hung heavy in the air. There was just no end to the hassle.

If you're into something goofy and dubious and you have a board about it, it can mean real trouble. Science-fiction game publisher Steve Jackson had his board seized in 1990. Some cryogenics people in California, who froze a woman for post-mortem preservation before she was officially, er, "dead," had their computers seized. People who sell dope-growing equipment have had their computers seized. In 1990, boards all over America went down: Illuminati, CLLI Code, Phoenix Project, Dr. Ripco. Computers are seized as "evidence," but since they can be kept indefinitely for study by police, this veers close to confiscation and punishment without trial. One good reason why Mitchell Kapor showed up at CyberView.

Mitch Kapor was the co-inventor of the mega-selling business program LOTUS 1-2-3 and the founder of the software giant, Lotus Development Corporation. He is currently the president of a newly-formed electronic civil liberties group,

the Electronic Frontier Foundation. Kapor, now 40, customarily wears Hawaiian shirts and is your typical post-hippie cybernetic multimillionaire. He and EFF's chief legal counsel, "Johnny Mnemonic," had flown in for the gig in Kapor's private jet.

Kapor had been dragged willy-nilly into the toils of the digital underground when he received an unsolicited floppy-disk in the mail, from an outlaw group known as the "NuPrometheus League." These rascals (still not apprehended) had stolen confidential proprietary software from Apple Computer, Inc., and were distributing it far and wide in order to blow Apple's trade secrets and humiliate the company. Kapor assumed that the disk was a joke, or, more likely, a clever scheme to infect his machines with a computer virus.

But when the FBI showed up, at Apple's behest, Kapor was shocked at the extent of their naivete. Here were these well-dressed federal officials, politely "Mr. Kapor"- ing him right and left, ready to carry out a war to the knife against evil marauding "hackers." They didn't seem to grasp that "hackers" had built the entire personal computer industry. Jobs was a hacker, Wozniak too, even Bill Gates, the youngest billionaire in the history of America -- all "hackers." The new buttoned-down regime at Apple had blown its top, and as for the feds, they were willing, but clueless. Well, let's be charitable -- the feds were "cluefully challenged." "Clue-impaired." "Differently clued...."

Back in the 70s (as Kapor recited to the hushed and respectful young hackers) he himself had practiced "software piracy" -- as those activities would be known today. Of course, back then, "computer software" hadn't been a major industry -- but today, "hackers" had police after them for doing things that the industry's own pioneers had pulled routinely. Kapor was irate about this. His own personal history, the lifestyle of his pioneering youth, was being smugly written out of the historical record by the latter-day corporate androids. Why, nowadays, people even blanched when Kapor forthrightly declared that he'd done LSD in the Sixties.

Quite a few of the younger hackers grew alarmed at this admission of Kapor's, and gazed at him in wonder, as if expecting him to explode.

"The law only has sledgehammers, when what we need are parking tickets and speeding tickets," Kapor said. Anti-hacker hysteria had gripped the nation in 1990. Huge law enforcement efforts had been mounted against illusory threats. In Washington DC, on the very day when the formation of the Electronic Frontier Foundation had been announced, a Congressional committee had been formally presented with the plotline of a thriller movie -- DIE HARD II, in which hacker terrorists seize an airport computer -- as if this Hollywood fantasy posed a clear and present danger to the American republic. A similar hacker thriller, WAR GAMES, had been presented to Congress in the mid-80s. Hysteria served no one's purposes, and created a stampede of foolish and unenforceable laws likely to do more harm than good.

Kapor didn't want to "paper over the differences" between his Foundation and the underground community. In the firm opinion of EFF, intruding into computers by stealth was morally wrong. Like stealing phone service, it deserved punishment. Not draconian ruthlessness, though. Not the ruination of a youngster's entire life.

After a lively and quite serious discussion of digital free-speech issues, the entire crew went to dinner at an Italian eatery in the local mall, on Kapor's capacious charge-tab. Having said his piece and listened with care, Kapor began glancing at his watch. Back in Boston, his six-year-old son was waiting at home, with a new Macintosh computer-game to tackle. A quick phone-call got the jet warmed up, and Kapor and his lawyer split town.

With the forces of conventionality -- such as they were -- out of the picture, the Legion of Doom began to get heavily into "Mexican Flags." A Mexican Flag is a lethal, multi-layer concoction of red grenadine, white tequila and green creme-de-menthe. It is topped with a thin layer of 150 proof rum, set afire, and sucked up through straws.

The formal fire-and-straw ritual soon went by the board as things began to disintegrate. Wandering from room to room, the crowd became howlingly rowdy,

though without creating trouble, as the CyberView crowd had wisely taken over an entire wing of the hotel.

"Crimson Death," a cheerful, baby-faced young hardware expert with a pierced nose and three earrings, attempted to hack the hotel's private phone system, but only succeeded in cutting off phone service to his own room.

Somebody announced there was a cop guarding the next wing of the hotel. Mild panic ensued. Drunken hackers crowded to the window.

A gentleman slipped quietly through the door of the next wing wearing a short terrycloth bathrobe and spangled silk boxer shorts.

Spouse-swappers had taken over the neighboring wing of the hotel, and were holding a private weekend orgy. It was a St Louis swingers' group. It turned out that the cop guarding the entrance way was an off-duty swinging cop. He'd angrily threatened to clobber Doc Holiday. Another swinger almost punched-out "Bill from RNOC," whose prurient hacker curiosity, naturally, knew no bounds.

It was not much of a contest. As the weekend wore on and the booze flowed freely, the hackers slowly but thoroughly infiltrated the hapless swingers, who proved surprisingly open and tolerant. At one point, they even invited a group of hackers to join in their revels, though "they had to bring their own women."

Despite the pulverizing effects of numerous Mexican Flags, Comsec Data Security seemed to be having very little trouble on that score. They'd vanished downtown brandishing their full-color photo in TIME magazine, and returned with an impressive depth-core sample of St Louis womanhood, one of whom, in an idle moment, broke into Doc Holiday's room, emptied his wallet, and stole his Sony tape recorder and all his shirts.

Events stopped dead for the season's final episode of STAR TREK: THE NEXT GENERATION. The show passed in rapt attention -- then it was back to harassing the swingers. Bill from RNOC cunningly out-waited the swinger guards, infiltrated the building, and decorated all the closed doors with globs of mustard from a pump-bottle.

In the hungover glare of Sunday morning, a hacker proudly showed me a large handlettered placard reading PRIVATE -- STOP, which he had stolen from the unlucky swingers on his way out of their wing. Somehow, he had managed to work his way into the building, and had suavely ingratiated himself into a bedroom, where he had engaged a swinging airline ticket-agent in a long and most informative conversation about the security of airport computer terminals. The ticket agent's wife, at the time, was sprawled on the bed engaging in desultory oral sex with a third gentleman. It transpired that she herself did a lot of work on LOTUS 1-2-3. She was thrilled to hear that the program's inventor, Mitch Kapor, had been in that very hotel, that very weekend.

Mitch Kapor. Right over there? Here in St Louis? Wow.

Isn't life strange.

- -

CyberView '91 Guest List
~~~~~~~~~~~~~~~~~~~~~~~~

Those known best by handles:	Those not:
Bill From RNOC / Circuit / The Conflict / Dead Lord	Dorothy Denning
Dispater / Doc Holiday / Dr. Williams / Cheap Shades	Michael Godwin
Crimson Death / Erik Bloodaxe / Forest Ranger / Gomez	Brad Hicks
Jester Sluggo / J.R. "Bob" Dobbs / Knight Lightning	Mitch Kapor
Malefactor / Mr. Fido / Ninja Master / Pain Hertz	Bruce Sterling
Phantom Phreaker / Predat0r / Psychotic Surfer of C&P	
Racer X / Rambone / The Renegade / Seth 2600 / Taran King	
Tuc <Tuc gets his own line just because he is cool!>	
~~~~~~~~~~~~~~~~~~~~~~~~

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 11 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue XXXIII / Part One           PWN
PWN                                             PWN
PWN          Compiled by Crimson Death          PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Sir Hackalot Raided By Georgia State Police

"They were pretty pissed because they didn't find anything on me."

Those were Sir Hackalot's remarks to Crimson Death shortly after his run in with the authorities. Sir Hackalot was raided by Georgia State Police in connection with Computer Fraud. The odd thing about it is that Sir Hackalot has been inactive for over a year and no real evidence was shown against him. They just came in and took his equipment. Although Sir Hackalot was not not arrested, he was questioned about three other locals bbs users who later found themselves receiving a visit the same day. Sir Hackalot is currently waiting for his equipment to be returned.

Could this recent raid have anything to do with the infamous seizure of Jolnet Public Access Unix from Lockport, Illinois in connection with the Phrack E911 case? Sir Hackalot was a user on the system and in the mindset of today's law enforcement community, that may well be enough for them to justify their recent incursion of SH's civil rights.

Square Deal for Cable Pirates

by David Hartshorn

National Programming Service has signed an agreement with 12 programmers representing 18 channel for an early conversion package for consumers with illegally modified VideoCipher II modules. The deal will be offered only to customers who convert their modified VideoCipher II modules to VC II Plus Consumer Security Protection Program (CSPP) modules. The program will be an option to NPS' current five-service minimum purchase required for conversion customers.

Participating programmers have agreed to offer complimentary programming through the end of 1991 for conversion customers. To qualify, customers must buy an annual subscription which will start on January 1, 1992 and run though December 31, 1992. Any additional programming customers want to buy will start on the day they convert and will run for 12 consecutive months.

NPS president Mike Schroeder said the objective of the program is to get people paying legally for programming from the ranks of those who are not. If a customer keeps his modified unit, he will be spending at least $600 for a new module in late 1992, plus programming, when he will be forced to convert due to a loss of audio in his modified unit. If a customer converts now to a VC II Plus with MOM (Videopal), then the net effective cost to the customer will be only $289.55 (figuring a $105 programming credit from Videopal and about $90 complimentary programming).

Included in the deal are ABC, A&E, Bravo, CBS, Discovery Channel, Family Channel, NBC, Lifetime, Prime Network, PrimeTime 24, TNN, USA Network, WPIX, WSBK, and WWOR. The package will retail for $179.99.

Details: (800)444-3474

Clark Development Systems Gets Tough

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Crimson Death (Sysop of Free Speech BBS)

Most of you have heard of PC-Board BBS software, but what you may not have heard is what Clark Development Systems are trying to do with people running illegal copies of his software. The Following messages appeared on Salt Air BBS, which is the support BBS for PC-Board registered owners.

- -

Date: 08-19-91 (11:21) Number: 88016 of 88042
To: ALL Refer#: NONE
>From: FRED CLARK Read: HAS REPLIES
Subj: WARNING Status: PUBLIC MESSAGE
Conf: SUPPORT (1) Read Type: GENERAL (A) (+)

********** WARNING **********

Due to the extent and nature of a number of pirate PCBoard systems which have been identified around the US and Canada, we are now working closely with several other software manufacturers through the SPA (Software Publisher's Association) in order to prosecute these people. Rather than attempting to prosecute them solely through our office and attorney here in Salt Lake, we will now be taking advantage of the extensive legal resources of the SPA to investigate and shut down these systems. Since a single copyright violation will be prosecuted to the full extent of $50,000 per infringement, a number of these pirates are in for a big surprise when the FBI comes knocking on their door. Please note that the SPA works closely with the FBI in the prosecution of these individuals since their crimes are involved with trafficking over state lines.

The SPA is now working closely with us and the information we have concerning the illegal distribution of our and other software publisher's wares. Please do not allow yourself to become involved with these people as you may also be brought into any suits and judgements won against them.

We are providing this information as reference only and are not pointing a finger at any one specific person or persons who are accessing this system. This message may be freely distributed.

Fred Clark
President
Clark Development Company, Inc.

- -

Date: 08-19-91 (08:28) Number: 47213 of 47308
To: AL LAWRENCE Refer#: NONE
>From: DAVID TERRY Read: NO
Subj: BETA CODE IS NOW OFFLINE Status: RECEIVER ONLY

PLEASE NOTE! (This message is addressed to ALL!)

The beta code is now offline and may be offline for a couple of days. After finding a program which cracks PCBoard's registration code I have taken the beta code offline so that I can finish up work on the other routines I've been working on which will not be cracked so easily. I'm sorry if the removal inconveniences anyone. However, it's quite obvious that SOMEONE HERE leaked the beta code to a hacker otherwise the hacker could not have worked on breaking the registration code.

I'm sorry that the few inconsiderates have to make life difficult for the rest of you (and us). If that's the way the game is played, so be it.

P.S. -- We've found a couple of large pirate boards (who we have not notified) who should expect to see the FBI show up on their doorstep in the not too distant future. Pass the word along. If people want to play rough then we'll up the ante a bit ... getting out of jail won't be cheap!
-- --
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Seems to me they are trying to scare everyone. I think the FBI has better things to do than go around catching System Operators who didn't purchase PC-Board. At least I hope they do. First they put in a key that was needed to run the beta version of PCB and you could only get it by typing REGISTER on Salt Air, it would then encrypt your name and give you the key so you could register you beta. Expiration date were also implemented into the beta code of 14.5a, but the first day this was released on Salt Air, pirates already designed a program to make your own key with any name you wanted. It appears that with this "new" technique that Clark Systems are trying failed too. As it is cracked already also. Maybe they should be more concerned on how PC-Board functions as a BBS rather than how to make it crack-proof. As most pirate system don't run PC-Board anyway!

Georgia's New Area Code
~~~~~~~~~~~~~~~~~~~~~~~

Telephone use in Georgia has increased so rapidly -- caused by increased population and the use of services like fax machines and mobile telephones that they are running out of telephone numbers.

Southern <Fascist> Bell will establish a new area code -- 706 -- in Georgia in May 1992. The territory currently designated by the 404 area code will be split.

Customers in the Atlanta Metropolitan local calling area will continue to use the 404 area code. Customers outside the Atlanta Metropolitan toll free calling area will use the 706 area code. The 912 area code (South Georgia) will not be affected by this change.

They realize the transition to a new area code will take some getting used to. So, between May 3, 1992 and August 2, 1992, you can dial EITHER 706 or 404 to reach numbers in the new area. After August 2, 1992, the use of the 706 area code is required.

They announced the the new area code far in advance to allow customers to plan for the change.

Unplug July 20, 1991
~~~~~~

>From AT&T Newsbriefs (and contributing sources; the San Francisco Chronicle (7/20/91, A5) and the Dallas Times Herald (7/20/91, A20)

A prankster who intercepted and rerouted confidential telephone messages from voice mail machines in City Hall <of Houston, Texas> prompted officials to pull the plug on the phone system. The city purchased the high-tech telephone system in 1986 for $28 million. But officials forget to require each worker to use a password that allows only that worker to retrieve or transfer voice messages from their "phone mailboxes," said AT&T spokesman Virgil Wildey. As a result, Wildey said, someone who understands the system can transfer messages around, creating chaos.

The Bust For Red October
~~~~~~~~~~~~~~~~~~~~~~~~

By Stickman, Luis Cipher, Orion, Haywire, Sledge, and Kafka Kierkegaard

At 8:00 AM on August 7, 1991 in Walnut Creek, California the house of Steven Merenko, alias Captain Ramius, was raided by Novell attorneys occompanied by five federal marshals. All of his computer equipment was confiscated by the Novell attorneys; including disks, tape backups, and all hardware.

Novell officials had filed an affidavit in the United States District Court for the Northern District of California. They charge Merenko had illegally distributing Novell NetWare files.

A Novell investigator logged on to Merenko's BBS as a regular user 11 times over a period of a several months. He uploaded a piece of commercial
~~~~~~~~~~~~~~~~~~~~~~~~

software from another company, with the company's permission, in order to gain credibility and eventually download a file part of Novell NetWare 386 v3.11, which with a full-blown installation costs more than $10,000.

Novell issued a Civil suit against The Red October BBS, and because of that Merenko will not go to jail if he is found guilty of letting other people download any copyrighted or commercial software. The maximum penalty in a civil case as this one is $100,000 per work infringed.

The Red October BBS was THG/TSAN/NapE Site with four nodes, 4 gigabytes of hard drive space online and had been running for four years.

- -

Novell's Anti-Piracy Rampage
~~~~~~~~~~~~~~~~~~~~~~~~~~~

Novell's raid on the Red October BBS on August 7, 1991 is the latest in a two-year ongoing anti-piracy venture. In the same week as the Red October bust, the original Wishlist BBS in Redondo Beach, California was also raided. Last April (1991), Novell sued seven resellers in five states that were accused of illegally selling NetWare. In the fall of last year they seized the computer equipment of two men in Tennessee accused of reselling NetWare over BBSs. According to David Bradford, senior vice president and general counsel at Novell and chairman of the Copyright Protection Fund of the Software Publisher's Association, the crackdown on software piracy has paid off.

Lottery May Use Nintendo As Another Way To Play September 1, 1991
~~~~~~

Taken from Minneapolis Star Tribune (Section B)

"Several kinks have yet to be worked out."

Minnesota gamblers soon could be winning jackpots as early as 1993 from the comfort of their own living rooms. The state will begin testing a new system next summer that will allow gamblers to pick numbers and buy tickets at home by using a Nintendo control deck. The system, to be created by the state and Control Data Corporation, would be somewhat similar to banking with an automated teller machine card. Gamblers would use a Nintendo control deck and a state lottery cartridge. The cartridge would be connected by phone to the lottery's computer system, allowing players to pick Lotto America, Daily 3 and Gopher 5 numbers, and play the instant cash games. Players would gain access to the system by punching in personal security codes or passwords. Incorrect passwords would be rejected. Only adults would be allowed to play.

A number of kinks, including setting up a pay-in-advance system for players to draw on, computer security and adult registration, must be worked out. 32% of Minnesota households have Nintendo units. About half of those who use the units are older than 18. Those chosen to participate in the summer experiment will be given a Nintendo control deck, phone modem and lottery cartridge.

15,000 Cuckoo Letters September 8, 1991
~~~~~~~~~~~~~~~~~~~~~

Reprinted from RISKS Digest
>From: Cliff Stoll

In 1989, I wrote, "The Cuckoo's Egg", the true story of how we tracked down a computer intruder. Figuring that a few people might wish to communicate with me, I included my e-mail address in the book's forward.

To my astonishment, it became a bestseller and I've received a tidal wave of e-mail. In 2 years, about 15,000 letters have arrived over four networks (Internet, Genie, Compuserve, and AOL). This suggests that about 1 to 3 percent of readers send e-mail.

I've been amazed at the diversity of the questions and comments: ranging from comments on my use of "hacker" to improved chocolate chip cookie recipes. Surprisingly, very few flames and insulting letters arrived - a few dozen or
~~~~~~~~~~~~~~~~~~~~~

so.

I've tried to answer each letter individually; lately I've created a few macros to answer the most common questions. About 5% of my replies bounce, I wonder how many people don't get through.

I'm happy to hear from people; it's a gas to realize how far the book's reached (letters from Moscow, the South Pole, Finland, Japan, even Berkeley); but I'm going to spend more time doing astronomy and less time answering mail.

Cheers, Cliff Stoll cliff@cfa.harvard.edu
stoll@ocf.berkeley.edu

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 12 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue XXXIII / Part Two           PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Legion of Doom Goes Corporate

The following is a compilation of several articles from by Michael Alexander of ComputerWorld Magazine about Comsec Data Security, Inc.

Comsec Data Security, Inc.

Chris Goggans a/k/a Erik Bloodaxe — 60 Braeswood Square
Scott Chasin a/k/a Doc Holiday — Houston, Texas 77096
Kenyon Shulman a/k/a Malefactor — (713)721-6500
Robert Cupps - Not a former computer hacker — (713)721-6579 FAX

- -

Hackers Promote Better Image (Page 124) June 24, 1991

HOUSTON -- Three self-professed members of the Legion of Doom, one of the most notorious computer hacker groups to operate in the United States, said they now want to get paid for their skills. Along with a former securities trader, the members launched a computer security firm called Comsec Data Security that will show corporations how to keep hackers out.

"We have been in the computer security business for the last 11 years -- just on the different end of the stick," said Scott Chasin who said he once used the handle Doc Holiday as a Legion of Doom member. The group has been defunct since late last year, Chasin said.

The start-up firm plans to offer systems penetration testing, auditing, and training services as well as security products. "We have information that you can't buy in bookstores: We know why hackers hack, what motivates them, why they are curious," Chasin said.

Already, the start-up has met with considerable skepticism.

"Would I hire a safecracker to be a security guy at my bank?" asked John Blackley, information security administrator at Capitol Holding Corporation in Louisville, Kentucky. "If they stayed straight for 5 to 10 years, I might reconsider, but 12 to 18 months ago, they were hackers, and now they have to prove themselves."

"You don't hire ne'er-do-wells to come and look at your system," said Tom Peletier, an information security specialist at General Motors Corporation. "The Legion of Doom is a known anti-establishment group, and although it is good to see they have a capitalist bent, GM would not hire these people."

Comsec already has three contracts with Fortune 500 firms, Chasin said.

"I like their approach, and I am assuming they are legit," said Norman Sutton, a security consultant at Leemah Datacom Corporation in Hayward, California. His firm is close to signing a distribution pact with Comsec, Sutton said.

Federal law enforcers have described the Legion of Doom in indictments, search warrants, and other documents as a closely knit group of about 15 computer hackers whose members rerouted calls, stole and altered data and

disrupted telephone service by entering telephone switches, among other activities.

The group was founded in 1984 and has had dozens of members pass through its ranks. Approximately 12 former members have been arrested for computer hacking-related crimes; three former members are now serving jail sentences; and at least three others are under investigation. None of the Comsec founders have been charged with a computer-related crime.

(Article includes a color photograph of all four founding members of Comsec)

- -

An Offer You Could Refuse? (Page 82) July 1, 1991

Tom Peletier, an information security specialist at General Motors in Detroit, says he would never hire Comsec Data Security, a security consulting firm launched by three ex-members of the Legion of Doom. "You don't bring in an unknown commodity and give them the keys to the kingdom," Peletier said. Chris Goggans, one of Comsec's founders, retorted: "We don't have the keys to their kingdom, but I know at least four people off the top of my head that do." Comsec said it will do a free system penetration for GM just to prove the security firm's sincerity, Goggans said. "All they have to do is sign a release form saying they won't prosecute."

- -

Group Dupes Security Experts (Page 16) July 29, 1991

"Houston-Based Comsec Fools Consultants To Gather Security Information"

HOUSTON -- Computer security consultants are supposed to know better, but at least six experts acknowledged last week that they were conned. The consultants said they were the victims of a bit of social engineering by Comsec Data Security, Inc., a security consulting firm recently launched.

Comsec masqueraded as a prospective customer using the name of Landmark Graphics Corporation, a large Houston-area software publisher, to gather information on how to prepare business proposals and conduct security audits and other security industry business techniques, the consultants said.

Three of Comsec's four founders are self-professed former members of the Legion of Doom, one of the nation's most notorious hacker groups, according to law enforcers.

"In their press release, they say, 'Our firm has taken a unique approach to its sales strategy,'" said one consultant who requested anonymity, citing professional embarrassment. "Well, social engineering is certainly a unique sales strategy."

Social engineering is a technique commonly used by hackers to gather information from helpful, but unsuspecting employees that may be used to penetrate a computer system.

"They are young kids that don't know their thumbs from third base about doing business, and they are trying to glean that from everybody else," said Randy March, director of consulting at Computer Security Consultants, Inc., in Ridgefield, Connecticut.

The consultants said gathering information by posing as a prospective customer is a common ploy, but that Comsec violated accepted business ethics by posing as an actual company.

"It is a pretty significant breech of business ethics to make the misrepresentation that they did," said Hardie Morgan, chief financial officer at Landmark Graphics. "They may not be hacking anymore, but they haven't changed the way they operate."

Morgan said his firm had received seven or eight calls from security consultants who were following up on information they had sent to "Karl

Stevens," supposedly a company vice president.

SAME OLD STORY

The consultants all told Morgan the same tale: They had been contacted by "Stevens," who said he was preparing to conduct a security audit and needed information to sell the idea to upper management. "Stevens" had asked the consultants to prepare a detailed proposal outlining the steps of a security audit, pricing and other information.

The consultants had then been instructed to send the information by overnight mail to a Houston address that later proved to be the home of two of Comsec's founders. In some instances, the caller had left a telephone number that when called was found to be a constantly busy telephone company test number.

Morgan said "Stevens" had an intimate knowledge of the company's computer systems that is known only to a handful of employees. While there is no evidence that the company's systems were penetrated by outsiders, Landmark is "battering down its security hatches," Morgan said.

Posing as a prospective customer is not an uncommon way to gather competitive information, said Chris Goggans, one of Comsec's founders, who once used the handle of Erik Bloodaxe.

"Had we not been who we are, it would be a matter of no consequence," Goggans said.

"They confirm definitely that they called some of their competitors," said Michael Cash, an attorney representing Comsec. "The fact they used Landmark Graphics was an error on their part, but it was the first name that popped into their heads. They did not infiltrate Landmark Graphics in any way."

- -

"LEGION OF DOOM--INTERNET WORLD TOUR" T-SHIRTS!

Now you too can own an official Legion of Doom T-shirt. This is the same shirt that sold-out rapidly at the "Cyberview" hackers conference in St. Louis. Join the other proud owners such as award-winning author Bruce Sterling by adding this collector's item to your wardrobe. This professionally made, 100 percent cotton shirt is printed on both front and back. The front displays "Legion of Doom Internet World Tour" as well as a sword and telephone intersecting the planet earth, skull-and-crossbones style. The back displays the words "Hacking for Jesus" as well as a substantial list of "tour-stops" (internet sites) and a quote from Aleister Crowley. This T-shirt is sold only as a novelty item, and is in no way attempting to glorify computer crime.

Shirts are only $15.00, postage included! Overseas add an additional $5.00. Send check or money-order (No CODs, cash or credit cards--even if it's really your card :-) made payable to Chris Goggans to:

Chris Goggans
5300 N. Braeswood #4
Suite 181
Houston, TX 77096

Steve Jackson Games v. United States of America

Articles reprinted from Effector Online 1.04 and 1.08
May 1, 1991 / August 24, 1991

"Extending the Constitution to American Cyberspace"

To establish constitutional protection for electronic media and to obtain redress for an unlawful search, seizure, and prior restraint on publication, Steve Jackson Games and the Electronic Frontier Foundation filed a civil suit against the United States Secret Service and others.

On March 1, 1990, the United States Secret Service nearly destroyed Steve Jackson Games (SJG), an award-winning publishing business in Austin, Texas.

In an early morning raid with an unlawful and unconstitutional warrant, agents of the Secret Service conducted a search of the SJG office. When they left they took a manuscript being prepared for publication, private electronic mail, and several computers, including the hardware and software of the SJG Computer Bulletin Board System. Yet Jackson and his business were not only innocent of any crime, but never suspects in the first place. The raid had "been staged on the unfounded suspicion that somewhere in Jackson's office there "might be" a document compromising the security of the 911 telephone system.

In the months that followed, Jackson saw the business he had built up over many years dragged to the edge of bankruptcy. SJG was a successful and prestigious publisher of books and other materials used in adventure role-playing games. Jackson also operated a computer bulletin board system (BBS) to communicate with his customers and writers and obtain feedback and suggestions on new gaming ideas. The bulletin board was also the repository of private electronic mail belonging to several of its users. This private mail was seized in the raid. Despite repeated requests for the return of his manuscripts and equipment, the Secret Service has refused to comply fully.

More than a year after that raid, the Electronic Frontier Foundation, acting with SJG owner Steve Jackson, has filed a precedent setting civil suit against the United States Secret Service, Secret Service Agents Timothy Foley and Barbara Golden, Assistant United States Attorney William Cook, and Henry Kluepfel.

"This is the most important case brought to date," said EFF general counsel Mike Godwin, "to vindicate the Constitutional rights of the users of computer-based communications technology. It will establish the Constitutional dimension of electronic expression. It also will be one of the first cases that invokes the Electronic Communications Privacy Act as a shield and not as a sword -- an act that guarantees users of this digital medium the same privacy protections enjoyed by those who use the telephone and the U.S. Mail."

Commenting on the overall role of the Electronic Frontier Foundation in this case and other matters, EFF's president Mitch Kapor said, "We have been acting as an organization interested in defending the wrongly accused. But the Electronic Frontier Foundation is also going to be active in establishing broader principles. We begin with this case, where the issues are clear. But behind this specific action, the EFF also believes that it is vital that government, private entities, and individuals who have violated the Constitutional rights of individuals be held accountable for their actions. We also hope this case will help demystify the world of computer users to the general public and inform them about the potential of computer communities."

Representing Steve Jackson and the Electronic Frontier Foundation in this suit are Harvey A. Silverglate and Sharon L. Beckman of Silverglate & Good of Boston; Eric Lieberman and Nick Poser of Rabinowitz, Boudin, Standard, Krinsky & Lieberman of New York; and James George, Jr. of Graves, Dougherty, Hearon & Moody of Austin, Texas.

Copies of the complaint, the unlawful search warrant, statements by Steve Jackson and the Electronic Frontier Foundation, a legal fact sheet and other pertinent materials are available by request from the EFF.

- -

Also made available to members of the press and electronic media on request were the following statement by Mitchell Kapor and a legal fact sheet prepared by Sharon Beckman and Harvey Silverglate of Silverglate & Good, the law firm central to the filing of this lawsuit.

"Why the Electronic Frontier Foundation Is
Bringing Suit On Behalf of Steve Jackson"

With this case, the Electronic Frontier Foundation begins a new phase of affirmative legal action. We intend to fight for broad Constitutional

protection for operators and users of computer bulletin boards.

It is essential to establish the principle that computer bulletin boards and computer conferencing systems are entitled to the same First Amendment rights enjoyed by other media. It is also critical to establish that operators of bulletin boards -- whether individuals or businesses -- are not subject to unconstitutional, overbroad searches and seizures of any of the contents of their systems, including electronic mail.

The Electronic Frontier Foundation also believes that it is vital to hold government, private entities, and individuals who have violated the Constitutional rights of others accountable for their actions.

Mitchell Kapor,
President, The Electronic Frontier Foundation

- -

"Legal Fact Sheet: Steve Jackson Games v. United States Secret Service, et al"

This lawsuit seeks to vindicate the rights of a small, successful entrepreneur/publisher to conduct its entirely lawful business, free of unjustified governmental interference. It is also the goal of this litigation to firmly establish the principle that lawful activities carried out with the aid of computer technology, including computer communications and publishing, are entitled to the same constitutional protections that have long been accorded to the print medium. Computers and modems, no less than printing presses, typewriters, the mail, and telephones -being the methods selected by Americans to communicate with one another -- are all protected by our constitutional rights.

Factual Background and Parties:

Steve Jackson, of Austin, Texas, is a successful small businessman. His company, Steve Jackson Games, is an award- winning publisher of adventure games and related books and magazines. In addition to its books and magazines, SJG operates an electronic bulletin board system (the Illuminati BBS) for its customers and for others interested in adventure games and related literary genres.

Also named as plaintiffs are various users of the Illuminati BBS. The professional interests of these users range from writing to computer technology.

Although neither Jackson nor his company were suspected of any criminal activity, the company was rendered a near fatal blow on March 1, 1990, when agents of the United States Secret Service, aided by other law enforcement officials, raided its office, seizing computer equipment necessary to the operation of its publishing business. The government seized the Illuminati BBS and all of the communications stored on it, including private electronic mail, shutting down the BBS for over a month. The Secret Service also seized publications protected by the First Amendment, including drafts of the about-to-be-released role playing game book GURPS Cyberpunk. The publication of the book was substantially delayed while SJG employees rewrote it from older drafts. This fantasy game book, which one agent preposterously called "a handbook for computer crime," has since sold over 16,000 copies and been nominated for a prestigious game industry award. No evidence of criminal activity was found.

The warrant application, which remained sealed at the government's request for seven months, reveals that the agents were investigating an employee of the company whom they believed to be engaged in activity they found questionable at his home and on his own time. The warrant application further reveals not only that the Secret Service had no reason to think any evidence of criminal activity would be found at SJG, but also that the government omitted telling the Magistrate who issued the warrant that SJG was a publisher and that the contemplated raid would cause a prior restraint on constitutionally protected speech, publication, and association.

The defendants in this case are the United States Secret Service and the

individuals who, by planning and carrying out this grossly illegal search and seizure, abused the power conferred upon them by the federal government. Those individuals include Assistant United States Attorney William J. Cook, Secret Service Agents Timothy M. Foley and Barbara Golden, as well Henry M. Kluepfel of Bellcore, who actively participated in the unlawful activities as an agent of the federal government.

These defendants are the same individuals and entities responsible for the prosecution last year of electronic publisher Craig Neidorf. The government in that case charged that Neidorf's publication of materials concerning the enhanced 911 system constituted interstate transportation of stolen property. The prosecution was resolved in Neidorf's favor in July of 1990 when Neidorf demonstrated that materials he published were generally available to the public.

Legal Significance:

This case is about the constitutional and statutory rights of publishers who conduct their activities in electronic media rather than in the traditional print and hard copy media, as well as the rights of individuals and companies that use computer technology to communicate as well as to conduct personal and business affairs generally.

The government's wholly unjustified raid on SJG, and seizure of its books, magazines, and BBS, violated clearly established statutory and constitutional law, including:

- The Privacy Protection Act of 1980, which generally prohibits the government from searching the offices of publishers for work product and other documents, including materials that are electronically stored;

- The First Amendment to the U. S. Constitution, which guarantees freedom of speech, of the press and of association, and which prohibits the government from censoring publications, whether in printed or electronic media.

- The Fourth Amendment, which prohibits unreasonable governmental searches and seizures, including both general searches and searches conducted without probable cause to believe that specific evidence of criminal activity will be found at the location searched.

- The Electronic Communications Privacy Act and the Federal Wiretap statute, which together prohibit the government from seizing electronic communications without justification and proper authorization.

- -

STEVE JACKSON GAMES UPDATE: THE GOVERNMENT FILES ITS RESPONSE

After several delays, the EFF has at last received the government's response to the Steve Jackson Games lawsuit. Our attorneys are going over these documents carefully and we'll have more detailed comment on them soon.

Sharon Beckman, of Silverglate and Good, one of the leading attorneys in the case said:

> "In general, this response contains no surprises for us. Indeed, it confirms that events in this case transpired very much as we thought that they did. We continue to have a very strong case. In addition, it becomes clearer as we go forward that the Steve Jackson Games case will be a watershed piece of litigation when it comes to extending constitutional guarantees to this medium."

Feds Arrest "Logic Bomber" July 1, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~

by Michael Alexander (ComputerWorld)(Page 10)

SAN DIEGO -- Federal agents arrested a disgruntled programmer last week
~~~~~~~~~~~~~~~~~~~~~~~~~

for allegedly planting a logic bomb designed to wipe out programs and data related to the U.S. government's billion-dollar Atlas Missile program. According to law enforcers, the programmer hoped to be rehired by General Dynamics Corporation, his former employer and builder of the missile as a high-priced consultant to repair the damage.

Michael J. Lauffenburger, age 31, who is accused of planting the bomb, was arrested after a co-worker accidentally discovered the destructive program on April 10, 1991, disarmed it and alerted authorities. Lauffenburger had allegedly programmed the logic bomb to go off at 6 p.m. on May 24, 1991 during the Memorial Day holiday weekend and then self-destruct.

Lauffenburger is charged with unauthorized access of a federal-interest computer and attempted computer fraud. If convicted, he could be imprisoned for up to 10 years and fined $500,000. Lauffenburger pleaded innocent and was released on $10,000 bail.

The indictment said that while Lauffenburger was employed at the General Dynamics Space Systems Division plant in San Diego, he was the principle architect of a database program known as SAS.DB and PTP, which was used to track the availability and cost of parts used in building the Atlas missile.

On March 20, he created a program called Cleanup that, when executed, would have deleted the PTP program, deleted another set of programs used to respond to government requests for information, and then deleted itself without a trace, according to Mitchell Dembin, the assistant U.S. attorney handling the case.

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 13 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN          Issue XXXIII / Part Three          PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Pentagon Welcomes Hackers!

September 9, 1991

>From USA Today

The FBI is investigating an Israeli teen's claim that he broke into a Pentagon computer during the gulf war. An Israeli newspaper Sunday identified the hacker as Deri Shraibman, 18. He was arrested in Jerusalem Friday but released without being charged. Yedhiot Ahronot said Shraibman read secret information on the Patriot missle -- used for the first time in the war to destroy Iraq's Scud missles in midflight.

"Nowhere did it say 'no entry allowed'," Shraibman was quoted as telli police. "It just said 'Welcome.'" The Pentagon's response: It takes "computer security very seriously," spokesman Air Force Capt. Sam Grizzle said Sunday. Analysts say it isn't the first time military computers have been entered. "No system of safeguards exists ... that is 100% secure," says Alan Sabrosky, professor at Rhodes College in Memphis.

Telesphere Sued By Creditors; Forced Into Bankruptcy

Compiled from Telecom Digest (comp.dcom.telecom)

On Monday, August 19, Telesphere Communications, Inc. was sued by a group of ten creditors who claim the company best known for its 900 service isn't paying its bills. The group of creditors, all information providers using 900 lines provided through Telesphere claim they are owed two million dollars in total for services rendered through their party lines, sports reports, horoscopes, sexual conversation lines and other services. They claim Telesphere has not paid them their commissions due for several months. The group of creditors filed in U.S. Bankruptcy Court in Maryland asking that an Involuntary Chapter 7 bankruptcy (meaning, liquidation of the company and distribution of all assets to creditors) be started against Telesphere.

The company said it will fight the effort by creditors to force it into bankruptcy. A spokesperson also said the company has already settled with more than 50 percent of its information providers who are owed money. Telesphere admitted it had a serious cash flow problem, but said this was due to the large number of uncollectible bills the local telephone companies are charging back to them. When end-users of 900 services do not pay the local telco, the telco in turn does not pay the 900 carrier -- in this case Telesphere -- and the information provider is charged for the call from a reserve each is required to maintain.

But the information providers dispute the extent of the uncollectible charges. They claim Telesphere has never adequately documented the charges placed against them (the information providers) month after month. In at least one instance, an information provider filed suit against an end-user for non-payment only to find out through deposition that the user HAD paid his local telco, and the local telco HAD in turn paid Telesphere. The information providers allege in their action against the company that Telesphere was in fact paid for many items charged to them as uncollectible, "and apparently are using the money to finance other aspects of their operation at the expense of one segment of their creditors; namely the information providers..." Telesphere denied these allegations.

Formerly based here in the Chicago area (in Oak Brook, IL), Telesphere is now based in Rockville, MD.

Theft of Telephone Service From Corporations Is Surging August 28, 1991

by Edmund L. Andrews (New York Times)

"It is by far the largest segment of communications fraud," said Rami Abuhamdeh, an independent consultant and until recently executive director of the Communications Fraud Control Association in McLean, Va. "You have all this equipment just waiting to answer your calls, and it is being run by people who are not in the business of securing telecommunications."

Mitsubishi International Corp. reported losing $430,000 last summer, mostly from calls to Egypt and Pakistan. Procter & Gamble Co. lost $300,000 in 1988. The New York City Human Resources Administration lost $529,000 in 1987. And the Secret Service, which investigates such telephone crime, says it is now receiving three to four formal complaints every week, and is adding more telephone specialists.

In its only ruling on the issue thus far, the Federal Communications Commission decided in May that the long-distance carrier was entitled to collect the bill for illegal calls from the company that was victimized. In the closely watched Mitsubishi case filed in June, the company sued AT&T for $10 million in the U.S. District Court in Manhattan, arguing that not only had it made the equipment through which outsiders entered Mitsubishi's phone system, but that AT&T, the maker of the switching equipment, had also been paid to maintain the equipment.

For smaller companies, with fewer resources than Mitsubishi, the problems can be financially overwhelming. For example, WRL Group, a small software development company in Arlington, Va., found itself charged for 5,470 calls it did not make this spring after it installed a toll-free 800 telephone number and a voice mail recording system machine to receive incoming calls. Within three weeks, the intruders had run up a bill of $106,776 to US Sprint, a United Telecommunications unit.

In the past, long-distance carriers bore most of the cost, since the thefts were attributed to weaknesses in their networks. But now, the phone companies are arguing that the customers should be liable for the cost of the calls, because they failed to take proper security precautions on their equipment.

Consumertronics, a mail order company in Alamogordo, N.M., sells brochures for $29 that describe the general principles of voice mail hacking and the particular weaknesses of different models. Included in the brochure is a list of 800 numbers along with the kind of voice mail systems to which they are connected. "It's for educational purposes," said the company's owner, John Williams, adding that he accepts Mastercard and Visa. Similar insights can be obtained from "2600 Magazine", a quarterly publication devoted to telephone hacking that is published in Middle Island, N.Y.

Proctor & Gamble August 22, 1991

Compiled from Telecom Digest

On 8-12-91, the "Wall Street Journal" published a front page story on an investigation by Cincinnati police of phone records following a request by Procter & Gamble Co. to determine who might have furnished inside information to the "Wall Street Journal". The information, ostensibly published between March 1st and June 10th, 1991, prompted P&G to seek action under Ohio's Trade Secrets Law. In respect to a possible violation of this law, a Grand Jury issued a subpoena for records of certain phone calls placed to the Pittsburgh offices of the "Wall Street Journal" from the Cincinnati area, and to the residence of a "Wall Street Journal" reporter. By way of context, the Pittsburgh offices of the "Wall Street Journal" allegedly were of interest in that Journal reporter Alecia Swasy was principally responsible for covering Procter & Gamble, and worked out of the Pittsburgh office.

On 8-13-91, CompuServe subscriber Ryck Bird Lent related the Journal story to other members of CompuServe's TELECOM.ISSUES SIG. He issued the following query:

> "Presumably, the records only show that calls were placed between two numbers, there's no content available for inspection. But what if CB had voice mail services? And what if the phone number investigations lead to online service gateways (MCI MAil, CIS), are those also subject to subpoena?"

At the time of Mr. Lent's post, it was known that the "Wall Street Journal" had alleged a large amount of phone company records had been provided by Cincinnati Bell to local police. An exact figure did not appear in Lent's comments. Thus, I can't be certain if the Journal published any such specific data on 8-12-91 until I see the article in question.

On 8-14-91, the Journal published further details on the police investigation into possible violation of the Ohio Trade Secrets Law. The Journal then asserted that a Grand Jury subpoena was issued and used by the Cincinnati Police to order Cincinnati Bell to turn over phone records spanning a 15-week period of time, covering 40 million calls placed from the 655 and 257 prefixes in the 513 area code. The subpoena was issued, according to the "Wall Street Journal", only four working days after a June 10th, 1991 article on problems in P&G's food and beverage markets.

Wednesday [8-14-91], the Associated Press reported that P&G expected no charges to be filed under the police investigation into possible violations of the Ohio Trade Secrets Law. P&G spokesperson Terry Loftus was quoted to say: "It did not produce any results and is in fact winding down". Lotus went on to explain that the company happened to "conduct an internal investigation which turned up nothing. That was our first step. After we completed that internal investigation, we decided to turn it over to the Cincinnati Police Department".

Attempts to contact Gary Armstrong, the principal police officer in charge of the P&G investigation, by the Associated Press prior to 8-14-91 were unsuccessful. No one else in the Cincinnati Police Department would provide comment to AP.

On 8-15-91, the Associated Press provided a summary of what appeared in the 8-14-91 edition of the "Wall Street Journal" on the P&G investigation. In addition to AP's summary of the 8-14-91 Journal article, AP also quoted another P&G spokesperson -- Sydney McHugh. Ms. McHugh more or less repeated Loftus' 8-13-91 statement with the following comments: "We advised the local Cincinnati Police Department of the matter because we thought it was possible that a crime had been committed in violation of Ohio law. They decided to conduct an independent investigation."

Subsequent to the 8-14-91 article in the Journal, AP had once again attempted to reach Officer Gary Armstrong with no success. Prosecutor Arthur M. Ney has an unpublished home phone number and was therefore unavailable for comment on Wednesday evening [08-14-91], according to AP.

In the past few weeks, much has appeared in the press concerning allegations that P&G, a local grand jury, and/or Cincinnati Police have found a "novel" way to circumvent the First Amendment to the U.S. Constitution. In its 8-15-91 summary of the 8-14-91 Journal article, AP quoted Cincinnati attorney Robert Newman -- specializing in First Amendment issues -- as asserting: "There's no reason for the subpoena to be this broad. It's cause for alarm". Newman also offered the notion that: "P&G doesn't have to intrude in the lives of P&G employees, let alone everyone else".

The same AP story references Cincinnati's American Civil Liberties Union Regional Coordinator, Jim Rogers, similarly commenting that: "The subpoena is invasive for anyone in the 513 area code. If I called "The Wall Street Journal", what possible interest should P&G have in that?"

In a later 8-18-91 AP story, Cleveland attorney David Marburger was quoted as observing that "what is troublesome is I just wonder if a small business in Cincinnati had the same problem, would law enforcement step in and help them

out?" Marburger also added, "it's a surprise to me," referring to the nature of the police investigation.

In response, Police Commander of Criminal Investigations, Heydon Thompson, told the Cincinnati Business Courier "Procter & Gamble is a newsmaker, but that's not the reason we are conducting this investigation." P&G spokesperson Terry Loftus responded to the notion P&G had over-reacted by pointing out: "We feel we're doing what we must do, and that's protect the shareholders. And when we believe a crime has been committed, to turn that information over to the police."

Meanwhile, the {Cincinnati Post} published an editorial this past weekend -- describing the P&G request for a police investigation as "kind of like when the biggest guy in a pick-up basketball game cries foul because someone barely touches him." Finally, AP referenced what it termed "coziness" between the city of Cincinnati and P&G in its 8-18-91 piece. In order to support this notion of coziness, Cincinnati Mayor David Mann was quoted to say: "The tradition here, on anything in terms of civic or charitable initiative, is you get P&G on board and everybody else lines up." As one who lived near Cincinnati for eight years, I recall Procter & Gamble's relationship with Cincinnati as rather cozy indeed.

Hacker Charged in Australia August 13; 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~

The Associated Press reports from Melbourne that Nahshon Even-Chaim, a 20-year old computer science student, is being charged in Melbourne's Magistrates' Court on charges of gaining unauthorized access to one of CSIRO's (Australia's government research institute) computers, and 47 counts of misusing Australia's Telecom phone system for unauthorized access to computers at various US institutions, including universities, NASA, Lawrence Livermore Labs, and Execucom Systems Corp. of Austin, Texas, where it is alleged he destroyed important files, including the only inventory of the company's assets. The prosecution says that the police recorded phone conversations in which Even-Chaim described some of his activities. No plea has been entered yet in the ongoing pre-trial proceedings.

Dial-a-Pope Catching on in the U.S. August 17, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

>From the Toronto Star

The Vatican is reaching out to the world, but it looks as if Canada won't be heeding the call. In the U.S., if you dial a 900 number, you can get a daily spiritual pick-me-up from Pope John Paul II. The multilingual, Vatican -authorized service, affectionately known as Dial-a-Pope, is officially titled "Christian Messaging From the Vatican." A spokesman from Bell Canada says there is no such number in this country. But Des Burge, director of communications for the Archdiocese of Toronto, says he thinks the service, for which U.S. callers pay a fee, is a good way to help people feel more connected to the Pope. (Toronto Star)

PWN Quicknotes
~~~~~~~~~~~~~~

1. Agent Steal is sitting in a Texas jail awaiting trial for various crimes including credit card fraud and grand theft auto.

---

2. Blue Adept is under investigation for allegedly breaking into several computer systems including Georgia Tech and NASA.

---

3. Control C had his fingerprints, photographs, and a writing sample subpoenaed by a Federal Grandy Jury after Michigan Bell employees, and convicted members of the Legion of Doom (specifically The Leftist and the Urvile) gave testimony.

Control C was formerly an employee of Michigan Bell in their security
~~~~~~~~~~~~~~

department until January 1990, when he was fired about the same time as the raids took place on Knight Lightning, Phiber Optic, and several others. Control C has not been charged with a crime, but the status of the case remains uncertain.

---

4. Gail Thackeray, a special deputy attorney in Maricopa County in Arizona, has been appointed vice president at Gatekeeper Telecommunications Systems, Inc., a start-up in Dallas. Thackeray was one of the law enforcers working on Operation Sun-Devil, the much publicized state and federal crackdown on computer crime. Gatekeeper has developed a device that it claims is a foolproof defense against computer hackers. Thackeray said her leaving will have little impact on the investigation, but one law enforcer who asked not to be identified, said it is a sure sign the investigation in on the skids. (ComputerWorld, June 24, 1991, page 126)

---

5. Tales Of The Silicon Woodsman -- Larry Welz, the notorious 1960s underground cartoonist, has gone cyberpunk. He recently devoted an entire issue of his new "Cherry" comice to the adventures of a hacker who gets swallowed by her computer and hacks her way through to the Land of Woz. (ComputerWorld, July 1, 1991, page 82)

---

6. The Free Software Foundation (FSF), founded on the philosophy of free software and unrestricted access to computers has pulled some of its computers off the Internet after malicious hackers <MOD> repeatedly deleted the group's files. The FSF also closed the open accounts on the system to shut out the hackers who were using the system to ricochet into computers all over the Internet following several complaints from other Internet users. Richard Stallman, FSF director and noted old-time hacker, refused to go along with his employees -- although he did not overturn the decision -- and without password access has been regulated to using a stand-alone machine without telecom links to the outside world.
(ComputerWorld, July 15, 1991, page 82)

---

7. The heads of some Apple Macintosh user groups have received a letter from the FBI seeking their assistance in a child-kidnapping case. The FBI is querying the user group leaders to see if one of their members fits the description of a woman who is involved in a custody dispute. It's unclear why the FBI believes the fugitive is a Macintosh user.
(ComputerWorld, July 29, 1991, page 90)

---

8. Computer viruses that attack IBM PCs and compatibles are nearing a milestone of sorts. Within the next few months, the list of viruses will top 1,000 according to Klaus Brunnstein, a noted German computer virus expert. He has published a list of known malicious software for MS-DOS systems that includes 979 viruses and 19 trojans. In all, there are 998 pieces of "malware," Brunnstein said.
(ComputerWorld, July 29, 1991, page 90)

---

9. High Noon on the Electronic Frontier -- This fall the Supreme Court of the United States may rule on the appealed conviction from U.S. v. Robert Tappan Morris. You might remember that Morris is the ex-Cornell student who accidentially shut down the Internet with a worm program. Morris is also featured in the book "Cyberpunk" by Katie Hafner and John Markoff.

---

10. FBI's Computerized Criminal Histories -- There are still "major gaps in automation and record completness" in FBI and state criminal records systems, the Congressional Office of Technology has reported in a study on "Automated Record Checks of Firearm Purchasers: Issues and Options." In the report, OTA estimates that a system for complete and accurate "instant" name checks of state and federal criminal history records when a person buys a firearm would take several years and cost $200-$300 million. The FBI is still receiving dispositions (conviction, dismissal, not guilty, etc.) on only half of the 17,000 arrest records it enters into its system

each day. Thus, "about half the arrests in the FBI's criminal history files ("Interstate Ident-ification Index" -- or "Triple I") are missing dispositions. The FBI finds it difficult to get these dispositions." The OTA said that Virginia has the closest thing to an instant records chck for gun purchasers. For every 100 purchasers, 94 are approved within 90 seconds, but of the six who are disapproved, four or five prove to be based on bad information (a mix-up in names, a felony arrest that did not result in conviction, or a misdemeanor conviction that is not disqualifying for gun ownership) (62 pages, $3 from OTA, Washington, D.C. 20510-8025, 202/224-9241, or U.S. Government Printing Office, Stock No.052-003-01247-2, Washington, D.C. 20402-9325, 202/783-3238).
(Privacy Journal, August 1991, page 3)

- - - -

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 1 of 13

Issue XXXIII Index

P H R A C K 3 3

September 15, 1991

~Technology for Survival~

On December 24, 1989, Taran King and I released the 30th issue of Phrack and began to prepare for the new decade. The future of Phrack seemed bright and full of great potential. A few weeks later, Phrack was shut down by the United States Secret Service as part of a large scale attack on the world famous hacking group, the Legion of Doom.

The legend of Phrack died... or did it? Several months later, a newsletter called Phrack and listed as issue 31 appeared under the editorship of Doc Holiday. Of course it was not the original Doc Holiday from Tennessee, but instead one of the founding members of Comsec Data Security, Scott Chasin. It may have called itself Phrack, but it wasn't.

On November 17, 1990, another attempt was made to resurrect Phrack. Crimson Death and Doc Holiday were back to try again, this time calling their product "Phrack Classic." That issue was not absolutely terrible, but the tone behind the articles was misplaced. The introduction itself showed a lack of responsibility and maturity at a time when it was needed most. To complicate matters, Crimson Death failed to produce another issue of Phrack Classic until September 1, 1991, almost 10 months later. This lack of predictability and continuity has become too much of a burden on the hacker community.

I am proud to announce that a new era of Phrack has thus begun. The new Phrack is listed as Phrack 33 despite the Phrack Classic issue of September 1st. To help ease the transition, the new Phrack staff has borrowed files from the PC 33 so they are chronicled correctly. Even Crimson Death has agreed that it is once again time to pass the torch.

The new Phrack editor is Dispater and other people involved in working on this issue include Ninja Master, Circuit, and The Not. Of course they are always looking for help and good articles. The new Phrack will be run slightly different than the old. The kind of information likely to be found in Phrack will not change drastically, but Phrack is intended for people to learn about the types of vulnerabilities in systems that some hackers might be likely to exploit. If you are concerned about your system being disrupted by computer intruders, allow the hackers who write for Phrack to point out some flaws you might wish to correct. Phrack still strongly supports the free exchange of information and will never participate in censorship except when it would be necessary to protect an individual's personal privacy. There is a delicate balance to be found in this arena and hopefully it can be discovered. Be patient and do not judge the new Phrack without really giving it a chance to work out the bugs.

I've said my piece, now it is time to turn over the reigns to Dispater. I wish him the best of luck, and for you the readers, I hope you enjoy the new Phrack as much as you have enjoyed the previous.

Sincerely,

:Knight Lightning (kl@STORMKING.COM)

- -

A few words from Dispater:

Phrack will be introducing a new regular column similar to a "letters to the editor" section. It will be featured as the second file in each issue,

beginning with issue 34. Any questions, comments, or problems that you the reader would like to air with Phrack publically will be answered there.

I'd really like to thank Crimson Death for his cooperation in helping us get Phrack started again. He is one of the coolest hackers I have met. We could not have done it without him. Other important people to mention are the The Monk and Twisted Pair.

Thanks to Tuc, Phrack will soon be using an Internet listserver. See Phrack 34 for more details. Phrack will also be found on various anonymous FTP sites across the Internet, including the anonymous ftp site at EFF.ORG, a Unix machine operated by the Electronic Frontier Foundation, an organization to which we at Phrack respect. It can also be found at the anonymous ftp site at CS.WIDENER.EDU

Off the Internet, we hope to establish several bulletin board systems as archive sites including Digital Underground (812)941-9427, which is operated by The Not. Submissions or letters to Phrack can be made there or on the Internet by sending mail to "phracksub@STORMKING.COM".

The new format will be a little more professional. This is because I have no desire to find myself in court one day like Knight Lightning. However, I have no intention of turning Phrack Inc. into some dry industry journal. Keeping things lite and entertaining is one of the ways that I was attracted to Phrack. I think most people will agree that there is a balance of fun and business to be maintained. If this balance is not met, you the reader, will get bored and so will I!

Check out Phrack World News Special Edition IV for the "details" on CyberView '91, the SummerCon-ference hosted by Knight Lightning that took place this past summer in St. Louis, Missouri.

Phrack XXXIII Table of Contents

1. Introduction to Phrack 33 by Knight Lightning and Dispater
2. Phrack Profile of Shooting Shark by Crimson Death
3. A Hacker's Guide to the Internet by The Gatsby
4. FEDIX On-Line Information Service by Fedix Upix
5. LATA Referance List by Infinite Loop
6. International Toll Free Code List by The Trunk Terminator
7. Phreaking in Germany by Ninja Master
8. TCP/IP: A Tutorial Part 1 of 2 by The Not
9. A REAL Functioning RED BOX Schematic by J.R."Bob" Dobbs
10. Phrack World News Special Edition IV (CyberView '91) by Bruce Sterling
11. PWN/Part01 by Crimson Death
12. PWN/Part02 by Dispater
13. PWN/Part03 by Dispater

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 2 of 13

-*[P H R A C K XXXIII P R O P H I L E]*-

-=>[by Crimson Death]<=-

This issue Phrack Profile features a hacker familiar to most of you. His informative files in Phrack and the Legion of Doom Technical Journals created a stampede of wanna-be Unix hackers. Your friend and mine...

Shooting Shark

Personal

Handle:	Shooting Shark
Call him:	'Shark'
Past handles:	None
Handle origin:	It's the title of the 3rd song on "Revolution By Night," which many consider to be Blue Oyster Cult's last good album.
Date of Birth:	11/25/66
Age at current date:	24
Approximate Location:	San Francisco Bay Area.
Height:	5'10"
Weight:	150 lbs.
Eye color:	Hazel
Hair Color:	Dark Brown
Computers:	First: Apple //e. Presently: ALR Business V EISA 386/33.

The Story of my Hacking Career

In 1984 I was lucky enough to be a Senior at a high school that had one of the pilot "Advanced Placement Computer Science" classes. I didn't know much about computers at the time, but I had a strong interest, so I signed up. "Advanced Placement Computer Science" meant programming in Pascal using the UCSD P-System on the newly-released Apple //e. I wasn't too crazy about programming in Pascal -- does ANYBODY really like Pascal? -- but I did enjoy the software piracy sessions that the class had after school and, much of the time, during class when the Instructor was lecturing about DO WHILE loops or something equally fascinating. Some of our favorite games at the time were ZORK II and what I still consider to be the best Apple II game ever, RESCUE RAIDERS. A few months into the school year, I somehow convinced my mother to buy me my very own Apple //e, with an entire 64K of RAM, a monochrome monitor, and a floppy drive. The first low-cost hard drive for the Apple II, the Sider, was $700 for 10Mb at the time, so it was out of the question.

Now at about this time, Coleco was touting their Adam add-on to the ColecoVision game unit, and they had these great guilt-inducing advertisements that had copy something like this:

TEACHER: "I want to talk to you about Billy. He's not doing very well in school. He just doesn't seem to understand new concepts as well as the other kids. All he does is sit there and pick his nose."

CONCERNED FATHER: "Well, golly, I just don't know what to do. It's probably probably because his mother drank so much when she was pregnant."

TEACHER: "Have you considered getting Billy a computer?"

And of course the next scene showed little Billy inserting a tape cartridge into his new Adam and pecking his way to higher grades.

Such was not the case with me when I got MY computer. All I did was go

home after school and play "Wizardry." I stopped doing homework and I failed 3 out of 6 classes my last semester of my Senior year of high school. Luckily enough, I had already been accepted to the local state University, so it didn't really matter. Shortly before graduating, I took the AP Computer Science test and got the minimum passing score. (I didn't feel so bad when Sir Francis Drake later told me that he failed it. Then again, he completed all the questions in BASIC.)

Worse yet, "Wargames" came out around this time. I'll admit it, my interest in hacking was largely influenced by that film.

Shortly after I (barely) graduated from high school, I saved up my money and bought a (get this) Hayes MicroModem //e. It was only something like $250 and I was in 300 baud heaven. I started calling the local "use your real name" BBSs and shortly graduated to the various small-time hacker BBSs. Note that 90% of the BBSs at this time were running on Apples using Networks, GBBS or some other variant. Few were faster than 300 baud. It was on one of these Apple Networks BBSs that I noticed some users talking about these mysterious numbers called "800 extenders." I innocently inquired as to what these were, and got a reply from Elric of Imrryr. He explained that all I needed to do was dial an 800 number, enter a six-digit code, and then I could call anywhere I wanted for FREE! It was the most amazing thing. So, I picked a handle, and began calling systems like Sherwood Forest II and Sherwood Forest III, OSUNY, and PloverNet. At their height, you could call any of these systems and read dozens of new messages containing lots of new Sprint and extender codes EVERY DAY. It was great! I kept pestering my mentor, Elric, and despite his undoubted annoyance with my stupid questions, we remained friends. By this time, I realized that my Hayes MicroModem //e was just not where it was at, and saved up the $400 to buy a Novation Apple Cat 300, the most awesomest modem of its day. This baby had a sound generation chip which could be used to generate speech, and more importantly, DTMF and 2600Hz tones. Stupidly enough, I began blue boxing. Ironically, at this time I was living in the very town that Steve Wozniak and Steve Jobs had gotten busted in for boxing ten years previously.

And THEN I started college. I probably would have remained a two-bit Apple hacker (instead of what I am today, a two-bit IBM hacker) to this day if a friend hadn't told me that it was easy to hack into the school's new Pyramid 90x, a "super mini" that ran a BSD 4.2 variant. "The professor for the C class has created a bunch of accounts, sequentially numbered, all with the same default password," he told me. "Just keep trying them until you get an account that hasn't been used by a student yet!" I snagged an account which I still use to this day, seven years later.

At about this time, I called The Matrix, run by Dr. Strangelove. This was my first experience with Ken's FORUM-PC BBS software. Dr. Strangelove was a great guy, even though he looks somewhat like a wood mouse (and I mean that in the nicest possible way). DSL helped me build my first XT clone for a total cost of about $400. He even GAVE me a lot of the components I needed, like a CGA card and a keyboard.

Shortly after that, The Matrix went down and was quickly replaced by IDI, run by Aiken Drum. It is here that I met Sir Francis Drake. Shortly after THAT, IDI went down and was quickly replaced by Lunatic Labs Unltd, run by my old friend The Mad Alchemist. TMA lived within walking distance of my house, so I called LunaLabs quite a bit. LunaLabs later became the home base of Phrack for a few issues when Knight Lightning and Taran King gave it upon entering their freshman year of college.

So during this time I just got really into Unix and started writing files for Phrack. I wrote about six articles for Phrack and then one for the 2nd LOD Technical Journal, which featured a brute-force password hacker. I know, that sounds archaic, but this was back in 1984, and I was actually one of the few people in the hacker community that knew quite a bit about Unix. I've been told by several people that it was my LOD TJ article that got *them* into Unix hacking (shucks). I also wrote the original Unix Nasties article for Phrack, and on two occasions, when I was later heavily into massive Internet node hopping, I would get into a virgin system at some backwoods college like MIT and find *my file* in somebody's directory.

During 1987, I got a letter from the local FBI office. It was addressed

to my real name and asked for any information I might wish to provide on a break-in in San Diego. Of course I declined, but they kept sending me more letters. Now that I was 18 years old I decided to stop doing illegal things. I know..."what a weenie." So Lunatic Labs, now being run by The Mad Alchemist, became my exclusive haunt because it was a local board. When Elric and Sir Francis Drake took over the editorship of Phrack for a few issues, I wrote all their intro files.

When my computer broke I let those days just fade away behind me. Occasionally, old associates would manage to find me and call me voice, much to my surprise. Somebody called me once and told me an account had been created for me on a BBS called "Catch 22," a system that must have been too good to last. I think I called it twice before it went down. Most recently, Crimson Death called me, asked me to write a Profile, and here we are.

What I'm Doing Now

After two years in the Computer Science program in college, I switched my major to Theater Arts for three reasons:

1) Theater Arts people were generally nicer people;
2) Most CS students were just too geeky for me (note I said "most"); and,
3) I just couldn't manage to pass Calculus III!

I graduated last year with a BA in Theater Arts, and like all newly graduated Theater majors, started practicing my lines, such as "Do you want fries with that?" and "Can I tell you about today's special?" However, I managed to have the amazing luck of getting a job in upper management at one of the west coast's most famous IBM video graphics card manufacturers. My position lets me play with a lot of different toys like AutoDesk 3D Studio and 24-bit frame buffers. A 24-bit image I created was featured on the cover of the November 1990 issue of Presentation Products magazine. For a while I was the system administrator of the company's Unix system, with an IP address and netnews and the whole works. Now I'm running the company's two-line BBS -- if you can figure out what company I work for, give it a call and leave me some mail sometime. I'm also into MIDI, and I've set my mother up with a nice little studio including a Tascam Porta One and a Roland MT-32. I was an extra in the films "Patty Hearst" (with The $muggler) and "The Doors" (for which I put in a 22-hour day at the Warfield Theater in San Francisco for a concert scene that WAS CUT FROM THE #*%& FILM) and I look forward to working on more films in a capacity that does not require me to wear bell-bottoms. I've also acted in local college theater and I'll be directing a full-length production at a local community theater next year. I like to consider myself a well-rounded person.

Oh yeah. I also got married last October.

People I Have Known

Elric of Imrryr -- My true mentor. He got me into the business. Too bad he moved to Los Angeles.

Shadow 2600 -- Known to some as David Flory, may he rest in peace. Early in my career he mentioned me and listed me as a collaborator for a 2600 article. That was the first time I saw my name in print.

Oryan QUEST -- After I had my first Phrack article published, he started calling me (he lived about 20 miles away at the time). He would just call me and give me c0deZ like he was trying to impress me or something. I don't know why he needed me for his own personal validation. I was one of the first people to see through him and I realized early on that he was a pathological liar. Later on he lied about me on a BBS and got me kicked off, because the Sysop though he was this great guy. Sheesh.

Sir Francis Drake -- Certainly one of the more unique people I've met. He printed a really crappy two-part fiction story I wrote in his WORM magazine. Shortly after that the magazine folded; I think there's a connection.

David Lightman -- Never met him, but he used to share my Unix account at

school.

The Disk Jockey -- He pulled a TRW report on the woman that I later ended up marrying. Incidentally, he can be seen playing basketball in the background in one scene of the film "Hoosiers."

Lex Luthor -- I have to respect somebody who would first publish my article in LOD TJ and then call me up for no reason a year later and give me his private Tymnet outdial code.

Dr. Strangelove -- He runs a really cool BBS called JUST SAY YES. Call it at (415) 922-2008. DSL is probably singularly responsible for getting me into IBM clones, which in turn got me my job (how many Apple // programmers are they hiring nowadays?).

BBSs
~~~

Sherwood Forest II and III, OSUNY -- I just thought they were the greatest systems ever.

Pirate's Bay -- Run by Mr. KRACK-MAN, who considered himself the greatest Apple pirate that ever lived. It's still up, for all I know.

The 2600 Magazine BBS -- Run on a piece of Apple BBS software called TBBS. It is there that I met David Flory.

The Police Station -- Remember THAT one?

The Matrix, IDI, Lunatic Labs -- Three great Bay Area Forum-PC boards.

Catch-22 -- 25 Users, No Waiting!

And, of course, net.telecom (the original), comp.risks, rec.arts.startrek...

Memories
~~~~~~~~

Remember Alliance Teleconferencing? Nothing like putting the receiver down to go get something to eat, forgetting about it, coming back in 24 hours, and finding the conference still going on.

Playing Wizardry and Rescue Raiders on my Apple //e until I lost the feeling in my fingers...

Carding 13 child-sized Garfield sleeping bags to people I didn't particularly care for in high school...

Calling Canadian DA Ops and playing a 2600Hz tone for them was always fun.

Trashing all the local COs with The Mad Alchemist...

My brush with greatness: I was riding BART home from school one night a few years ago when Steve Wozniak got onto my car with two of his kids. He was taking them to a Warriors game. I was the only person in the car that recognized him. He signed a copy of BYTE that I happened to have on me and we talked about his new venture, CL-9, the universal remote controller. (Do you know anybody who ever BOUGHT one of those?)

....And now, for the question
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

"Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks?"

Back in my Apple pirating days, I met quite a few young men who were definitely members of the Order of the Geek. However, I can count the number of true phreaks/hackers I have met personally on one hand. None of them are people I'd consider geeks, nerds, spazzes, dorks, etc. They're all people who live on the fringe and do things a bit differently -- how many LEGAL people do you know that have a nose ring? -- but they're all people I've respected. Well, let me take back what I just said. Dr. Strangelove looks kinda geeky in
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

my opinion (my mother thinks he's cute, but then again she said that Sir Francis Drake is "cute" and when I told him that it bothered him to no end), but I consider him a good friend and a generally k-kool d00d. (I'm sure I'll be getting a voice call from him on that one...) The only phreak that I've ever taken a genuine disliking to was Oryan QUEST, but that was only because he was a pathological liar and a pest. Who knows, he might be a nice person now, so no offense intended, especially if he knows my home address.

So, Anyway...

-> Thanks for your time Shooting Shark.

Crimson Death

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 3 of 13

A Hacker's Guide to the Internet

By The Gatsby

Version 2.00 / AXiS / July 7, 1991

---

1 Index

Part:	Title:
1	Index
2	Introduction
3	Glossary, Acronyms, and Abbreviations
4	What is the Internet?
5	Where You Can Access The Internet
6	TAC
7	Basic Commands
a	TELNET command
b	ftp ANONYMOUS to a Remote Site
c	Basic How to tftp the Files
d	Basic Fingering
8	Networks
9	Internet Protocols
10	Host Names and Addresses

2 Introduction

The original release of this informative file was in an IRG newsletter, but it had some errors that I wanted to correct. I have also added more technical information.

This file is intended for the newcomer to Internet and people (like me) who are not enrolled at a university with Internet access. It covers the basic commands, the use of Internet, and some tips for hacking through Internet. There is no MAGICAL way to hacking a UNIX system. If you have any questions, I can be reached on a number of boards.

- The Crypt - - 619/457+1836 - - Call today -
- Land of Karrus - - 215/948+2132 -
- Insanity Lane - - 619/591+4974 -
- Apocalypse NOW - - 2o6/838+6435 - <*> AXiS World HQ <*>

Mail me on the Internet: gats@ryptyde.cts.com
bbs.gatsby@spies.com

The Gatsby

*** Special Thanks go to Haywire (a/k/a Insanity: SysOp of Insanity Lane), Doctor Dissector, and all the members of AXiS.

3 Glossary, Acronyms, and Abbreviations

ACSE - Association Control Service Element, this is used with ISO to help manage associations.

ARP - Address Resolution Protocol, this is used to translate IP protocol to Ethernet Address.

ARPA - Defense Advanced Research Project Agency

ARPANET - Defense Advanced Research Project Agency or ARPA. This is an experimental PSN which is still a sub network in the Internet.

CCITT - International Telegraph and Telephone Consultative Committee is a

international committee that sets standard. I wish they would set a standard for the way they present their name!

CERT - Computer Emergency Response Team, they are responsible for coordinating many security incident response efforts. They have real nice reports on "holes" in various UNIX strands, which you should get because they are very informative.

CMIP - Common Management Information Protocol, this is a new HIGH level protocol.

CLNP - Connection Less Network Protocol is OSI equivalent to Internet IP

DARPA - Defence Advanced Research Project Agency. See ARPANET

DDN - Defence Data Network

driver - a program (or software) that communicates with the network itself, examples are TELNET, FTP, RLOGON, etc.

ftp - File Transfer Protocol, this is used to copy files from one host to another.

FQDN - Fully Qualified Domain Name, the complete hostname that reflects the domains of which the host is a part.

Gateway - Computer that interconnects networks.

Host - Computer that is connected to a PSN.

Hostname - Name that officially identifies each computer attached internetwork.

Internet - The specific IP-base internetwork.

IP - Internet Protocol which is the standard that allows dissimilar host to connect.

ICMP - Internet Control Message Protocol is used for error messages for the TCP/IP.

LAN - Local Area Network

MAN - Metropolitan Area Network

MILNET - DDN unclassified operational military network.

NCP - Network Control Protocol, the official network protocol from 1970 until 1982.

NIC - DDN Network Information Center

NUA - Network User Address

OSI - Open System Interconnection. An international standardization program facilitate to communications among computers of different makes and models.

Protocol - The rules for communication between hosts, controlling the information by making it orderly.

PSN - Packet Switched Network

RFC - Request For Comments, is technical files about Internet protocols one can access these from anonymous ftp at NIC.DDN.MIL.

ROSE - Remote Operations Service Element, this is a protocol that is used along with OSI applications.

TAC - Terminal Access Controller; a computer that allow direct access to Internet.

TCP - Transmission Control Protocol

TELNET - Protocol for opening a transparent connection to a distant host.

tftp - Trivial File Transfer Protocol, one way to transfer data from one host to another.

UDP - User Datagram _Protocol

Unix - This is copyrighted by AT&T, but I use it to cover all the look-alike Unix systems, which you will run into more often.

UUCP - Unix-to-Unix Copy Program, this protocol allows UNIX file transfers. This uses phone lines using its own protocol, X.25 and TCP/IP. This protocol also exist for VMS and MS-DOS.

uucp - uucp when in lower case refers to the UNIX command uucp. For more information on uucp read files by The Mentor in the Legion of Doom Technical Journals.

WAN - Wide Area Network

X.25 - CCITTs standard protocol that rules the interconnection of two hosts.

In this file I have used several special charters to signify certain things. Here is the key;

* - Buffed from UNIX itself. You will find this on the left side of the margin. This is normally "how to do" or just "examples" of what to do when using Internet.

- This means these are commands, or something that must be typed in.

4 What is the Internet?

To understand the Internet you must first know what it is. The Internet is a group of various networks, ARPANET (an experimental WAN) was the first. ARPANET started in 1969, this experimental PSN used Network Control Protocol (NCP). NCP was the official protocol from 1970 until 1982 of the Internet (at this time also known as DARPA Internet or ARPA Internet). In the early 80's DARPA developed the Transmission Control Protocol/Internet Protocol which is the official protocol today, but much more on this later. Due to this fact, in 1983 ARPANet split into two networks, MILNET and ARPANET (both are still part of the DDN).

The expansion of Local Area Networks (LAN) and Wide Area Networks (WAN) helped make the Internet connecting 2,000+ networks strong. The networks include NSFNET, MILNET, NSN, ESnet and CSNET. Though the largest part of the Internet is in the United States, the Internet still connects the TCP/IP networks in Europe, Japan, Australia, Canada, and Mexico.

5 Where You Can Access Internet

Internet is most likely to be found on Local Area Networks or LANs and Wide Area networks or WANs. LANs are defined as networks permitting the interconnection and intercommunication of a group of computers, primarily for the sharing of resources such as data storage device and printers. LANs cover a short distance (less than a mile) and are almost always within a single building complex. WANs are networks which have been designed to carry data calls over long distances (many hundreds of miles). You can also access Internet through TymNet or Telenet via gateway. You'll have to find your own NUAs though.

6 TAC

TAC (terminal access controller) is another way to access Internet. This is just dial-up terminal to a terminal access controller. You will need to get a password and an account. TAC has direct access to MILNET. One example of a TAC dialup is (800)368-2217, but there are several out there to be found. In fact, CERT has a report circulating about people attempting to find these dialups through social engineering.

If you want the TAC manual you can write a letter to:

Defense Communications Agency
Attn: Code BIAR
Washington, DC 2o3o5-2ooo

Be sure to write that you want the TAC User Guide, 310-p70-74.

In order to logon, you will need a TAC Access Card. You would probably get it from the DDN NIC. Here is a sample logon:

```
Use Control-Q for help...

*
* PVC-TAC 111: 01                \ TAC uses to this to identify itself
* @ #o 124.32.5.82                \ Use ``O'' for open and the internet
*                                 / address which yea want to call.
*
* TAC Userid: #THE.GATSBY
* Access Code: #10kgb0124
* Login OK
* TCP trying...Open
*
*
```

7 Basic Commands

a: Basic TELNET Commands

Situation: You have an account on a UNIX system that is a host on Internet. Now you can access the entire world! Once the UNIX system you should see a prompt, which can look like a '$' or '%' (it also depends on what shell you are in and the type of Unix system). At the prompt you can do all the normal UNIX commands, but when on a Internet host you can type 'telnet' which will bring you to the 'telnet' prompt.

```
*
* $ #telnet
* ^   ^
  |   |
  |  the command that will bring you to the telnet prompt
  |
  a normal UNIX prompt
```

You should get this:

```
*
* telnet>
*
```

At this prompt you will have a whole different set of commands which are as follows (This comes from UCSD, so it may vary from place to place).

```
*
* telnet> #help
*
* close           close current connection
* display         display operating parameters
* open            connect to a site
* quit            exit telnet
* send            transmit special character
* set             set operating parameters
* status          print status information
* toggle          toggle operating parameters
* ?               to see what you are looking at now
*
```

close - this command is used to 'close' a connection, when multitasking or jumping between systems.

display - this set the display setting, commands for this are as follow.

```
^E    echo.
^]    escape.
^H    erase.
^O    flushoutput.
^C    interrupt.
^U    kill.
^\    quit.
^D    eof.
```

open - type 'open [host]' to connect to a system

```
*
* $ #telnet ucsd.edu
*
```

or

```
*
* telnet> #open 125.24.64.32.1
*
```

quit - to get out of telnet and back to UNIX

```
send   - send files
set    - set
echo   - character to toggle local echoing on/off
escape - character to escape back to telnet command mode
```

The following need 'localchars' to be toggled:

```
erase         -  character to cause an Erase Character
flushoutput   -  character to cause an Abort Output
interrupt     -  character to cause an Interrupt Process
kill          -  character to cause an Erase Line
quit          -  character to cause a Break
eof           -  character to cause an EOF
?             -  display help information
```

b: ftp ANONYMOUS to a remote site

ftp or file transfer protocol is used to copy files from a remote host to the one that you are on. You can copy anything. Security has really clamped down on the passwd file, but it will still work here and there (always worth a shot).

This could be useful when you see a Internet CuD (Computer Underground Digest) site that accepts a anonymous ftps, and you want to read the CuDs, but do not feel like wasting your time on boards downloading them. The best way to start out is to ftp a directory to see what you are getting.

Example: The CuD archive site has an Internet address of 192.55.239.132 and my account name is "gats".

```
*
* $ #ftp
* ^  ^
  |  |
  | ftp command
  |
 UNIX prompt

*
* ftp> #open 192.55.239.132
* Connected to 192.55.239.132
* 220 192.55.239.132 FTP Server (sometimes the date, etc)
* Name (192.55.239.132:gats): #anonymous
*             ^          ^         ^
              |          |         |
              |          |       This is where you type 'anonymous' unless
              |          |     you have a account on 192.55.239.132.
              |          |
              |        This is the name of my account or [from]
              |
            This is the Internet address or [to]
*
* Password: #gats
*            ^
             |
            For this just type your username or anything you feel like typing
            in at that time.  It doesn't matter.

*
* % ftp 192.55.239.132
* Connected to 192.55.239.132
* ftp> #ls
*       ^
        |
       You are connected now, thus you can ls it.
```

Just move around like you would in a normal unix system. Most of the commands still apply on this connection. Here is a example of me getting a

```
copy of the Electronic Frontier Foundation's Effector (issue 1.04) from
Internet address 192.55.239.132.

*
* % #ftp
* ftp> #open 128.135.12.60
* Trying 128.135.12.60...
* 220 chsun1 FTP server (SunOS 4.1) ready.
* Name (128.135.12.60:gatsby): anonymous
* 331 Guest login ok, send ident as password.
* Password: #gatsby
* 230 Guest login ok, access restrictions apply.
* ftp> #ls
* 200 PORT command successful.
* 150 ASCII data connection for /bin/ls (132.239.13.10,4781) * (0 bytes).
* .hushlogin
* bin
* dev
* etc
* pub
* usr
* README
* 226 ASCII Transfer complete.
* 37 bytes received in 0.038 seconds (0.96 Kbytes/s)
* ftp>

     ____________________________________________________________________
     |
     |  This is where you can try to 'cd' the "etc" dir or just 'get'
     |  /etc/passwd, but grabbing the passwd file this way is a dieing art.
     |____________________________________________________________________

* ftp> #cd pub
* 200 PORT command successful.
* ftp> #ls
* ceremony
* cud
* dos
* eff
* incoming
* united
* unix
* vax
* 226 ASCII Transfer cmplete.
* 62 bytes received in 1.1 seconds (0.054 Kbytes/s)
* ftp> #cd eff
* 250 CWD command successful.
* ftp> #ls
* 200 PORT command successful.
* 150 ASCII data connection for /bin/ls (132.239.13.10,4805) (0 bytes).
* Index
* eff.brief
* eff.info
* eff.paper
* eff1.00
* eff1.01
* eff1.02
* eff1.03
* eff1.04
* eff1.05
* realtime.1
* 226 ASCII Transfer complete.
* 105 bytes received in 1.8 seconds (0.057 Kbytes/s)
* ftp> #get
* (remote-file) #eff1.04
* (local-file) #eff1.04
* 200 PORT command successful.
* 150 Opening ASCII mode data connection for eff1.04 (909 bytes).
* 226 Transfer complete.
* local: eff1.04 remote: eff1.04
```

```
* 931 bytes received in 2.2 seconds (0.42 Kbytes/s)
* ftp> #close
* Bye...
* ftp> #quit
* %
*
```

To read the file you can just 'get' the file and buffer it. If the files are just too long, you can 'xmodem' it off the host you are on. Just type 'xmodem' and that will make it much faster to get the files. Here is the set up (as found on ocf.berkeley.edu).

If you want to:	type:
send a text file from an apple computer to the ME	xmodem ra <filename>
send a text file from a non-apple home computer	xmodem rt <filename>
send a non-text file from a home computer	xmodem rb <filename>
send a text file to an apple computer from the ME	xmodem sa <filename>
send a text file to a non-apple home computer	xmodem st <filename>
send a non-text file to a home computer	xmodem sb <filename>

xmodem will then display:

```
*
* XMODEM Version 3.6 -- UNIX-Microcomputer Remote File Transfer Facility
* File filename Ready to (SEND/BATCH RECEIVE) in (binary/text/apple) mode
* Estimated File Size (file size)
* Estimated transmission time (time)
* Send several Control-X characters to cancel
*
```

Hints- File transfer can be an iffy endeavor; one thing that can help is to tell the annex box not to use flow control. Before you do rlogin, type

```
 stty oflow none
 stty iflow none
```

at the annex prompt. This works best coming through 2-6092.

Some special commands used during ftp session are cdup (same as cd ..) and dir (gives a detailed listing of the files).

c: How to tftp the Files

tftp (Trivial File Transfer Protocol, the command is NOT in caps, because UNIX is case sensitive) is a command used to transfer files from host to host. This command is used sometimes like ftp, in that you can move around using UNIX commands. I will not go into this part of the command, but I will go into the basic format, and structure to get files you want. Moreover, I will be covering how to flip the /etc/passwd out of remote sites.

There is a little trick that has been around a while. It helps you to "flip" the /etc/passwd file out of different sites, which gets you the passwd file without out breaking into the system. Then just run Brute Hacker (the latest version) on the thing and you save time and energy. This 'hole' (not referring to the method of obtaining Unix superuser status) may can be found on SunOS 3.X, but has been fixed in 4.0. It has sometimes appeared in System V, BSD and a few others.

The only problem with this 'hole' is that the system manager will often realize what you are doing. The problem occurs when attempts to tftp the /etc/passwd is happen too many times. You may see this (or something like this) when you logon on to your account. This was buffered off of plague.berkeley.edu. I guess they knew what I was doing.

```
*
* DomainOS Release 10.3 (bsd4.3) Apollo DN3500 (host name):
*         This account has been deactivated due to use in system cracking
* activities (specifically attempting to tftp /etc/passwd files from remote
```

* sites) and for having been used or broken in to from <where the calls are
* from>. If the legitimate owner of the account wishes it reactivated,
* please mail to the staff for more information.
*
* - Staff
*

The tftp is used in this format:

tftp -<command> <any name> <Internet Address> /etc/passwd <netascii>

Command	-g is to get the file, this will copy the file onto your 'home' directory, thus you can do anything with the file.
Any Name	If your going to copy it to your 'home' directory, it needs a name.
Internet Address	This is the address that you want to snag the passwd file from. There are hundreds of thousands of them.
/ETC/PASSWD	THIS IS THE FILE THAT YOU WANT. You do not want John Smith's even though it would be trivial to retreive it.
netascii	This how you want the file to be transferred.
&	Welcome to the power of UNIX, it is multitasking, this little symbol place at the end will allow you to do other things (such as grab the passwd file from the UNIX that you are on).

Here is the set up: We want to get the passwd file from sunshine.ucsd.edu. The file in your 'home' directory is going to be named 'asunshine'.

*
* $ #tftp -g asunshine sunshine.ucsd.edu /etc/passwd &
*

d Basic Fingering

Fingering is a real good way to get an account on remote sites. Typing 'who' or just 'finger <account name> <CR>' you can have names to "finger". This will give you all kinds information on the person's account. Here is a example of how to do it:

*
* % #who
* joeo ttyp0 Jun 10 21:50 (bmdlib.csm.edu)
* gatsby ttyp1 Jun 10 22:25 (foobar.plague.mil)
* ddc crp00 Jun 10 11:57 (aogpat.cs.pitt.edu)
* liliya display Jun 10 19:40

/and fingering what you see

* % #finger bbc
* Login name: ddc In real life: David Douglas Cornwall
* Office: David C. Co
* Directory: //aogpat/users_local/bdc Shell: /bin/csh
* On since Jun 10 11:57:46 on crp00 from aogpat Phone 555-1212
* 52 minutes Idle Time
* Plan: I like to eat apples and bananas.
* %
*

Now you could just call (or Telnet to) 'aogpat.cs.pit.edu' and try to hack out an account. Try the last name as the password, the first name, the middle name, and try them all backwards. The chances are real good that you WILL get in because people are stupid.

If there are no users online for you to type "who" you can just type "last" and all of the users who logged on will come rolling out. Now "finger" them. The only problem with using the "last" command is aborting it.

You can also try telephoning individual users and tell them you are the system manager (i.e. social engineer them). However, I have not always seen phone numbers in everyone's ".plan" file (the file you see when you finger the user).

8 Other Networks

AARNet – Australian Academic and Research Network. This network supports research for various Australian Universities. This network supports TCP/IP, DECnet, and OSI (CLNS).

ARPANET – We've already discussed this network.

BITNET – Because It's Time NETwork (BITNET) is a worldwide network that connects many colleges and universities. This network uses many different protocols, but it dose use the TCP/IP.

CREN CSNET – Corporation for Research and Educational Network (CREN) or Computer + Science research NETwork (CSNET). This network links scientists at sites all over the world. CSNET providing access

to the Internet, CREN to BITNET. CREN is the name more often used today.

CSUNET – California State University Network (CSUNET). This network connects the California State University campuses and other universities in California. This network is based on the CCITT X.25 protocol, and also uses TCP/IP, SNA/DSLC, DECnet, and others.

The Cypress Net – This network started as a experimental network. The use of this network today is as a connection to the TCP/IP Internet as a cheap price.

DRI – Defense Research Internet is a WAN that is used as a platform from which to work from. This network has all kind of services, such as multicast service, real-time conference and more. This network uses the TCP/IP (also see RFC 907-A for more information on this network).

ESnet – This is the new network operated by the Department of Energy's Office of Energy Research (DoE OER). This net is the backbone for all DoE OER programs. This network replaced the High Energy Physics DECnet (HEPnet) and also the Magnetic Fusion Energy network (MFEnet). The protocols offered are IP/TCP and also DECnet service.

JANET – JANET is a Joint Academic NETwork based in the UK, connected to the Internet. JANET is a PSN (information has pass through a PAD) using the protocol X.25 though it does support the TCP/IP. This network also connects PSS (Packet Switched Service is a PSN that is owned and operated by British telecom).

JUNET – Japan's university message system using UUCP, the Internet as its backbone, and X.25 (see RFC 877). This network is also a part of USENET (this is the network news).

Los Nettos – Los Nettos is a high speed MAN in the Los Angeles area. This network uses the IP/TCP.

MILNET – When ARPANET split, the DDN was created and MILNET (MILitary NETwork) is also a part of the network. MILNET is unclassified, but there are three other classified networks that make up the

DDN.

NORDUNet – This net is the backbone to the networks in the Nordic Countries, Denmark (DENet), Finland (FUNET), Iceland (SURIS), Norway (UNINETT), and Sweden (SUNET). NORDUnet supports TCP/IP, DECNet, and X.25.

NSN – NASA Science Network (NSN). This network is used by NASA to send and relay information. The protocols used are TCP/IP. NSN has a sister network called Space Physics Analysis Network (SPAN) for DECNet.

ONet – Ontario Network is a TCP/IP network used for research.

NSFNet – National Science Foundation Network, this network is in the IP/TCP family, but in any case it uses UDP (User Diagram Protocol) and not TCP. NSFnet is the network for the US scientific and engineering research community. Listed below are all the NSFNet Sub-networks:

BARRNet – Bay Area Regional Research Network is located in the San Francisco area. This network uses TCP/IP.

CERFnet – California Education and Research Federation Network is a research based network supporting Southern California Universities communication services. This network uses TCP/IP.

CICNet – Committee on Institutional Cooperation. This network services the BIG 10, and University of Chicago. This network uses TCP/IP.

JvNCnet – John von Neumann National Supercomputer Center. This network uses TCP/IP.

Merit – Merit connects Michigan’s academic and research computers. This network supports TCP/IP, X.25 and Ethernet for LANs.

MIDnet – MIDnet connects 18 universities and research centers in the midwest United States. The support protocols are TELNET, FTP and SMTP.

MRNet – Minnesota Regional Network, this network services Minnesota. The network protocols are TCP/IP.

NEARnet – New England Academic and Research Network, connects various research/educational institutions. You can get more information about this net by mailing ’nearnet-staff@bbn.com’.

NCSAnet – The National Center for Supercomputing Applications supports the whole IP family (TCP, UDP, ICMP, etc).

NWNet – North West Network provides service to the Northwestern United States and Alaska. This network supports IP and DECnet.

NYSERNet – New York Service Network is a autonomous nonprofit network. This network supports the TCP/IP.

OARnet – Ohio Academic Resources Network gives access to the Ohio Supercomputer Center. This network supports TCP/IP.

PREPnet – Pennsylvania Research and Economic Partnership is a network operated and managed by Bell of Pennsylvania. It supports TCP/IP.

PSCNET – Pittsburgh Supercomputer Center serving Pennsylvania,

Maryland, and Ohio. It supports TCP/IP, and DECnet.

SDSCnet - San Diego Super Computer Center is a network whose goal is to support research in the field of science. The Internet address is 'y1.ucsc.edu' or call Bob at (619)534-5060 and ask for a account on his Cray.

Sesquinet - Sesquinet is a network based in Texas. It supports TCP/IP.

SURAnet - Southeastern Universities Research Association Network is a network that connects institutions in the Southeast United States.

THEnet - Texas Higher Education Network is a network that is run by Texas A&M University. This network connects to hosts in Mexico.

USAN/NCAR - University SAtellite Network (USAN)/National Center for Atmospheric Research is a network for information exchange.

Westnet - Westnet connects the western part of the United States, but not including California. The network is supported by Colorado State University.

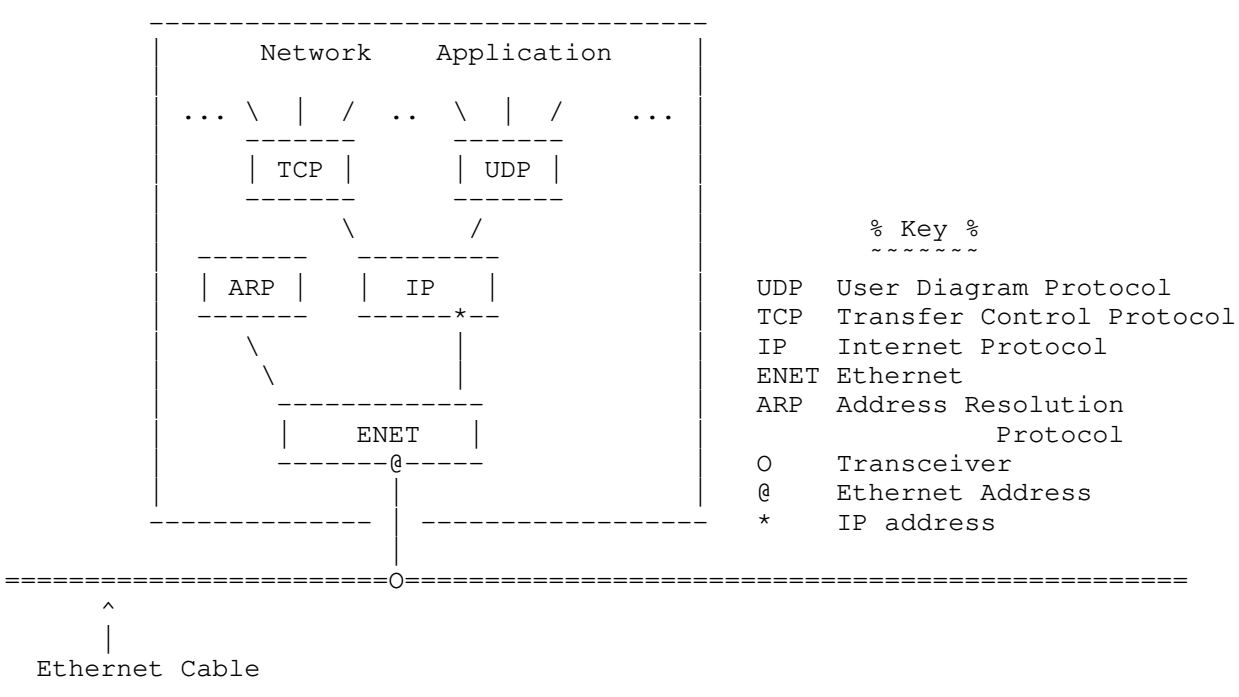
USENET - USENET is the network news (the message base for the Internet). This message base is quite large with over 400 different topics and connecting to 17 different countries.

9 Internet Protocols

TCP/IP is a general term relating to the whole family of Internet protocols. The protocols in this family are IP, TCP, UDP, ICMP, ROSE, ACSE, CMIP, ISO, ARP and Ethernet for LANs. If if you want more information, get the RFCs.

TCP/IP protocol is a "layered" set of protocols. In this diagram taken from RFC 1180 you will see how the protocol is layered when connection is made.

Figure is of a Basic TCP/IP Network Node:



TCP/IP: If connection is made is between the IP module and the TCP module the packets are called a TCP datagram. TCP is responsible for making

sure that the commands get through the other end. It keeps track of what is sent, and retransmits anything that does not go through. The IP provides the basic service of getting TCP datagram from place to place. It may seem like the TCP is doing all the work, this is true in small networks, but when connection is made to a remote host on the Internet (passing through several networks) this is a complex job. Say I am connected from a server at UCSD to LSU (SURAnet) the data grams have to pass through a NSFnet backbone. The IP has to keep track of all the data when the switch is made at the NSFnet backbone from the TCP to the UDP. The only NSFnet backbone that connects LSU is the University of Maryland, which has different circuit sets. The cable (trunk)/circuit types are the T1 (a basic 24-channel 1.544 Md/s pulse code modulation used in the US) to a 56 Kbps. Keeping track of all the data from the switch from T1 to 56Kbs and TCP to UDP is not all it has to deal with. Datagrams on their way to the NSFnet backbone (at the University of Maryland) may take many different paths from the UCSD server.

All the TCP does is break up the data into datagrams (manageable chunks), and keeps track of the datagrams. The TCP keeps track of the datagrams by placing a header at the front of each datagram. The header contains 160 (20 octets) pieces of information about the datagram. Some of this information is the FQDN (Fully Qualified Domain Name). The datagrams are numbers in octets (a group of eight binary digits, say there are 500 octets of data, the numbering of the datagrams would be 0, next datagram 500, next datagram 1000, 1500 etc.

UDP/IP: UDP is one of the two main protocols of the IP. In other words the UDP works the same as TCP, it places a header on the data you send, and passes it over to the IP for transportation throughout the Internet. The difference is that it offers service to the user's network application. It does not maintain an end-to-end connection, it just pushes the datagrams out.

ICMP: ICMP is used for relaying error messages. For example you might try to connect to a system and get a message back saying "Host unreachable", this is ICMP in action. This protocol is universal within the Internet, because of its nature. This protocol does not use port numbers in it's headers, since it talks to the network software itself.

Ethernet: Most of the networks use Ethernet. Ethernet is just a party line. When packets are sent out on the Ethernet, every host on the Ethernet sees them. To make sure the packets get to the right place, the Ethernet designers wanted to make sure that each address is different. For this reason 48 bits are allocated for the Ethernet address, and a built in Ethernet address on the Ethernet controller.

The Ethernet packets have a 14-octet header, this includes address "to" and "from." The Ethernet is not too secure, it is possible to have the packets go to two places, thus someone can see just what you are doing. You need to take note that the Ethernet is not connected to the Internet. A host on both the Ethernet and on the Internet has to have both an Ethernet connection and an Internet server.

ARP: ARP translates the IP address into an Ethernet address. A conversion table is used (the table is called ARP Table) to convert the addresses. Therefore, you would never even know if you were connected to the Ethernet because you would be connecting to the IP address.

The following is a real sketchy description of a few Internet protocols, but if you would like to get more information you can access it via anonymous ftp from several hosts. Here is a list of RFCs that deal with the topic of protocols.

RFC:	Description:

rfc1011	Official Protocols of the Internet
rfc1009	NSFnet gateway specifications
rfc1001/2	netBIOS: networking for PC's
rfc894	IP on Ethernet
rfc854/5	telnet - protocols for remote logins
rfc793	TCP
rfc792	ICMP
rfc791	IP
rfc768	UDP

10 Host Name and Address

Internet addresses are long and difficult hard to remember (i.e., 128.128.57.83) so we use host names. All hosts registered on the Internet must have names that reflect them domains under which they are registered. Such names are called Fully Qualified Domain Names (FQDNs). Lets dissect a name and see the domains:

```
 lilac.berkeley.edu
   ^      ^      ^
   |      |      |
   |      |      |____  "edu" shows that this host is sponsored by an
   |      |             education related organization.  This is a top-level
   |      |             domain.
   |      |
   |      |___________  "berkeley" is the second-level domain.  This shows
   |                    that it is an organization within University of
   |                    Calironia at  Berkeley.
   |
   |_________________   "lilac" is the third-level domain.  This indicates the
                        local host name is 'lilac'.
```

Common Top-Level Domains

COM - commercial enterprise
EDU - educational institutions
GOV - nonmilitary government agencies
MIL - military (non-classified)
NET - networking entities
ORG - nonprofit intuitions

A network address is the numerical address of a host, gateway, or TAC. The addresses are made up of four decimal numbered slots, which are separated by a period.

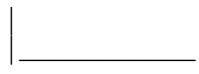
There are three classes that are used most, these are Class A, Class B, and Class C.

Class A - from '0' to '127'
Class B - from '128' to '191'
Class C - from '192' to '223'

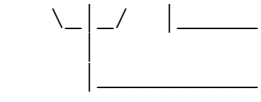
Class A - Is for MILNET net hosts. The first part of the address has the network number. The second is for the physical PSN port number. The third is for the logical port number, since it is on MILNET, it is a MILNET host. The fourth part is for which PSN it is on. On 29.34.0.9. '29' is the network it is on. '34' means it is on port '34'. '9' is the PSN number.

Class B - This is for the Internet hosts, the first two "clumps" are for the network portion. The second two are for the local port.

```
 128.28.82.1
   \_/   \_/
    |     |_____ Local portion of the address
```



Class C - The first three "clumps" are the network portion and the last one is the local port.



==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 4 of 13

FEDIX
On-Line Information Service

Written by the people at FEDIX

Like Fedix Upix

What is FEDIX?

FEDIX is an on-line information service that links the higher education community and the federal government to facilitate research, education, and services. The system provides accurate and timely federal agency information to colleges, universities, and other research organizations.

There are NO REGISTRATION FEES and NO ACCESS CHARGES for using FEDIX. The only cost is for the phone call.

FEDIX provides daily information updates on:

- Federal EDUCATION and RESEARCH PROGRAMS (including descriptions, eligibility, funding, deadlines).
- SCHOLARSHIPS, FELLOWSHIPS, and GRANTS
- Available used government RESEARCH EQUIPMENT
- New funding for specific research and education activities from the COMMERCE BUSINESS DAILY, FEDERAL REGISTER, and other sources.
- MINORITY ASSISTANCE research and education programs
- NEWS & CURRENT EVENTS within participating agencies
- GENERAL INFORMATION such as agency history, budget, organizational structure, mission statement, etc.

PARTICIPATING AGENCIES

Currently FEDIX provides information on 7 federal agencies broken down into 2 general categories:

1. Comprehensive Education and Research Related Agency Information
- The Department of Energy (DOE)
- Office of Naval Research (ONR)
- National Aeronautics and Space Administration (NASA)
- Federal Aviation Administration (FAA)

2. Minority Assistance Information
- National Science Foundation (NSF)
- Department of Housing and Urban Development (HUD)
- Department of Commerce (DOC)

Additional government agencies are expected to join FEDIX in the future.

REQUIRED HARDWARE AND SOFTWARE

Any microcomputer with communications software (or a dumb terminal) and a modem operating at 1200 or 2400 baud can access the system.

HOURS OF OPERATION

The system operates 24 hours a day, 7 days a week. The only exceptions are for periodic system updating or maintenance.

TELEPHONE NUMBERS

* Computer (data line): 301-258-0953 or 1-800-232-4879
* HELPLINE (technical assistance): 301-975-0103.

The HELPLINE (for problems or comments) is open Monday-Friday 8:30 AM-4:30 PM Eastern Daylight Time, except on federal holidays.

SYSTEM FEATURES

Although FEDIX provides a broad range of features for searching, scanning, and downloading, the system is easy to use. The following features will permit quick and easy access to agency databases:

Menus
-- Information in the system is organized under a series of branching menus. By selecting appropriate menu options (using either the OPTION NUMBER or the two-character MENU CODE), you may begin at the FEDIX Main Menu and work your way through various intermediate menus to a desired sub-menu. However, if you already know the menu code of a desired menu, you may bypass the intermediate menus and proceed directly to that menu by typing the menu code at the prompt.

Help screens are available for key menus and can be viewed by typing '?' at the prompt.

Capturing Data
-- If you are using a microcomputer with communicaions software, it is likely that your system is capable of storing or "capturing" information as it comes across your screen. If you "turn capture on", you will be able to view information from the databases and store it in a file on your system to be printed later. This may be desirable at times when downloading is not appropriate. Refer to your communications software documentation for instructions on how to activate the capture feature.

Downloading
-- Throughout the system, options are available which allow you to search, list, and/or download files containing information on specific topics. The download feature can be used to deliver text files (ASCII) or compressed, self-extracting ASCII files to your system very quickly for later use at your convenience. Text files in ASCII format, tagged with a ".MAC" extension, are downloadable by Macintosh users. Compressed ASCII files, tagged with an ".EXE" extension, may be downloaded by users of IBM compatible computers. However, your system must be capable of file transfers. (See the documentation on your communication software).

Mail
-- An electronic bulletin board feature allows you to send and receive messages to and from the SYSTEM OPERATOR ONLY. This feature will NOT send messages between users. It can be used to inquire about operating the system, receive helpful suggestions from the systems operator, etc.

Utility Menu
-- The Utility Menu, selected from the FEDIX Main Menu, enables you to modify user information, prioritize agencies for viewing, search and download agency information, set a default calling menu, and set the file transfer protocol for downloading files.

INDEX OF KEY INFORMATION ON FEDIX

Key information for each agency is listed below with the code for the menu from which the information can be accessed. Please be advised that this list is not comprehensive and that a significant amount of information is available on FEDIX in addition to what is listed here.

AGENCY/DATABASE	MENU CODE
DEPARTMENT OF ENERGY (DOE)/DOEINFO	
Available Used Research Equipment	:EG:

Research Program Information	:IX:
Education Program Information	:GA:
Search/List/Download Program Information	:IX:
Research and Training Reactors Information	:RT:
Procurement Notices	:MM:
Current Events	:DN:

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION/NASINFO

Research Program Information	:RP:
Education Program Information	:EA:
Search/List/Download Program Information	:NN:
Description/Activities of Space Centers	:SC:
Procurement Notices	:EV:
Proposal/Award Guidelines	:NA:

OFFICE OF NAVAL RESEARCH/ONRINFO

Research Program Information	:RY:,:AR:
Special Programs (Special Research and Education Initiatives)	:ON:
Search/List/Download Program Information	:NR:
Description/Activities of Laboratories and other ONR Facilities	:LB:
Procurement Notices (Broad Agency Announcements, Requests for Proposals, etc.	:NE:
Information on the Preparation and Administration of Contracts, Grants, Proposals	:AD:

FEDERAL AVIATION ADMINISTRATION/FAAINFO

Education Program Information - Pre-College	:FE:
Mio rity Aviation Education Programs	:FY:
Search/List/Download Program Information	:FF:
Aviation Education Resources (Newsletters, Films/Videos, Publications)	:FR:
Aviation Education Contacts (Government, Industry, Academic, Associations)	:FO:
College-Level Airway Science Curriculum Information	:FC:
Procurement Notice	:FP:
Planned Competitive and Noncompetitive Procurements for the Current Fiscal Year	:F1:
Employment Information	:FN:
Current Events	:FV:

MINORITY/MININFO

U. S. Department of Commerce

Research/Education Minority Assistance Programs	:CP:
Procurement Notices (ALL Notices for Agency)	:M1:
Current Events	:M1:
Minority Contacts	:M1:

Department of Energy

Research/Education Minority Assistance Programs	:EP:
Procurement Notices (ALL Notices for Agency)	:M2:
Current Events	:M2:
Minority Contacts	:M2:

U.S. Department of Housing and Urban Development

Research/Education Minority Assistance Programs	:HP:
Procurement Notices (ALL Notices for Agency)	:M3:
Current Events	:M3:
Minority Contacts	:M3:

National Aeronautics and Space Administration

Research/Education Minority Assistance Programs	:NP:
Procurement Notices (ALL Notices for Agency)	:M4:
Current Events	:M4:
Minority Contacts	:M4:

National Science Foundation

Research/Education Minority AssisdaXce Programs	:SP:
Procurement Notices (ALL Notices for Agency)	:M5:
Budget Information	:SB:
NSF Bulletin	:M5:
Minority Contacts	:M5:

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 5 of 13

```
|\/\/\/\/\/\/\/\/\/\/\/\/\/|
|                          |
|    LATA Referance List   |
|                          |
|     by Infinite Loop     |
|                          |
|/\/\/\/\/\/\/\/\/\/\/\/\/\|
```

United States telephone LATA official designation numbers:

STATE	NAME	NUMBER
AK	ALASKA	832
AL	BIRMINGHAM	476
AL	HUNTSVILLE	477
AL	MONTGOMERY	478
AL	MOBILE	480
AR	FORT SMITH	526
AR	LITTLE ROCK	528
AR	PINE BLUFF	530
AZ	PHOENIX	666
AZ	TUCSON	668
AZ	NAVAJO RESERVATION	980
CA	SAN FRANCISCO	722
CA	CHICO	724
CA	SACRAMENTO	726
CA	FRESNO	728
CA	LOS ANGELES	730
CA	SAN DIEGO	732
CA	BAKERSFIELD	734
CA	MONTEREY	736
CA	STOCKTON	738
CA	SAN LUIS OBISPO	740
CA	PALM SPRINGS	973
CO	DENVER	656
CO	COLORADO SRPINGS	658
CT	CONNECTICUT <SNET>	920
DC	WASHINGTON	236
FL	PENSACOLA	448
FL	PANAMA CITY	450
FL	JACKSONVILLE	452
FL	GAINESVILLE	454
FL	DAYTONA BEACH	456
FL	ORLANDO	458
FL	SOUTHEAST	460
FL	FORT MYERS	939
FL	GULF COST	952
FL	TALLAHASSEE	953
GA	ATLANTA	438
GA	SAVANNAH	440
GA	AUGUSTA	442
GA	ALBANY	444
GA	MACON	446
HI	HAWAII	834
IA	SIOUX CITY	630
IA	DES MOINES	632
IA	DAVENPORT	634
IA	CEDAR RAPIDS	635
ID	IDAHO	652
ID	COEUR D’ALENE	960
IL	CHICAGO	358
IL	ROCKFORD	360
IL	CAIRO	362
IL	STERLING	364

IL	FORREST	366
IL	PEORIA	368
IL	CHAMPAIGN	370
IL	SPRINGFIELD	372
IL	QUINCY	374
IL	MATTOON	976
IL	GALESBURG	977
IL	OLNEY	978
IN	EVANSVILLE	330
IN	SOUTH BEND	332
IN	AUBURN/HUNTINGTON	334
IN	INDIANAPOLIS	336
IN	BLOOMINGTON	338
IN	RICHMOND	937
IN	TERRE HAUTE	938
KS	WICHITA	532
KS	TOPEKA	534
KY	LOUISVILLE	462
KY	OWENSBORO	464
KY	WINCHESTER	466
LA	SHREVEPORT	486
LA	LAFAYETTE	488
LA	NEW ORLEANS	490
LA	BATON ROUGE	492
MA	WESTERN MASSACHUSETT	126
MA	EASTERN MASSACHUSETT	128
MD	BALTIMORE	238
MD	HAGERSTOWN	240
MD	SALISBURY	242
ME	MAINE	120
MI	DETROIT	340
MI	UPPER PENINSULA	342
MI	SAGINAW	344
MI	LANSING	346
MI	GRAND RAPIDS	348
MN	ROCHESTER	620
MN	DULUTH	624
MN	ST CLOUD	626
MN	MINNEAPOLIS	628
MO	ST LOUIS	520
MO	WESTPHALIA	521
MO	SPRINGFIELD	522
MO	KANSAS CITY	524
MS	JACKSON	482
MS	BILOXI	484
MT	GREAT FALLS	648
MT	BILLINGS	650
MT	KALISPELL	963
NC	ASHEVILLE	420
NC	CHARLOTTE	422
NC	GREENSBORO	424
NC	RALEIGH	426
NC	WILMINGTON	428
NC	FAYETTEVILLE	949
NC	ROCKY MOUNT	951
ND	FARGO	636
ND	BISMARCK	638
NE	OMAHA	644
NE	GRAND ISLAND	646
NE	LINCOLN	958
NH	NEW HAMPSHIRE	122
NJ	ATLANTIC COSTAL	220
NJ	DELAWARE VALLEY	222
NJ	NORTH JERSEY	224
NM	NEW MEXICO	664
NV	RENO	720
NV	PAHRUMP	721
NY	NEW YORK METRO	132
NY	POUGHKEEPSIE	133
NY	ALBANY	134

NY	SYRACUSE	136
NY	BINGHAMTON	138
NY	BUFFALO	140
NY	FISHERS ISLAND	921
NY	ROCHESTER	974
OH	CLEAVELAND	320
OH	YOUNGSTOWN	322
OH	COLUMBUS	324
OH	AKRON	325
OH	TOLEDO	326
OH	DAYTON	328
OH	CINCINNATI BELL	922
OH	MANSFIELD	923
OK	OKLAHOMA CITY	536
OK	TULSA	538
OR	EUGENE	670
OR	PORTLAND	672
PA	CAPITAL	226
PA	PHILADELPHIA	228
PA	ALTOONA	230
PA	NORTHEAST	232
PA	PITTSBURG	234
PA	ERIE	924
PR	PUERTO RICO	820
RI	RHODE ISLAND	130
SC	GREENVILLE	430
SC	FLORENCE	432
SC	COLUMBIA	434
SC	CHARLESTON	436
SD	SOUTH DAKOTA	640
TN	MEMPHIS	468
TN	NASHVILLE	470
TN	CHATTANOOGA	472
TN	KNOXVILLE	474
TN	BRISTOL	956
TX	EL PASO	540
TX	MIDLAND	542
TX	LUBBOCK	544
TX	AMARILLO	546
TX	WICHITA FALLS	548
TX	ABILENE	550
TX	DALLAS	552
TX	LONGVIEW	554
TX	WACO	556
TX	AUSTIN	558
TX	HOUSTON	560
TX	BEAUMONT	562
TX	CORPUS CHRISTI	564
TX	SAN ANTONIO	566
TX	BROWNSVILLE	568
TX	HEARNE	570
TX	SAN ANGELO	961
US	MIDWAY/WAKE	836
UT	UTAH	660
UT	NAVAJO RESERVATION	981
VA	ROANOKE	244
VA	CULPEPER	246
VA	RICHMOND	248
VA	LYNCHBURG	250
VA	NORFOLK	252
VA	HARRISONBURG	927
VA	CHARLOTTESVILLE	928
VA	EDINBURG	929
VI	US VIRGIN ISLANDS	822
VT	VERMONT	124
WA	SEATTLE	674
WA	SPOKANE	676
WI	NORTHEASST	350
WI	NORTHWEST	352
WI	SOUTHWEST	354

WI	SOUTHEAST	356
WV	CHARLESTON	254
WV	CLARKSBURG	256
WV	BLUEFIELD	932
WY	WYOMING	654

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 6 of 13

International Toll-free, Local Rated, and Specially Toll Services

by The Trunk Terminator

The following indicates access codes and numbers used within various countries for toll-free and special paid services. The dialing codes shown represent how they would be dialed within the country involved. Generally, it is not possible to access another country's domestic toll-free or specialty network directly. Where an international access is available, it is normally done by using the domestic services which then forward the call to the destination country.

Where possible, the number of digits has been indicated with 'n' (a number from 2 to 8) or 'x' (any number). An ellipsis (...) indicates that there are a variable number of extra digits, or possibly a conflict in the reports of numbers of digits used.

Toll-free or equivalent local charge services

A u s t r a l i a

008 xxx xxx	That is how Phrack Inc. recomends it be written to differentiate it from STD area codes which are written with area codes (0x) thru (0xxx) and numbers n xxxx through nxx xxxx.
0014 ttt xxx xxx	International Toll free access from Australia (ttt is reported as "800" or other toll-free access code; or, ttt may not be present at all.
	(Canada Direct uses 0014 881 150)

B e l g i u m

11 xxxx

D e n m a r k

800 xxxxx
8001 xxxx (charged as local call)

F i n l a n d

9800 xxxxx (...)	(PTT as local service provider)
0800 xxxxx (...)	(Private phone company as local service provider)

9800 costs the same as a local call (dialable from all areas in Finland), while 0800 are truly toll-free and dialable from all private telco areas.

F r a n c e

05 xxxxxx This is outside area code 1, so from Paris 16 05.

05 19 xx xx These numbers terminate outside France.

36 63 xx xx (local call rate)

'11' is computer directory information.
'12' is voice directory information (equivalent to 411).

G e r m a n y (w e s t)

0130 xxxx (...xx) The number to use AT&T is 0130-0010 and U.S. Sprint is 0130-0013. For a general toll-free number listings, pick up a copy of the International Herald newspaper and look in the sports section is for an AT&T add. You will find a number for dialing the US from various countries. Mearly, chop off the exchange and only use the "area code" number.

I r e l a n d

1800 xxxxxx
1850 xxxxxx (local rate)

I t a l y

167 xxxxx (digits length)

We're not 100% sure about the length of digits for Italy. One way to check these is to get a copy of an *international* edition of the weekly magazines like TIME, all ads and little contents. But they do goof up regularly, like printing Paris numbers as (01) xxxxxxxx when they mean (1) xxxxxxxx.

M e x i c o

91 800 xxxxx....

N e t h e r l a n d s

06-0xxx
06-0xxxxxx
06-4xx(x) 06-2229111 is AT&T USA direct and Sprint & MCI have operator services on 06-022xxxx. It used to be possible to call 06-022xxxx to Denmark, and then use the CCITT no. 4 signalling system to phreak calls to anywhere in the world.

06-11 This is the Dutch equivalent of 911, it is free when dialled from a phone company operated payphone, otherwise the charge is one unit, DFL 0.15, about US $ 0.08. There were discussions about making such calls free from any phone, but I haven't followed them recently. Calling a toll-free number from a payphone requires a deposit of one coin, which is returned after the call.

The total length of the numbers varies from 4 to 10 digits and the dash indicates the secondary dial tone. It is not possible to reach 06 prefixed numbers from abroad.

New Zealand

0800 xxx xxx — That is through the state telco, Telecom New Zealand. Clear Communications, the recently started alternative LD carrier, does not offer a toll-free service as yet. When Clear offer one, it will more than likely be to the subscribers existing number (eg Dial toll free 050-04-654-3210) as they are not in control of number issue. 0800 is strictly Telecom at this stage.

North America

1 800 nxx xxxx — Access to toll free numbers can vary according to region, state or country (ie. not all 800 numbers are accessible to all regions).

The nxx prefix portion of the 800 number presently determines which long distance carrier or 800 service company will handle the call (and in some cases determine the geographical region).

Spain

900 xxxxxx — The number for ATT direct in Spain is 900-99-00-11. The payphones are all push-button but generate pulses. It takes forever to get connected.

Sweden

020 xxxxxx — (without dialtone after '020').

Switzerland

04605 xxxx — (not toll-free but metered at lowest rate)
155 xx xx — ("green number")

In Switzerland there is nothing exactly like the equivalent to United States "800" service. The PTT is now encouraging the use of "green numbers" beginning with 155. The direct marketing ads on TV often give the order number for Switzerland as a number such as 155 XX XX. The access number for MCI Call USA is for example 155 02 22. There are two problems with this:

1] When calling from a model AZ44(older model) payphone all numbers which begin with a "1" are treated as "service" numbers and the payphone begins to sound a "cuckoo clock noise" once the 155 is entered. The "cuckoo clock noise" is to alert operators on the "service numbers" that the caller is using a payphone (fraud protection). This noise is quite a distraction when calling someone in the USA using MCI Call USA.

2] The newer style TelcaStar phones are programmed to block the keypad after 3 digits are dialed of a "service number". It used to be that the only numbers beginning with "1" were

"service numbers" and all "service numbers" were 3 digits. The PTT is aware of this problem and are said to be considering what instructions to give the manufacturer of the payphones.

AT&T USA Direct has an access number of 046 05 00 11. This is not a free call, but the time is metered at the lowest rate. This number does not suffer the "cuckoo clock noise" problem.

Canada Direct uses 046 05 83 30.

U n i t e d K i n g d o m

0800 xxx xxx (Toll-free)
0345 xxx xxx (Local rate)

Tolled/Specialty Pay services

A u s t r a l i a

0055 x yxxx where y=0-4,8 means the number is Australia wide (and costs more),
y=5 means the number is only state wide,
y=6,7,9 means the number is for the capital city only.

F i n l a n d

9700 xxxxx (PTT-operated)
0700 xxxxx (Private telco-operated)

The cost ranges from about 0.5 USD to 5 USD per minute.

F r a n c e

36 65 xx xx (5 message units each call for up to 140 seconds)

These are for various information services as well as chat lines.

N e t h e r l a n d s

06-9 xx...
06-321 xx...
06-8 xx... (3 to 40ct/min)

Other codes (such as 06-9) precede special tariff calls (similar to 900 in the US). The highest special rate is (currently) DFL 0.50 / minute.

N o r t h A m e r i c a

1 900 nxx xxxx (various rates, depending on provider)

1 (npa) 976 xxxx (in many area codes, connected through regional telco;
in some areas, the call requires the area code where
depending on the intra-area dialing used)

(other exchange prefixes within area codes such as 540, 720
or 915 are used for other pay services such as group chat,
other types of recorded messages, etc. These vary depending
on the area code within North America, and not all regions in
North America have these.)

==========
S w e d e n
==========

071 x xxxxx

The Swedish answer to the United States "900"-number, 071 are
as follows.

(Charges are related to the next digit)

code	SEK/minute
0712xxxxx	3,65
0713xxxxx	4,90
0714xxxxx	6,90
0715xxxxx	9,90
0716xxxxx	12,50
0717xxxxx	15,30
0719xx	varying fees, cannot be dialled directly but needs operator

Numbers starting with 0713-0717 can only be dialled from
phones connected to AXE exchanges. At present about half of
all phones in Sweden are connected to such exchanges.

Another special toll number is domestic number information:
07975 (6,90 SEK/minute).

==========
U n i t e d K i n g d o m
==========

0836 xxx xxx
0898 xxx xxx

The rate seems to be uniform as 34p per minute cheap rate,
45p at all other times.

=-=-=-

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 7 of 13

```
 //---------------------\\
||   P h r e a k i n g   ||
||                       ||
||          i n          ||
||                       ||
||     G e r m a n y     ||
||                       ||
||          by           ||
||                       ||
||   -=+Ninja Master+=-  ||
||                       ||
||          of           ||
||                       ||
|| -[The Hellfire Club]- ||
 \\---------------------//
```

Phreaking in Germany at this moment is at an all time high. The main reason is because of the German reunification. Most, if not all, of the equipment in Germany is still mechanical (especially on the former Communist side). So Boxing is VERY easy to do, as are line taps.

Tracing on the other hand, is still hard to do. This is because with the mechanical switches they need many technicians who look at the switches and follow the wires on their own. They usually don't know where the wire leads, so they have to physically follow the wire to trace it.

There are two main ways of phreaking in Germany at the moment. One is Boxing and the other is through Cordless Phones, both of which I will describe.

```
 //------\\
|| Boxing ||
 \\------//
```

Boxing in Germany is somewhat similar to the US, but I will describe to you the whole process.

Most boxing in Germany is started with a call to a toll free number (most of which produce a connection to a firm in the US, AT&T.) To initiate the call, you dial 0130 - 81 and the number. Germany's toll free net starts with 0130. 81 is for connection to the US. You wait for the connection, and blast the dissconect signal. As we all know, in the US it's 2600 Hz, but in Germany it's a mixture of 2400 and 2600 Hz. After that, you send a single 2400 Hz frequency to hold the line. Then you decide if you want a local US call, or an International call. Don't forget, you are connected to the US now, so it looks as if anything out of it as International, even though your calling from Germany. Calls within the US are done normally, with KP+0+AC+NNNNNNN.
To make the international call, it's KP2+internalional code+0+number.
You have to drop the zero though from the number you care calling. For example, in Germany all numbers start with a 02366.

One big difference between boxing in the US and Germany, are the laws. In Germany, they look very strictly at data-security, but the laws are not clear in
the area of phreaking. No one knows if a phreak is really stealin something from the German phone company, since he is using a normal phone number. This may sound stupid to us, but that's how they view it. Phreaks getting busted for in Germany is usually a rare occassion, if ever.

```
 //---------------\\
|| Cordless Phones ||
 \\---------------//
```

When I am refering to "cordless phones", I'm not talking about portable phones in the cellular phone system. I'm talking about simple cordless phones that you have in your home. Cordless phones broadcast on a speciffic radio

frequency (around 46MHz) to a "base unit" that is connected to the wall jack.

What the you do now is put a long antenna on the roof of your car. Then connect the antenna to your handset. The length of the antenna is usually best around 1.5 meters long. You only need the handset, because you are going to be connecting to another persons base, but make sure the batteries in the handset are fully charged. Now, the next step is to drive around in your car, until you hear a free line. Then, mearly call anywhere you like! Usually you have to situate yourself, and find where the best postion is to recieve the signal clearly, and that the person who's base your connected to can't see you.

One reason this works quite well, is because most cordless phones in Germany don't have the code feature that is so prominent here (where you can select a scrambling code on the handset and base).

One of the incentives to phreak in this manner is because, cordless phones being illegal, the person, who's dial tone you used, would much rather pay a few high long distance bills than the even higher fines for geting caught with a cordless phone.

Cordless phones are forbidden in Germany, although you can buy them almost anywhere. What is illegal is to physically connect them to the phone system. The phone company there actually searches for people with cordless phones, by using a specially equiped van. Once they find that you have a cordless phone connected, they come with two policmen and a search warrant. You can be charged with anything from illegal connection of nontested equipment to forging of a document.

```
 //----------\\
|| Conclusion ||
 \\----------//
```

Well, I hope this gave you a little bit of understanding of how disorganized the phone system is in over there, and gave you a few helpfull hints in case you ever happen to find yourself in Germany.

If you have any comments, corrections, or additions, you can reach me through Phrack, or the following boards:

Lightning Systems	9th Dimension
414-363-4282	818-783-5320

Until next time!

-=+Ninja Master+=-
-[The Hellfire Club]-
"Tell Telco We're Phreaking, Phreaking USA!"

\\--//

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 8 of 13

A TCP/IP Tutorial : Behind The Internet
Part One of Two

September 12, 1991

by The Not

Table of Contents

1. Introduction
2. TCP/IP Overview
3. Ethernet
4. ARP

1. Introduction

This tutorial contains only one view of the salient points of TCP/IP, and therefore it is the "bare bones" of TCP/IP technology. It omits the history of development and funding, the business case for its use, and its future as compared to ISO OSI. Indeed, a great deal of technical information is also omitted. What remains is a minimum of information that must be understood by the professional working in a TCP/IP environment. These professionals include the systems administrator, the systems programmer, and the network manager.

This tutorial uses examples from the UNIX TCP/IP environment, however the main points apply across all implementations of TCP/IP.

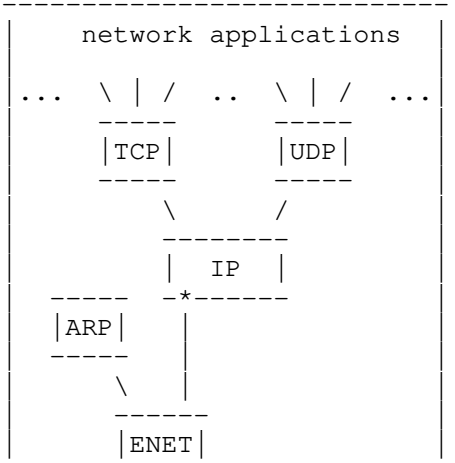
Note that the purpose of this memo is explanation, not definition. If any question arises about the correct specification of a protocol, please refer to the actual standards defining RFC.
The next section is an overview of TCP/IP, followed by detailed descriptions of individual components.

2. TCP/IP Overview

The generic term "TCP/IP" usually means anything and everything related to the specific protocols of TCP and IP. It can include other protocols, applications, and even the network medium. A sample of these protocols are: UDP, ARP, and ICMP. A sample of these applications are: TELNET, FTP, and rcp. A more accurate term is "internet technology". A network that uses internet technology is called an "internet".

2.1 Basic Structure

To understand this technology you must first understand the following logical structure:



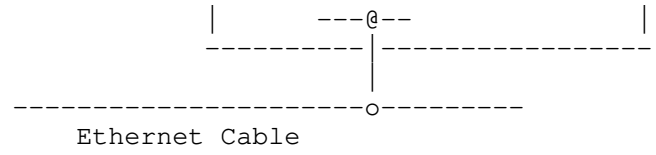


Figure 1. Basic TCP/IP Network Node

This is the logical structure of the layered protocols inside a computer on an internet. Each computer that can communicate using internet technology has such a logical structure. It is this logical structure that determines the behavior of the computer on the internet. The boxes represent processing of the data as it passes through the computer, and the lines connecting boxes show the path of data. The horizontal line at the bottom represents the Ethernet cable; the "o" is the transceiver. The "*" is the IP address and the "@" is the Ethernet address. Understanding this logical structure is essential to understanding internet technology; it is referred to throughout this tutorial.

2.2 Terminology

The name of a unit of data that flows through an internet is dependent upon where it exists in the protocol stack. In summary: if it is on an Ethernet it is called an Ethernet frame; if it is between the Ethernet driver and the IP module it is called a IP packet; if it is between the IP module and the UDP module it is called a UDP datagram; if it is between the IP module and the TCP module it is called a TCP segment (more generally, a transport message); and if it is in a network application it is called a application message.

These definitions are imperfect. Actual definitions vary from one publication to the next. More specific definitions can be found in RFC 1122, section 1.3.3.

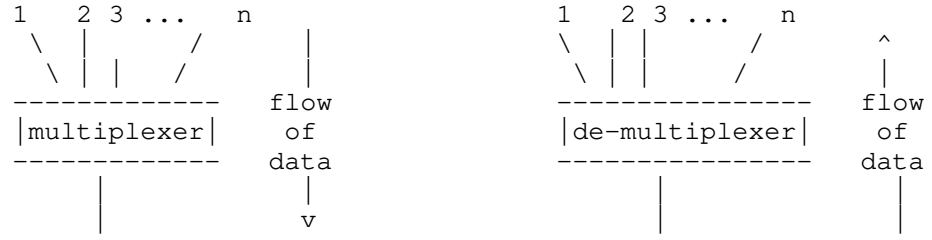
A driver is software that communicates directly with the network interface hardware. A module is software that communicates with a driver, with network applications, or with another module.

The terms driver, module, Ethernet frame, IP packet, UDP datagram, TCP message, and application message are used where appropriate throughout this tutorial.

2.3 Flow of Data

Let’s follow the data as it flows down through the protocol stack shown in Figure 1. For an application that uses TCP (Transmission Control Protocol), data passes between the application and the TCP module. For applications that use UDP (User Datagram Protocol), data passes between the application and the UDP module. FTP (File Transfer Protocol) is a typical application that uses TCP. Its protocol stack in this example is FTP/TCP/IP/ENET. SNMP (Simple Network Management Protocol) is an application that uses UDP. Its protocol stack in this example is SNMP/UDP/IP/ENET.

The TCP module, UDP module, and the Ethernet driver are n-to-1 multiplexers. As multiplexers they switch many inputs to one output. They are also 1-to-n de-multiplexers. As de-multiplexers they switch one input to many outputs according to the type field in the protocol header.



1 1

Figure 2. n-to-1 multiplexer and 1-to-n de-multiplexer

If an Ethernet frame comes up into the Ethernet driver off the network, the packet can be passed upwards to either the ARP (Address Resolution Protocol) module or to the IP (Internet Protocol) module. The value of the type field in the Ethernet frame determines whether the Ethernet frame is passed to the ARP or the IP module.

If an IP packet comes up into IP, the unit of data is passed upwards to either TCP or UDP, as determined by the value of the protocol field in the IP header.

If the UDP datagram comes up into UDP, the application message is passed upwards to the network application based on the value of the port field in the UDP header. If the TCP message comes up into TCP, the application message is passed upwards to the network application based on the value of the port field in the TCP header.

The downwards multiplexing is simple to perform because from each starting point there is only the one downward path; each protocol module adds its header information so the packet can be de-multiplexed at the destination computer.

Data passing out from the applications through either TCP or UDP converges on the IP module and is sent downwards through the lower network interface driver.

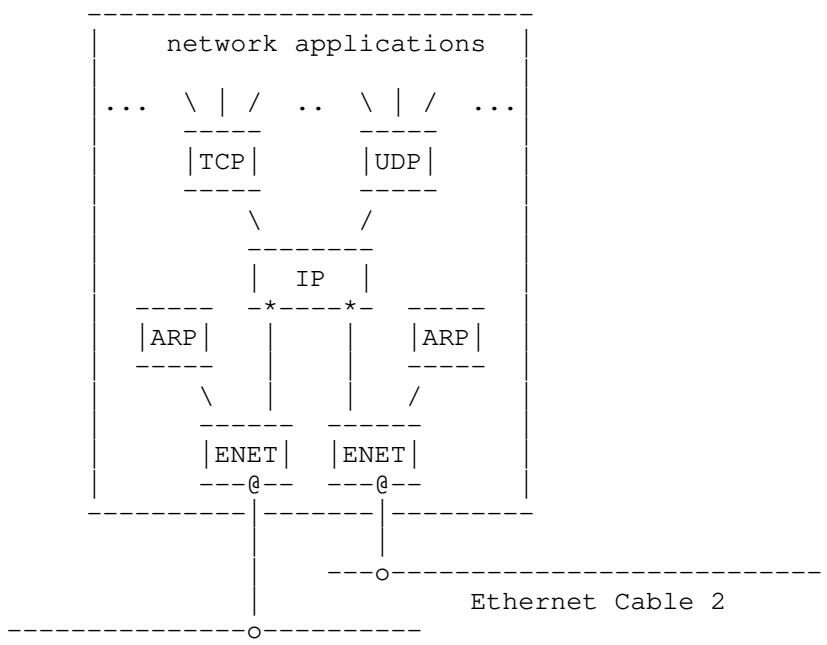
Although internet technology supports many different network media, Ethernet is used for all examples in this tutorial because it is the most common physical network used under IP. The computer in Figure 1 has a single Ethernet connection. The 6-byte Ethernet address is unique for each interface on an Ethernet and is located at the lower interface of the Ethernet driver.

The computer also has a 4-byte IP address. This address is located at the lower interface to the IP module. The IP address must be unique for an internet.

A running computer always knows its own IP address and Ethernet address.

2.4 Two Network Interfaces

If a computer is connected to 2 separate Ethernets it is as in Figure 3.



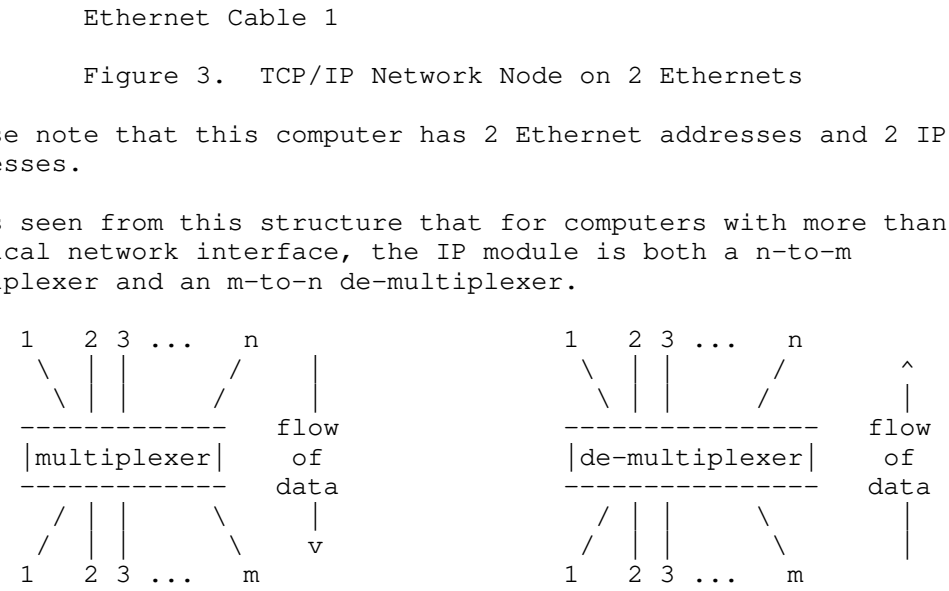


Figure 3. TCP/IP Network Node on 2 Ethernets

Please note that this computer has 2 Ethernet addresses and 2 IP addresses.

It is seen from this structure that for computers with more than one physical network interface, the IP module is both a n-to-m multiplexer and an m-to-n de-multiplexer.

Figure 4. n-to-m multiplexer and m-to-n de-multiplexer

It performs this multiplexing in either direction to accommodate incoming and outgoing data. An IP module with more than 1 network interface is more complex than our original example in that it can forward data onto the next network. Data can arrive on any network interface and be sent out on any other.

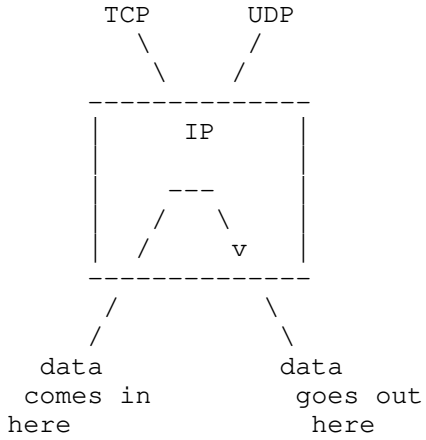


Figure 5. Example of IP Forwarding a IP Packet

The process of sending an IP packet out onto another network is called "forwarding" an IP packet. A computer that has been dedicated to the task of forwarding IP packets is called an "IP-router".

As you can see from the figure, the forwarded IP packet never touches the TCP and UDP modules on the IP-router. Some IP-router implementations do not have a TCP or UDP module.

2.5 IP Creates a Single Logical Network

The IP module is central to the success of internet technology. Each module or driver adds its header to the message as the message passes down through the protocol stack. Each module or driver strips the corresponding header from the message as the message climbs the protocol stack up towards the application. The IP header contains the IP address, which builds a single logical network from multiple physical networks. This interconnection of physical networks is the source of the name: internet. A set of interconnected physical networks that limit the range of an IP packet is called an "internet".

2.6 Physical Network Independence

IP hides the underlying network hardware from the network applications. If you invent a new physical network, you can put it into service by implementing a new driver that connects to the internet underneath IP. Thus, the network applications remain intact and are not vulnerable to changes in hardware technology.

2.7 Interoperability

If two computers on an internet can communicate, they are said to "interoperate"; if an implementation of internet technology is good, it is said to have "interoperability". Users of general-purpose computers benefit from the installation of an internet because of the interoperability in computers on the market. Generally, when you buy a computer, it will interoperate. If the computer does not have interoperability, and interoperability can not be added, it occupies a rare and special niche in the market.

2.8 After the Overview

With the background set, we will answer the following questions:

When sending out an IP packet, how is the destination Ethernet address determined?

How does IP know which of multiple lower network interfaces to use when sending out an IP packet?

How does a client on one computer reach the server on another?

Why do both TCP and UDP exist, instead of just one or the other?

What network applications are available?

These will be explained, in turn, after an Ethernet refresher.

3. Ethernet

This section is a short review of Ethernet technology.

An Ethernet frame contains the destination address, source address, type field, and data.

An Ethernet address is 6 bytes. Every device has its own Ethernet address and listens for Ethernet frames with that destination address. All devices also listen for Ethernet frames with a wild-card destination address of "FF-FF-FF-FF-FF-FF" (in hexadecimal), called a "broadcast" address.

Ethernet uses CSMA/CD (Carrier Sense and Multiple Access with Collision Detection). CSMA/CD means that all devices communicate on a single medium, that only one can transmit at a time, and that they can all receive simultaneously. If 2 devices try to transmit at the same instant, the transmit collision is detected, and both devices wait a random (but short) period before trying to transmit again.

3.1 A Human Analogy

A good analogy of Ethernet technology is a group of people talking in a small, completely dark room. In this analogy, the physical network medium is sound waves on air in the room instead of electrical signals on a coaxial cable.

Each person can hear the words when another is talking (Carrier Sense). Everyone in the room has equal capability to talk (Multiple Access), but none of them give lengthy speeches because they are polite. If a person is impolite, he is asked to leave the room (i.e., thrown off the net).

No one talks while another is speaking. But if two people start speaking at the same instant, each of them know this because each

hears something they haven't said (Collision Detection). When these two people notice this condition, they wait for a moment, then one begins talking. The other hears the talking and waits for the first to finish before beginning his own speech.

Each person has an unique name (unique Ethernet address) to avoid confusion. Every time one of them talks, he prefaces the message with the name of the person he is talking to and with his own name (Ethernet destination and source address, respectively), i.e., "Hello Jane, this is Jack, ..blah blah blah...". If the sender wants to talk to everyone he might say "everyone" (broadcast address), i.e., "Hello Everyone, this is Jack, ..blah blah blah...".

4. ARP

When sending out an IP packet, how is the destination Ethernet address determined?

ARP (Address Resolution Protocol) is used to translate IP addresses to Ethernet addresses. The translation is done only for outgoing IP packets, because this is when the IP header and the Ethernet header are created.

4.1 ARP Table for Address Translation

The translation is performed with a table look-up. The table, called the ARP table, is stored in memory and contains a row for each computer. There is a column for IP address and a column for Ethernet address. When translating an IP address to an Ethernet address, the table is searched for a matching IP address. The following is a simplified ARP table:

IP address	Ethernet address
223.1.2.1	08-00-39-00-2F-C3
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

TABLE 1. Example ARP Table

The human convention when writing out the 4-byte IP address is each byte in decimal and separating bytes with a period. When writing out the 6-byte Ethernet address, the conventions are each byte in hexadecimal and separating bytes with either a minus sign or a colon.

The ARP table is necessary because the IP address and Ethernet address are selected independently; you can not use an algorithm to translate IP address to Ethernet address. The IP address is selected by the network manager based on the location of the computer on the internet. When the computer is moved to a different part of an internet, its IP address must be changed. The Ethernet address is selected by the manufacturer based on the Ethernet address space licensed by the manufacturer. When the Ethernet hardware interface board changes, the Ethernet address changes.

4.2 Typical Translation Scenario

During normal operation a network application, such as TELNET, sends an application message to TCP, then TCP sends the corresponding TCP message to the IP module. The destination IP address is known by the application, the TCP module, and the IP module. At this point the IP packet has been constructed and is ready to be given to the Ethernet driver, but first the destination Ethernet address must be determined.

The ARP table is used to look-up the destination Ethernet address.

4.3 ARP Request/Response Pair

But how does the ARP table get filled in the first place? The answer is that it is filled automatically by ARP on an "as-needed" basis.

Two things happen when the ARP table can not be used to translate an address:

1. An ARP request packet with a broadcast Ethernet address is sent out on the network to every computer.

2. The outgoing IP packet is queued.

Every computer's Ethernet interface receives the broadcast Ethernet frame. Each Ethernet driver examines the Type field in the Ethernet frame and passes the ARP packet to the ARP module. The ARP request packet says "If your IP address matches this target IP address, then please tell me your Ethernet address". An ARP request packet looks something like this:

Sender IP Address	223.1.2.1
Sender Enet Address	08-00-39-00-2F-C3
Target IP Address	223.1.2.2
Target Enet Address	<blank>

TABLE 2. Example ARP Request

Each ARP module examines the IP address and if the Target IP address matches its own IP address, it sends a response directly to the source Ethernet address. The ARP response packet says "Yes, that target IP address is mine, let me give you my Ethernet address". An ARP response packet has the sender/target field contents swapped as compared to the request. It looks something like this:

Sender IP Address	223.1.2.2
Sender Enet Address	08-00-28-00-38-A9
Target IP Address	223.1.2.1
Target Enet Address	08-00-39-00-2F-C3

TABLE 3. Example ARP Response

The response is received by the original sender computer. The Ethernet driver looks at the Type field in the Ethernet frame then passes the ARP packet to the ARP module. The ARP module examines the ARP packet and adds the sender's IP and Ethernet addresses to its ARP table.

The updated table now looks like this:

IP address	Ethernet address
223.1.2.1	08-00-39-00-2F-C3
223.1.2.2	08-00-28-00-38-A9
223.1.2.3	08-00-5A-21-A7-22
223.1.2.4	08-00-10-99-AC-54

TA
BLE 4. ARP Table after Response

4.4 Scenario Continued

The new translation has now been installed automatically in the table, just milli-seconds after it was needed. As you remember from step 2 above, the outgoing IP packet was queued. Next, the IP address to Ethernet address translation is performed by look-up in the ARP table then the Ethernet frame is transmitted on the Ethernet. Therefore, with the new steps 3, 4, and 5, the scenario for the

sender computer is:

1. An ARP request packet with a broadcast Ethernet address is sent out on the network to every computer.

2. The outgoing IP packet is queued.

3. The ARP response arrives with the IP-to-Ethernet address translation for the ARP table.

4. For the queued IP packet, the ARP table is used to translate the IP address to the Ethernet address.

5. The Ethernet frame is transmitted on the Ethernet.

In summary, when the translation is missing from the ARP table, one IP packet is queued. The translation data is quickly filled in with ARP request/response and the queued IP packet is transmitted.

Each computer has a separate ARP table for each of its Ethernet interfaces. If the target computer does not exist, there will be no ARP response and no entry in the ARP table. IP will discard outgoing IP packets sent to that address. The upper layer protocols can't tell the difference between a broken Ethernet and the absence of a computer with the target IP address.

Some implementations of IP and ARP don't queue the IP packet while waiting for the ARP response. Instead the IP packet is discarded and the recovery from the IP packet loss is left to the TCP module or the UDP network application. This recovery is performed by time-out and retransmission. The retransmitted message is successfully sent out onto the network because the first copy of the message has already caused the ARP table to be filled.

==Phrack Inc.==

Volume Three, Issue Thirty-Three, File 9 of 13

A Real Functioning RED BOX Schematic

Written by: R.J. "BoB" Dobbs

::What is a Red Box?::

Essentially, the Red Box is a device used to fool the phone company's computer into thinking coins are deposited into a payphone. Every time you drop a coin into a payphone, the phone signals the type of coin inserted with one or more bursts of a combination of 1700hz and 2200hz. The tone bursts are coded as follows:

Nickel : One 60 millisecond pulse
Dime : Two 60 millisecond pulses separated by 60 milliseconds
Quarter: Five 35 millisecond pulses separated by 35 milliseconds

::How to use it::

Simply dial a long distance number (some areas require you to stick in a genuine nickel first), wait for the ACTS computer to demand your cash, and press the "deposit" button on the red box for each coin you want to simulate. The coin signals are coupled from the red box into the phone with a small speaker held to the mouthpiece. For local calls, either you must first deposit a genuine nickle before simulating more coins or place your call through the operator with 0+xxx+yyyy. Use some care when the operator is on the line - sometimes they catch on to your beeper ploy.

::Circuit Operation::

Each time the pushbutton is pressed, it triggers half of IC1, configured as a monostable multivibrator to energize the rest of the circuit for a length of time determined by the setting of the coin selector switch. This in turn starts the other half of IC1, configured as an astable multivibrator, pulsing on and off at regular intervals at a rate determined by the 100k pot between pins 12 and 13. The output of the astable thus alternately powers of IC2, configured as a square wave oscillator, providing the required 1700hz and 2200hz to the op amp which acts as a buffer to drive the speaker.

::Alignment & Testing::

When you are making this thing by no means should you use a 9v AC to DC adapter! I also suggest not using a bread board. So be careful with that sodering iron. Both of these things will cause you problems.

For alignment, a frequency counter is desired but you can use a good oscilloscope as well. (These are not ABSOLUTELY necessary, but to help.) In order to figure frequency in Hz with your scope you can use the following formula.

$$Hz = \frac{1}{S*(T*10^{-6})}$$

S = The measurement of the wave that is on the display

T = The setting of the time selector (milliseconds)

$$Hz = \frac{1}{9.1 * 50ms * 10^{-6}} \quad Hz = 2198$$

Carefully remove IC1 from it's socket. Install a temporary jumper from +9v supply to pin 14 of IC2 and temporarily disconnect the 0.01uF capacitors from pins 5 and 9 of IC2. Power up the circuit. Measuring the output from pin 5 of IC2 with the frequency counter or scope, adjust the 50k pot between pins 1 and 6 for an output of 1700hz. Now adjust the 50k pot between pins 8 and 13 for an output of 2200hz from pin 9 of IC2. Remove the temporary jumper and

re-attach the capacitors to pins 5 and 9 of IC2, and re-insert IC1. (Note: if no frequency counter is available, the outputs can be adjusted by ear one at a time by zero-beating the output tone with a computer generated tone of known precision.)

Next, using a multimeter, adjust the 10K pot at the cathode of the "quarter" diode for resistance of approximately 8K ohms. (This sets the difference between the duration of the quarter pulses and those of the nickel/dime -- fine tuning of this ratio may be necessary durring the latter stages of alignment; this can be done by ear.)

Now, temporarily disconnect the wire between pins 5 and 10 of IC1. Set coin selector switch in the "N" (nickel) position. With the oscilloscope measuring the output from pin 9 of IC1, adjust the 100k pot between pins 12 and 13 of IC1 for output pulses of 60 millisecond duration. Reconnect the wire between pins 5 and 10. (Note: If no scope is available, adjust the pulse rate by ear using computer generated tones for comparison.)

Leave the selector switch in the "N" position. Adjust the 50K pot labeled "Nickel" for a single beep each time the deposit pushbutton is pressed.

Next set the coin selector switch to "Dime". Adjust the 50k pot labelled "Dime" for a quick double beep each time the pushbutton is pressed.

Finally, set the selector to "Quarter". Adjust the 50k pot labelled "Quarter" until exactly 5 very quick beeps are heard for each button press. Don’t worry if the quarter beeps sound shorter and faster than the nickel and dime ones. They should be.

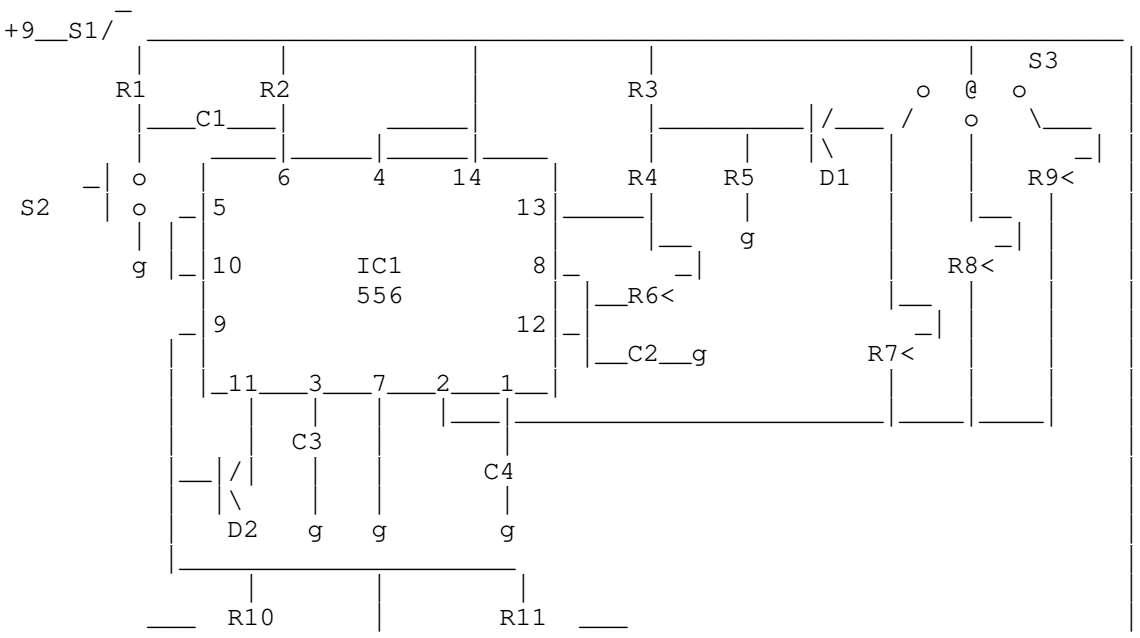
::Conclusion::

If all went well to this point, your red box should be completely aligned and functional. A final test should now be conducted from a payphone using the DATL (Dial Access Test Line) coin test. Dial 09591230 and follow the computer instructions using the red box at the proper prompts. The computer should correctly identify all coins "simulated" and flag any anomalies. With a little discretion, your red box should bring you many years of use. Remember, there is no such thing as spare change!

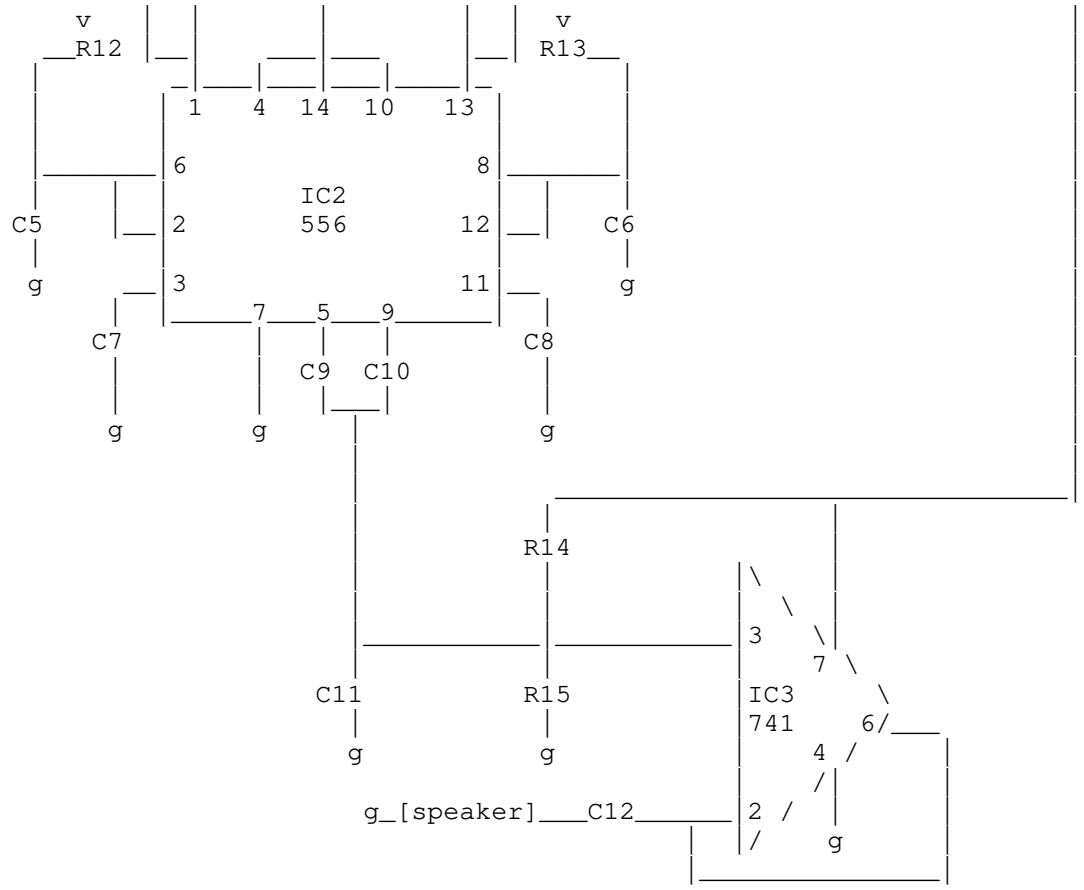
::Parts list for Red Box::

2 556 Dual Timer IC’s	8 0.01uF Caps
1 741 Op Amp IC	2 0.1uF Cap
2 1N914 Diodes	1 1.0uF Electrolytic Cap
5 10k Resistors	2 10uF Electrolytic Caps
1 4.7k Resistor	1 3 Position Rotary Switch
2 100k Resistors	1 SPST Toggle Switch
1 100k PC Mount Pots	1 Momentary Push Button Switch (n/o)
3 50k PC Mount Pot	1 9v Battery Clip
1 10k PC Mount Pot	2 14 Pin Dip Socket
2 50k Multi-Turn Pots	1 8 Pin Dip Socket

::Schematic::



```
        v   |  |        |        |  |  v                                  |
     __R12  |__|     ___|___     |__| R13__                              |
    |        _|___|___|___|____|_        |                              |
    |       | 1   4  14  10   13 |        |                              |
    |       |                    |        |                              |
    |_______|6                  8|_______|                              |
    |    |  |        IC2         |  |    |                              |
   C5    |__|2       556       12|__|   C6                              |
    |       |                    |        |                              |
    g     __|3                  11|__     g                              |
        |  |_____7___5___9______|  |                                    |
       C7        |   |   |        C8                                     |
        |        |  C9  C10        |                                     |
        |        |   |___|         |                                     |
        g        g     |           g                                     |
                       |                                                 |
                       |          ___________________________________|
                       |          |                  |
                       |         R14                 |
                       |          |           |\     |
                       |          |           |  \   |
                       |__________|___________|3   \|
                       |          |           |    7 \
                     C11         R15          |IC3     \
                       |          |           |741    6/___
                       g          g           |    4 /     |
                                              |    /|      |
                        g_[speaker]___C12_____|2 /  |      |
                                          |  |/    g      |
                                          |_______________|
```



::Schematic Parts Code::

R1:10K	R4:10K	R7:50K pot	R10:10K	R13:50K pot
R2:10K	R5:10K	R8:50K pot	R11:10K	R14:100K
R3:4.7K	R6:100K pot	R9:50K pot	R12:50K pot	R15:100K
C1:0.01uf	C4:10uf	C7:0.01uf	C10:0.01uf	
C2:1.00uf	C5:0.01uf	C8:0.01uf	C11:0.10uf	D1 :1N914
C3:0.01uf	C6:0.01uf	C9:0.01uf	C12:10uf	D2 :1N914

S1 - SPST toggle
S2 - Momentary push button Normally Open
S3 - 3-position rotary switch g - Ground

\\?//