E.U.A

Volume One, Issue 4 **New Years Eve Edition**

The newbie's guide to the arts of Hacking, Phreaking, Cypher- & Cryptopunking, w3-surfing, bad-assed type of mag that give people the "inside information." Are you interested? Do you want to know more? The Electronic Underground Affiliations sole purpose is to provide current information about network security, Internet news, information about the local scene and how you fit into it all.

"The reason 'hackers' seek out new knowledge is not for personal profit, but for general knowledge."

Inside this Edition

"AUT HACK VINCERE AUT MORI"

Submission of Articles, Letters, & General BS type of stuff

So you want to write for the Electronic Underground Affiliation? You have some good 411 for the rest of the world and you want a way to share it? Well then you need to get in touch with Archive and let him know! :How do I do that?" you ask? Simple! email article submissions and general letters to:

archive_@hotmail.com

About the New Years Eve Edition & Special Thanks

EUA New Years Eve edition is actually out on time for a change! ! ! Special thanks and to Long Beach, CA 2nd Street Starbucks Coffee for supplying the coffee afterhours while in LA. PostPro for providing lodging and showing me around LA. Apothos for giving some insight into world events, even before CNN knew. Jump0 for helping me find my way. Zarkov for wanting to be in the mix. This Edition of the EUA was cranked out to many hours of editing, research, Coffee, & Raw, Loud and Heavy Tunes and Jams.

FINE PRINT & LEGAL DISCLAIMER: The E.U.A. will, from time to time, contain articles on activities that are illegal. ***WE DO NOT CONDONE ILLEGAL ACTIVITIES.*** This information is provided purely for informational and educational purposes only. E.U.A. and the Information Attic is protected under the First Amendment of the United States Constitution. We do not promote, endorse, or condone the use of any information in this publication for the purpose of illegal or illicit gain. This publication may contain articles and/or topics that may be offensive to some people. If you can not handle these topics PLEASE DO NOT READ THIS PUBLICATION. Again YOU should NOT participate in any actions that can be construed as illegal by the United States, Regional, and Local Governments. This information is purely for educational and informational use only.

With that, the lawyers & judges should be happy.

Freedom of Information and Right to Privacy ! ! !

Remember privacy is a right! Don’t allow your privacy to be taken, make it a part of your everyday life. The E.U.A. staff endorses the use of PGP. If you need help with encryption or cryptography feel free to contact us for help. The use of encryption in today's “online” society ensures that your information being passed through the many switches, networks and hubs is secure against theft, tampering, and most of all ensures your privacy of what you are discussing. If you want to remain free use public key encryption and support cryptography!

Fight for Internet Freedom of Speech

Looking for a Mentor?

Are you looking for a mentor and a teacher in the dark arts of hacking and phreaking? Want to learn all you can about how computer and telephone networks really work? Well join us on irc.xnet.org in #ASHE or #EUA and join in. Old School Style or hit our web sites at one of the:

EUA & ASHE
http://members.xoom.com/archive_/
http://www.cryogen.com/ASHE

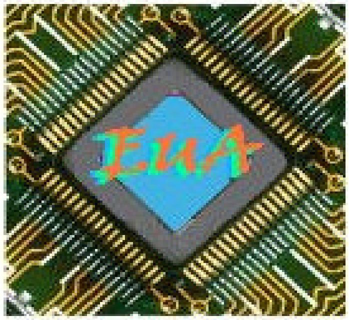
FREE KEVIN

Freedom of Information

Know your rights! Information that has been restricted from public knowledge can now be requested and provided by the members of ASHE and the EUA. We operate solely on the basis of Freedom of Information. Our rights as citizens allow us to freely exchange Information and Ideas so if you are looking for something check us out and let us know what is the 411. L8R All

Who are we? ASHE & EUA

American Society of the Hacker Elite We are here to unite hackers from all over the world. Our main goal is to provide a safe and legal environment where hackers can share information. We run on a strictly legal basis, thus there is no risk of legal actions being taken against our members. We allow **no** hacking to be done in association with our organization. If you decide to do any illegal hacking, it is your on decision and we are in no way responsible for your actions. This organization merely unites hackers and allows the sharing of information for educational purposes. We also share information with businesses to help them to prevent hacking on their local networks. By sharing hacking information we better understand how to safeguard systems against hacking attempts. And what better way to learn than from others that have knowledge in the many fields of hacking.



Electronic Underground Affiliation is a organization that was originally started in the early '90's by a few of the Chicagoland hacker's who were started to get disgusted with societies sudden plunge into the realms of the bit and the baud. Tired of the way things were going Archive, Highlander, Fringe, Subhuman, and about a dozen others in the Old School Chicagoland Hacker Community decided to form the Electronic Underground Affiliation (EUA) in a way to guide, leading the next generation of hackers into the dark arts and mystery of hacking — old school style. Basing our ethics on the old school beliefs, the EUA has grown by leaps and bounds. The EUA is aimed itself at aligning and organizing various cells of hacker's, phreaks, cipher-&cryptopunks throughout the world. The EUA is predominately made up of old school hackers & phreaks that act in various positions from mentors to information brokers to coders. We are an organization that cares about the Freedom of Information and the continued Free Exchange of Ideas.

L0pht Heavy Industries Advisories

Lotus “Domino Security Flaw”

this is a
L0pht Security Advisory

URL Origin: http://www.l0pht.com/advisories.html
Release Date: October 9th, 1998
Application: Lotus Domino
Severity: Web users can retrieve sensitive data in many Domino based Internet applications
Author: nardo@l0pht.com
Operating Sys: All platforms

I. Description

The L0pht has received reports regarding a vulnerability in some implementations of Domino based applications which result in the internet publication of sensitive information belonging to customers of Lotus/IBM and their business partners. This information is widely available to anyone with a web browser and includes such things as credit card numbers, addresses, phone numbers, etc. The information about this vulnerability has been posted to various public mailing lists and newsgroups.

The vulnerability affects websites created by Lotus Business Partners who provide training services and accept credit card numbers via the web; however, in theory the vulnerabilities could extend to any e-Commerce site. Several Lotus' Business Partners were confirmed to be affected by this.

This advisory does not attempt to place blame on the software vendor or on the application developers. Many will see this as a flaw in the design or documentation of the product and many will see this as ignorance on the part of the web site builders. This advisory is designed to alert consumers that they should be wary on putting sensitive information into internet web applications. The consumer has no way of knowing if the web application has been designed to correctly protect that data from anonymous internet access.

II. Details

Web users can navigate to the portion of the site used for processing registration and/or payment information and remove everything to the right of the database name in the URL (the databases typically end in .nsf.) In one example of this vulnerability, all the database views were then exposed which included a view containing previous registrations and a view containing "All Documents". These views could then be accessed by clicking on the link and browsing the data within the view (typically consisting of business and customer names, addresses, phone numbers, and payment information.)

In another example, the views were protected from direct browsing, but could still be searched using the standard URL format for searches in Domino. This particular method would then allow the database to be searched for everyone who paid with a specific credit card or everyone who lives within a certain city.

II a. To Test

Navigate through a Domino site, and once a database has been accessed, remove the information after the .nsf or after the first set of numbers following the server portion of the URL and replace it with "?Open". If you are then presented with a list of views, your site is potentially vulnerable to having anonymous users access the information contained within the views listed. Lotus recommends blocking this access through a $$ViewTemplateDefault. If this technique is used, the second vulnerability comes into play, which is to access the view by using the following URL format: "http://www.server.com/database.nsf/viewname?SearchView&Query="*" ". This technique will bypass the $$ViewTemplateDefault if the database is full-text indexed. Many full text indexed sites were found vulnerable to this "feature" that their developers didn't plan for.

III. Solution

The sites affected could have been protected using reader and author names fields to prevent unauthorized access to their client's sensitive data. The internal registration views could've been hidden from anonymous users.
They should've included a $$SearchTemplateDefault with no $$ViewBody field to block any unwelcome searching. Additionally, every Domino site should disallow anonymous access for at least these databases: names.nsf; catalog.nsf; log.nsf; domlog.nsf; domcfg.nsf.

For specific questions about this advisory, please contact nardo@l0pht.com

----
For more L0pht (that's L - zero - P - H - T) advisories check out:
http://www.l0pht.com/advisories.html
----

some tips on trashing

submitted by BrainKandy

(borrowed from Columbia 2032)

Go on the day before trash pickup around 6. Light drizzle always helps as you won't be soaked, and the garbage won't get damaged or get stunk up, but no one wants to be out then.

Bring a knife of any kind to rip the bags open. Also bring a book bag. I have one from an Army surplus store than can hold a 75% filled garbage bag... that's with the bag. I suggest this and not a school bag par se. You need bout three school bags, big-pocketed cargo pants and huge hands to equal two army surplus bags. These only cost about $10. Medical Gloves (plastic, tight fitting, powdery ones) are good for keeping prints off the can. If you're going somewhere with the possibility of glass or that sort, thick rubber or leather gloves work best, but you can't grab well with them. I go in my normal clothes simply because I wear shit that you can't really tell if anything's on it. But I would think you should use a pair of old sweats and a big sweatshirt over your normal clothes, if you get caught and are chased, you can ditch them somewhere and not think about losing' good stuff, like a new Flannel or something. This also keeps your clothes (underneath) clean. As for a disguise, wear sunglasses, just from the hell of it, and baggy clothes will hide your height (sort of) and weight (damn near totally).

I grab anything when I start trashing a place. Some people read it on site, but my magic number at any one Locale is 15 minutes. Any more and you're asking to get caught, any less and you won't get enough for the trouble. Once you trash at a place a few times, you learn common friend to friend formats versus memo's and even learn to judge the importance of memo's or letters. I know what a fax from any one area to another looks like and what a serious memo is. You have to learn to spot, any semi-neat pile that has one or two friendly memo's really ain't worth it once u have a couple of names of people working there. Given a lot of scheduled things are useful on those and sometimes they may put passwords and dialups on there, but for the most part its nothing. After you get to be picky (but quick) you can look for specific things, Hand written anything is good, but you want to strangle the people whose writing you can't read. Any manuals you find are GREAT finds and I suggest running once you think you got the last one, as you DON'T want to get caught on premises

with that.
Trashing a Truck is tricky; I've only done it once and was damn near shitting in my pants when I did. Some people will break into a van with a rock or whatever, then just grab two things with an alarm blaring and run. That's fine for petty vandals, but we're hackers, that car is a system if not computer. It's an interacting set of parts. If the door is open, open it QUIETLY and quickly look to your right if you went in through the non-cockpit right side. There should be a bank of manuals, I had a cluttered one but all shouldn't be like that. This was only in the repair truck we saw, but the van had the tool place built in, so I think that's the normal place for everything. The Linemen's handset will be either right by the side door or back. Or both. Again this was my experience but those are also the only logical places for things. If it was unlocked then you grab your shit and you RUN. The truck we had was gone in 15 minutes, so you get in, get out, and get MOVING.

Runs are dangerous, don't go with less than 2 people. A third person is a good idea anywhere that you go, which means you can have a second searcher or have a second lookout. But only three for a truck since that's a felony and then they can identify more people. If you go trashing, bring as many people as possible. This is good for two reasons. First, you can look like just a group of kids goofing off to anyone looking, (if one of you is underage and smokes, you can use this as an excuse for being in an alley or whatever, they'll say "Don't do that" and shoo you away). And second you can move entire bags into a dark ally or whatever if you have multiple people. Trashing shouldn't be limited to hackers or phreaks or whatnot only. Bring anyone who really wouldn't care about the stuff in there, and who will take risks.

If you get caught, the most you can get charged with is trespassing that I know of, and if they don't have a "private property" sign, you can use that. They, realistically, won't bother pressing charges. Maybe call your folks or something. No biggy.

-
B R Alt F4 N K Alt N
D F14 -

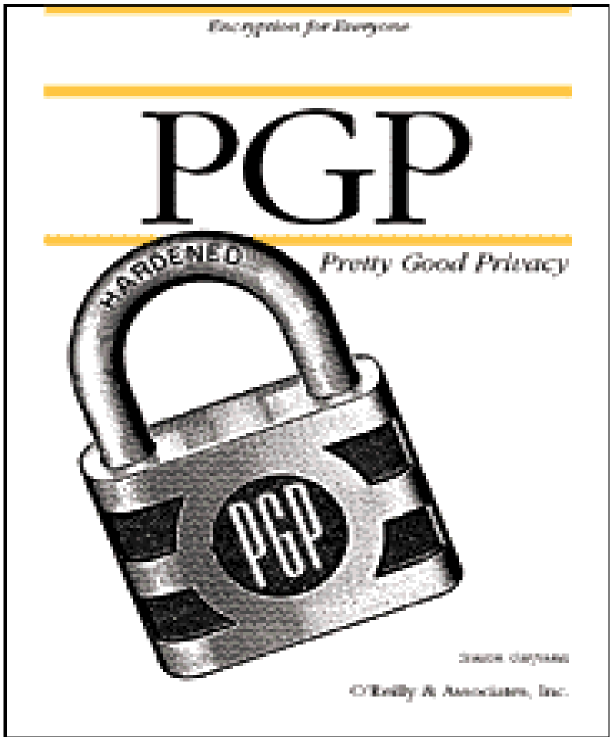
FREE KEVIN MITNICK
www.kevinmitnick.com
'stop the violence, hack the planet'

e-mail:
brainkandy@mindspring.com
icq, *aim*, and *irc* upon request

Remember that it doesnt hurt to look through other peoples garbage. You never know what you might find laying around in a garbage can. Of course if you hit a really cool place such as a telco, it probably wont look as nice as my trash can here.

The PGP symmetric algorithms

provided by Archive



Alright tech heads, this article get's into the guts of the PGP encryption program that I so push when I talk to you guys. This should provided you with some information that will keep you biting on your gums for a while.

PGP offers a selection of different secret key algorithms to encrypt the actual message. By secret key algorithm, we mean a conventional, or symmetric, block cipher that uses the same key to both encrypt and decrypt. The three symmetric block ciphers offered by PGP are CAST, Triple-DES, and IDEA. They are not "home-grown" algorithms. They were all developed by teams of cryptographers with distinguished reputations.

For the cryptographically curious, all three ciphers operate on 64-bit blocks of plaintext and ciphertext. CAST and IDEA have key sizes of 128 bits, while Triple-DES uses a 168-bit key. Like Data Encryption Standard (DES), any of these ciphers can be used in cipher feedback (CFB) and cipher block chaining (CBC) modes. PGP uses them in 64-bit CFB mode.

The CAST encryption algorithm in PGP because shows promise as a good block cipher with a 128-bit key size, it's very fast, and it's free. Its name is derived from the initials of its designers, Carlisle Adams and Stafford Tavares of Northern Telecom (Nortel). Nortel has applied for a patent for CAST, but they have made a commitment in writing to make CAST available to anyone on a royalty-free basis. CAST appears to be exceptionally well designed, by people with good reputations in the field. The design is based on a very formal approach, with a number of formally provable assertions that give good reasons to believe that it probably requires key exhaustion to break its 128-bit key. CAST has no weak or semiweak keys. There are strong arguments that CAST is completely immune to both linear and differential cryptanalysis, the two most powerful forms of cryptanalysis in the published literature, both of which have been effective in cracking DES. CAST is too new to have developed a long track record, but its formal design and the good reputations of its designers will undoubtedly attract the attentions and attempted cryptanalytic attacks of the rest of the academic cryptographic community. I'm getting nearly the same preliminary gut feeling of confidence from CAST that I got years ago from IDEA, the cipher I selected for use in earlier versions of PGP. At that time, IDEA was also too new to have a track record, but it has held up well. The IDEA (International Data Encryption Algorithm) block cipher is based on the design concept of “mixing operations from different algebraic groups.” It was developed at ETH in Zurich by James L. Massey and Xuejia Lai, and published in 1990. Early published papers on the algorithm called it IPES (Improved Proposed Encryption Standard), but they later changed the name to IDEA. So far, IDEA has resisted attack much better than other ciphers such as FEAL, REDOC-II, LOKI, Snefru and Khafre. And IDEA is more resistant than DES to Biham and Shamir’s highly successful differential cryptanalysis attack, as well as attacks from linear cryptanalysis. As this cipher continues to attract attack efforts from the most formidable quarters of the cryptanalytic world, confidence in IDEA is growing with the passage of time. Sadly, the biggest obstacle to IDEA’s acceptance as a standard has been the fact that Ascom Systec holds a patent on its design, and unlike DES and CAST, IDEA has not been made available to everyone on a royalty-free basis. As a hedge, PGP includes three-key Triple-DES in its repertoire of available block ciphers. The DES was developed by IBM in the mid-1970s. While it has a good design, its 56-bit key size is too small by today’s standards. Triple-DES is very strong, and has been well studied for many years, so it might be a safer bet than the newer ciphers such as CAST and IDEA. Triple-DES is the DES applied three times to the same block of data, using three different keys, except that the second DES operation is run backwards, in decrypt mode. While Triple-DES is much slower than either CAST or IDEA, speed is usually not critical for email applications. Although Triple-DES uses a key size of 168 bits, it appears to have an effective key strength of at least 112 bits against an attacker with impossibly immense data storage capacity to use in the attack. According to a paper presented by Michael Weiner at Crypto96, any remotely plausible amount of data storage available to the attacker would enable an attack that would require about as much work as breaking a 129-bit key. Triple-DES is not encumbered by any patents.

PGP public keys that were generated by PGP Version 5.0 or later have information embedded in them that tells a sender what block ciphers are understood by the recipient’s software, so that the sender’s software knows which ciphers can be used to encrypt. Diffie-Hellman/DSS public keys accept CAST, IDEA, or Triple-DES as the block cipher, with CAST as the default selection. At present, for compatibility reasons, RSA keys do not provide this feature. Only the IDEA cipher is used by PGP to send messages to RSA keys, because older versions of PGP only supported RSA and IDEA.

Known bugs in PGP 5.5.3i for Windows 95/NT

Outlook Plugin

Don't use the plugin with Outlook 98! Your mail may go out unencrypted!

Outlook Express Plugin

The Outlook Express plugin is very buggy running on Win NT 4 - SP3. Look here for details.

Problems building the installer

The setup.rul file included with the Windows source code distribution contains a couple of errors. This file worked for me. I also had to modify build.bat to get it to work on my NT 4 box.

Too long Version: line in ASCII armor

The Version: line of 5.5.3i is 72 characters long (because of the "i" in 5.5.3i and www.pgpi.com). Many mail programs and news readers default to word wrap at 70. Thus if you are using cut and paste <http://www.pgpi.com> ends up on a different line. If verifying or decrypting with 5.5.3 or 5.5.3i this does not matter. However if the recipient is using 2.6.3(i) he/she will get an invalid signature or similar error.

The simplest solution is to increase word wrap to 72 characters.

“N I P C?”

straight from the www.fbi.gov website

FEDERAL BUREAU OF INVESTIGATION

The mission of the NIPC is both a national security and law enforcement effort to detect, deter, assess, warn of, respond to, and investigate computer intrusions and unlawful acts, both physical and "cyber," that threaten or target our critical infrastructures.

The NIPC's job is not simply to investigate and respond to attacks *after* they occur, but to learn about them *beforehand* and prevent them.

"The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means for facilitating and coordinating the Federal Government's resources to an incident, mitigating attack."

President William Clinton
Presidential Decision Directive 63,
May 22, 1998

"Critical Infrastructures" are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

President William J. Clinton,
Presidential Decision Directive 63, May 22, 1998
Executive Order 13010, July 15, 1996

Well recently I’ve been getting a lot of questions to the basic idea of “Well what can the FBI or Secret Service bust me for:” and what is considered “Really Bad” by governmental standards. So I decided to do a little research and find out just what the FBI considers “critical to survival” So here is some 411 for all you neophytes who want to know the low down on it.

- Forward & Research by Apothos

DEFINITION OF A CRITICAL INFRASTRUCTURE

A critical infrastructure characterized by computing and telecommunications equipment, software, processes, and people that support:

- the processing, storage, and transmission of data and information,
- the processes and people that convert data into information and information into knowledge, and
- the data and information themselves

Banking and Finance: A critical infrastructure characterized by entities, such as retail and commercial organizations, investment institutions, exchange boards, trading houses, and reserve systems, and associated operational organizations, government operations, and support activities, that are involved in all manner of monetary transactions, including its storage for saving purposes, its investment for income purposes, its exchange for payment purposes, and its disbursement in the form of loan and other financial instruments.

Water Supply: A critical infrastructure characterized by the source of water, reservoirs and holding facilities, aqueducts and other transport systems, the filtration, cleaning and treatment systems, the pipeline, the cooling systems and other delivery mechanisms that provide for domestic and industrial applications, including systems for dealing with water runoff, waste water, and firefighting.

Transportation: A critical infrastructure characterized by the physical distribution system critical to supporting the national security and economic well-being of this nation, including aviation; the national airspace system; airlines and aircraft; and airports; roads and highways, trucking and personal vehicles and intelligent transportation systems; waterborne commerce; ports and waterways and the vessels operating thereon; mass transit, both rail and bus; pipelines, including natural gas, petroleum, and other hazardous material; freight and long haul passenger rail; and delivery services.

Emergency Services: A critical infrastructure characterized by medical, police, fire, and rescue systems and personnel that are called upon when an individual or community is responding to emergencies. These services are typically provided at the local level (county or metropolitan area). In addition, state and Federal response plans define emergency support functions to assist in response and recovery.

Public Health Services

- Prevention
- Surveillance
- Laboratory Services
- Personal Health Services

Continuity of Government Services: Sufficient capabilities at the Federal, state and local levels of government are required to meet the needs for essential services to the public.

Electrical Power: A critical infrastructure characterized by generation stations, transmission and distribution networks that create and supply electricity to end-users so that end-users achieve and maintain nominal functionality, including the transportation and storage of fuel essential to that system.

Oil and Gas Production and Storage: A critical infrastructure characterized by the production and holding facilities for natural gas, crude and refined petroleum, petroleum-derived fuels, and the refining and processing facilities for these fuels.

Remote Explorer: Attack on MCI Network Systems

I DON T THINK IT S HYPERBOLE TO CALL THIS AN INFORMATION TIME BOMB, HODGES SAID.

SECURITY EXPERTS FROM NETWORK ASSOCIATES Inc. described it as a “new era in the virus field ... an entirely new kind of virus.”
Once in place, Remote Explorer wreaks havoc by encrypting files on users machines — from programs to text files. These were not destroyed, however, and Network Associates says it will soon have a fix on its Web site which can restore the encrypted files.
The “smart virus” attacks Windows NT-based networks and propagates over the local network, said Gene Hodges, a general manager at Network Associates in Santa Clara, Calif.
Remote Explorer goes by the file name IE403r.sys and utilizes NT’s remote management tools to act like a human network administrator. It then orders copies of itself around the network. Once on a workstation, it loads a process into Task Manager.
“To someone not suspecting this, you wouldn’t notice Remote Explorer just sitting as a service,” said Vincent Gullotto of Network Associates. “If you do discover it, you can’t close it down.”
The virus had been running for at least a week before detection, the company said.
It was unclear whether the virus was downloaded from the Internet or planted on a server internally. Because part of the source code of the virus was encrypted, it will be difficult to determine the motivation of its author. Files encrypted by the virus were apparently chosen at random.

THE VIRUS COMPRESSES THE EXECUTABLE FILES OF SERVERS AND WORKSTATIONS THAT IT ENCOUNTERS, RENDERING THEM UNUSABLE. IT ALSO ENCRYPTS .DOC OR .XLF FILES.

But a spokesman for Computer Associates said the program was too sophisticated to be the work of indiscriminate pranksters.
“These guys were very smart,” Hodges said. The company estimates the program took 200 hours to write. “They had a good enough idea of where to put it in order to make it spread very quickly.”
The virus compresses the executable files of servers and

IT CANNOT PROPAGATE IN A UNIX OR NETWARE-BASED NETWORK.

workstations that it encounters, rendering them unusable. It also encrypts .DOC or .XLF files with a cipher that researchers still have not identified, making it impossible to gain access to those files, Hodges said

“Clearly, we don’t know who developed this virus,” he said. “But it’s clear as to how it was first planted and how it spreads and that this person was very knowledgeable of network administration features and planned for this virus to cause serious damage.”

The virus itself, which is written in C and also partly encrypted, is a savvy piece of programming, Hodges said. It logs itself in through domain administrative controls and then copies itself over the network, attacking other servers and even workstations that access those servers. It can use any link that can identify NT resources. It cannot propagate in a Unix or NetWare-based network.

It is also huge by virus standards at 120KB. Discovered Thursday, it was operating on a timing mechanism so that it propagated faster between 3 p.m. and 6 a.m. — hours when network administration staffing is typically lower at the infected company. The company severed its WAN connections in order to isolate the problem.

“It’s clear that the virus writer has a good Unix and NT background,” Hodges said.

Researchers at Network Associates say they have broken the compression algorithm and will post a fixing technique that is specific to Network Associates software by early this afternoon. Peter Watkins, general manager, Network Security Division, said the virus did not destroy any data — the fix will be able to restore infected, encrypted files.

A detector for the “smart virus” has already been posted. Hodges said the company is working with Microsoft Corp., has also been in touch with other anti-virus groups and is developing a formal warning. “I don’t think it’s hyperbole to call this an information time bomb,” Hodges said.

WinGate

Connect your entire LAN to the Internet with just one modem !!

of course once the EUA would have to add a little twist to the normal operation to it

How to Wingate

Brought to you by

-=Zarkov=-

So you've seen people on IRC or where ever using other hostmasks and wondering HOW THE HELL do they do that? Well, the answer isn't that difficult. But first some background on how it is possible- it's possible because of the program WinGate that many users have installed to use the same modem for two or more computers. But WinGate has a bug. This bug allows people to connect to someone using WinGate and use them as a shell. The process is quite simple. First, you must find someone using WinGate. This can be done either by:

1. Using a domain scanner to search for services running on port 23, or
2. DNSing the target and searching their ISP's nodes (ie. 0.0.0.* in intervals of 5 and trying to connect to them).

Method 1 works much better, but if you don't have a scanner Method 2 will do. Once you have acquired a target, connect to them with Telnet on port 23. You should get a WinGate> prompt. If you don't get a prompt you must not have gotten a valid target, try again. At the WinGate> prompt, type a server you'd like to connect to, followed by the port number. You will be connected from the WinGate user's IP. Anyone ready for some password guessing? :)

SecurID's discussed

BASIC USE AND UTILIZATION.

pimped for you by
fringe

Background:

SecurID's are credit card-like security devices used by many large corporations in order to verify user authentication when a user is calling in to a proprietary computer system. These are approximately the same size as a credit card and they have an lcd on them.

This is an overview of how they are utilized.

---

communication settings

The following settings are required for the authentication server:

Parity	None
Data bits	8
Stop bits	1
Duplex	Half
Flow Control	On

you will need a normal terminal program to call the system, however a lot of corporations have specialized software for mac's and pc's to make it more user friendly for their employees.. you may have heard of appletalk software and other such programs that are vastly used by corps.. these gui's can be helpful to have in case you are having trouble "getting in". they usually have a few scripts to run for this and that.. everything's point and click... blah blah blah.. back to the issue at hand.

call the SecurID dial-up that you have.. and you do need this in order to use the card.

```
CONNECT 14400
```

to activate it.. do the following if you can't get it to work right off the bat:

when prompted for Username:, you need to type the correct login that is used to activate that corp/company's card. most of them use the account 'activate' without the 's of course.

At the login: prompt type your SecurID userid in lower case. At the Enter PASSCODE prompt type the digits shown on the SecurID. you will then be prompted to enter your PIN code;

- this will be your 4 to 8 digit Personal Identification Number

- only numbers can be used, without leading zeroes

You will then be prompted to confirm this number by re-entering it

You will be prompted to wait for the displayed number on your card to change, then enter the PIN chosen above followed by the number displayed on your SecurID card.

If you were successful, the following will be displayed:

```
*NOTICE*
Your SecurID card has been verified and turned on....
Please press enter to exit....
ACCEPTED
```

go ahead, press enter. You should get the following response:

```
Connection closed by foreign host (WOW!)
```

Call back up to start a new normal good vibes session.

At the Username: prompt enter in the SecurID userid in lower case. At the password prompt enter your PIN and SecurID card number together, without anything between them (for example: 123456999999 where 123456 is your PIN and 999999 is da numba displayed on the card). At this point, you will be at a terminal server prompt, and from here on it depending on what corp/company you're in, there are different things to do. nonetheless, at this point, you're 'in' the system hopefully successfully.

problem?

receiving message Access Denied when logging in with SecurID?

- you probably entered the PASSCODE wrong

- your card could have been clicked off due to 3 invalid logins in a row

- your SecurID has become out of sync with the authentication server.

have fun.. some of the largest peoples using this include telco's..
and when their cards are found.. well they usually tend to leave all the info with it.. telco people are slow like that.

The following has been provided as a courtesy of the SecurID Web Propaganda Site

These first 7 Steps Will Be Required One Time Only

1. Enter your UserID in the UserID field (John Doe = jdoe)
2. Enter the 6 digit tokencode **(number showing on your token)** in the Passcode field.
3. Press Send.
4. Create your own 4-8 digit PIN **(cannot begin with zero)**
5. Re-enter your new PIN for verification.
6. Press Send.
7. **Wait 60 seconds or until the number on your token changes.**

HACKING ARAPANET Part 1

BY

The Source

STRAIGHT FROM THE
CATACOMBS OF ARCHIVE COMES
AN OLDIE BUT GOODIE

INTRODUCTION

ARAPANET (Advanced Research Projects Agency NETwork) was funded by the Department of Defense (DOD) in 1969 as an experiment in sharing the resources of many different types of computers. Earlier DOD systems (AUTODIN,for example), relied on linking computers that were the same make, using the same operating systems. Work on ARAPANET was performed under contract by many organizations, including educational institutions, and today it is universities who are the primary network users.

Once logged onto ARRANT a user may conference with, or use the program resources and available data files of any other computer that is on the system. Hundreds of computers are available over ARRANT including computers at non-university research centers like Rand Corporation, SRI and other military-industrial think tanks.

Until late 1983 and early 1984, military computers were also a major ARRANT resource. With the threat from young computer "hackers", however, the military computers have moved to their own ARRANT-like network called MILNET. The two networks are now part of what is known as the "DDN" or Defense Data Network. ARRANT nodes may be used to dial-up MILNET nodes as long as the caller can enter the proper authorization code and password once connected to the MILNET node. MILNET users can, likewise, use ARRANT resources.

ARRANT is also used as a resource for students as well as computer scientists and engineering specialists. Because of the variety of users, the system tends to be very talkative about itself and very helpful. Periodically, however, certain ARRANT nodes decrease the amount of help that they provide online.

Despite the fact that dozens of different types of computers are interfaced in ARRANT, it is a simple system to use because all nodes (called TIP's), use fundamentally the same operating systems on either DEC (Digital Equipment Corporation) models 20 or 10 mainframes. The operating system is called the "EXEC" and is called the TOPS-20 Monitor (on the DEC 20).

Access numbers for local ARRANT nodes can be found from users of certain bulletin boards, by calling the system manager, or by asking someone who attends a major university.

GETTING ON

Once connected to the system, hit <CR> once for 300 baud or twice if you are using 1200 baud. The EXEC then recognizes you and displays a welcome message as below:

```
WELCOME TO ARRANT
**FOR OFFICIAL USE ONLY**
Call the NIC at 1-800-235-3155 for TAC user problems.
Type @n for news.
SU TAC 110 #:13
```

At this point there are only two commands that the Exec will recognize: @N for news, and @O for onto the host system. Start by checking out the news. The node you have reached may be willing to be very helpful and informative.

NEWS FROM THE EXECUTIVE

A sample executive session follows below:

```
    @N  <user entry>
    TCP Trying...Open
    SRI-NIC, TOPS-20 Monitor 5.3(5731)-1
    *  For TACNEWS, enter:  tacnews<RETURN>
    *  To find the host administrator for host xy-z, enter:  whois xy-z<RETURN>
    *  Report system problems to Action@SRI-NIC or call (415) 859-5921
    There are 7+12 jobs with load average  1.13

@TACNEWS  <exec provides @ prompt, user replies "tacnews">

    SRI-NIC TACnews 1.3(15)-2 on Sunday, 23-Sep-84 11:13pm-PDT
    Send bugs or comments to TACNEWS@SRI-NIC.ARPA
    1. Announcements (updated 14-Sep-84)
```

```
        2. Dial-Ups (MILNET TAC telephone numbers, updated 17-Sep-84)
        3. Login (Help with TAC login, updated 24-Aug-84)
        4. Newsletters (DDN News, updated 24-Jan-84)
         5. Bulletins (DDN Management bulletins, updated 17-Sep-84)
Type a menu number ('HELP<CR>' for more info): HELP
```

The NetNews program lets you access sets of news files at the DDN Network Information Center (NIC). So far, you have entered the program and seen a menu of available sets and documents. Documents are marked in the menu with a '*' in the first column. To view a document, or browse through a set, type its menu number followed by carriage return, <CR>. If you choose a set, you will then be shown a summary of the most recent issues, and by typing its menu number may read the item. Type 'TOP<CR>' at any time to get back to the first menu.

useful commands are:

```
    ?                    To see a list of commands
    ^O (control-o)       To stop the typeout of an issue
    HELP                 To get more information
    TOP                  To return to the beginning menu
    QUIT                 To exit

        Terminate all commands, except '?', with a carriage return, <CR>.
```

<monitor then returns to the menu and we type QUIT so we can learn what else is available to someone who has not logged in.>

```
        Killed Job 34, User TACNEWS, Account QUERY, TTY 110, at 23-Sep-84
        23:15:47
        Used 0:00:01 in 0:01:53
        Host closing connection
        Closed
```

GETTING HELP

<Each function is treated as an unique job. The HELP command is part of the QUERY program. A log report is made when the user QUITs. The user must then begin all over again with the @N prompt, read the herald again, and then proceed to other options when the system responds with its own @ prompt. We skip these redundancies in this example.>

```
        @HELP  <user enters HELP>
```

To see a list of your options for commands or arguments, try typing question mark. Typing "?" to the "@" prompt gives you a list of the commands the Exec understands. Typing "?" after one of these commands tells you what you can type next. For example,

```
@HELP ?
```

will show you a list of some of the more important topics for which Help is available. The question mark invokes a help message without affecting what you've typed so far; you can go on typing the command just as if you hadn't typed "?". Also, the question mark is read immediately; you don't have to type RETURN.

If you make a mistake while typing a command, use BACKSPACE to delete the last character you typed. Ctrl/W will delete your last Word, and Ctrl/U will delete your entire command line, allowing you to start again. If you feel hopelessly lost, typing Ctrl/C twice will return you to the Exec "@".

```
@HELP ? RETURN for general help
or * to see all topics
or the name of an EXEC command
or one of the following:

ATTACH        BLANK         BREAK         DAYTIME    ECHO
FINGER        HELP          INFORMATION   KK         LOGIN
LOGOUT        NIC           SET           SYSTAT     TACNEWS
TERMINAL      UNATTACH      WHOIS
```

<above is a list of the help files available at this particular session. At other times either more or fewer files are available.>

E. U. A.

Electronic Underground Affiliation

A .S.H.E.

American Society of the Hacker Elite

The Electronic Underground Affiliation is aimed at setting a new standard in the hacker community based on the old school idea for the "Free Exchange of Information and Ideas."

ELECTRONIC UNDERGROUND AFFILIATION AND THE AMERICAN SOCIETY OF THE HACKER ELITE

Idea:	The Free Exchange of Information and Knowledge.
Purpose:	To Ensure that Information and Knowledge are available to anyone seeking.
Goal:	To enlist the assistance, wisdom, knowledge and information of as many IS specialists, hackers, crypto- &cypherpunks, users as possible.
Ethic:	Unlike society, the EUA does not be hindered by the social stigmas of our day. We will not discriminate others on the basis of: 1) Sex, 2) Race, 3) Religious Beliefs, 4) Affiliation, 5) Physical Impairments, or 6) Age.

The Moto: Aut Hack Vincere Aut Mori

E.U.A. Staff & Shout Outs

ß-Editor/Publisher.	**Archive**
SoCal Digital Publishing	**BRaiN KaNDy**
	PostPro
Northern IL Digital Publishing	**Highlander**
Chicagoland Digital Publishing	**Subhuman**
	Fringe
NC Digital Publishing	**Aptohos**
PA Digital Publishing	**CyberMonk**
OR Digital Publishing	**Phrack Wolf**
Canadian Digital Publishing	**Zarkov**
Australian Digital Publishing	**Fs0**

Special Thanks and Credits go to the following for their article submissions and help with publication for this months edition of the E.U.A.:

Apothos — Conspiracy Theorist & Slut
Zarkov — How to Wingate
Jump0 — For helping me find my way.
Fringe — Chicagoland Support

Visit our website @
http://members.xoom.com/archive_/