EUA

Volume Two, Issue 2 March 25th, 1999

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

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

You want to write for the EUA Monthly? You have some good 411 for the rest of the world and you want a way to share it? How do I do that?" you ask? Simple! email article submissions and general letters to: archive_@hotmail.com

About this Edition of the EUA Monthly

Well things have gotten a little wild and crazy after my trip down to Peurto Rico. It looks like the leader of ASHE has disbanded the orginazation, a splinter faction called p3ni5 has started to fill the role now. Well, I have about two weeks until I have my trip to Europe. Raven has agreed to help take over the press and publications to get the Zine out to you. I'll be keeping in touch primarily through e-mail and working the publications while I am in the euro-land. I'd like to take the time to thank the following: The staff at HNN, the Hacker News Network, and the staff of the 719 hacker group, thanks for the additions to our little zine. Thanks go out to Dildog of L0pht Heavy Industries for the advisory. I want to give shouts out to Raven for her support in helping get this pub out, Durab and Fade2Black for branching off and keeping the community alive. I don't know how much of an impact that

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.

Fight for Internet Freedom

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 #EUA and join in. Old School Style or hit our web sites at one of the:

http://www.freespeech.org/eua/

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 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

The EUA Monthly will be reposting information from HNN, the Hacker News Network. Their mission: The Hacker News Network's mission is twofold. Our first mission is to deliver the real news from the computer underground **for** the computer underground. The reporting will not be dumbed down to match the computer illiteracy of the average TV viewer. Our second mission is to report the activities of the underground without the biases of the mainstream media. You will not see the terms "hacker" and "criminal" used interchangeably, nor the phrases "brilliant misguided youth" and "script kiddie". The HNN site is updated every day, except weekends and holidays with the latest news effecting the hacker scene. We try to have the days update posted before 12 noon EST. If you want to share something cool you have seen or

Who are we? EUA

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

Document: L0phT Security Advisory
URL Origin: http://www.l0pht.com/advisories.html
Release Date: February 18, 1999
Application: Microsoft Windows NT 4.0
Severity any local user can gain admin privileges
Author: dildog (dildog@l0pht.com)
Operating System: MS Windows NT 4.0

---
Overview :
---

Microsoft Windows NT 4.0 implements a system-wide cache of file-mapping objects for the purpose of loading system dynamic link libraries (DLLs) as quickly as possible. These cache objects, located in the system's internal object namespace, are created with permissions such that the 'Everyone' group has full control over them. Hence, it is possible to delete these cache objects and replace them with others that point to different DLLs.

When processes are created, the loader maps/loads the loading executable's imported DLLs into the process space. If there is a DLL cache object available, it is simply mapped into the process space, rather than going to the disk. Hence, there is an exploitable condition, when a low-privilege user replaces a DLL in the cache with a trojan DLL, followed by a high-privelege account launching a process. The high priveleged process will map in the trojan DLL and execute code on behalf of the low privelege user.

---
Affected systems:
---

Windows NT 4.0 Server SP4
Windows NT 4.0 Workstation SP4
Other service packs are likely to be vulnerable, but the exploit has not been tested on them, neither has the fix presented below.

Description :

The Windows NT object namespace is the place where the kernel keeps the names of mutexes, semaphores, filemapping objects, and other kernel objects. It is organized hierarchically, like a directory structure. Amongst the directories are:

\Device
\BaseNamedObjects
\Driver
\KnownDlls
...

The NT object namespace is browsable with a tool called 'WinObj 2.0' from System Internals (their website is http://www.sysinternals.com). You may wish to look around this namespace and browse the default permissions of objects. It is quiet entertaining, really.

The "\Knowndlls" directory contains a list of DLLs in the c:\winnt\system32 directory, like:

\KnownDlls\COMCTL32.dll
\KnownDlls\MPR.dll
\KnownDlls\advapi32.dll
\KnownDlls\kernel32.dll
..

All of these objects are created at boot time, and are 'permanent shared objects'. Normally, users can not create permanent shared objects (it's an advanced user right, and it is normally not assigned to any group, even Administrators). But the system pr eloads this cache for you. Permanent shared objects differ from regular shared objects only in the fact that they have a flag set, and an incremented reference count, such that if you create one, and then terminate the creating process or close all handle s to the object, it does not disappear from the object space.

To exploit the poor permissions on this cache, one first needs to delete one of the shared objects by name, in order to later replace it. So we make a call to the NTDLL.DLL native function "OpenSection()", getting a handle to the object. Then we call the TOSKRNL.EXE native function "ZwMakeTemporaryObject()" which removes the 'permanent' flag and decrements the reference counter from the object. Now we just call NTDLL.DLL:NtClose() on the handle and it is destroyed.

To create a section, one calls NTDLL.DLL:CreateSection(), which is undocumented. There are other calls one needs to make in order to set up the object and open the KnownDlls directory, but they are trivial and will not be discussed here. Feel free to browse the source code presented at the end of this advisory to see what you need to do though. Anyway, you create a section (aka file-mapping) object that points to a trojan DLL. A good candidate for DLL trojan is KERNEL32.DLL, since it is loaded by pretty much every executable you're going to run.

Note that any DLL cache objects you create as a user can not be 'permanent', hence, when you log out, the cache object _will_ disappear. So how can we get a higher privelege process to run while we're logged in? There are many ways. We can wait for an 'A t' job to go off, or we can set up the DLL hack as an 'At' job that goes off when someone else is logged in. But more reliable is this:

When a new Windows NT subsystem is started, it creates a subsystem process to handle various system details. Examples of these processes are LSASS.EXE and PSXSS.EXE. The PSXSS.EXE is the POSIX subsystem. But since no one ever really uses the POSIX subsys tem under NT. So, chances are, it won't be loaded into memory yet. Once it is, though, it's loaded until the machine reboots. If it loaded, reboot the machine, and it won't be :P.

So, we launch our DLL cache hack, and then run a POSIX subsystem command, thus launching PSXSS.EXE (which runs as 'NT AUTHORITY\SYSTEM', the system account), and running our DLL with local administrator privileges. Incidentally, other subsystems have the same effect, such as the OS/2 subsystem (the only other one that probably isn't started yet).

---

Workarounds/Fixes:

---

I developed a patch for this security problem in the form of a Win32 Service program that can be installed by the Administrator of the system. It sets itself to run every time the system is started, and before the user has the opportunity to start a program, it adjusts the permissions of the DLL cache to something much safer. The source code for t his service is also provided, along with a compiled version. Links to the programs can be found at http://www.l0pht.com/advisories.html.

One can verify the validity of the patch by downloading the WinObj v2.0 tool from System Internals (www.sysinternals.com) and inspecting the permissions of the KnownDlls directory, and the section objects within it.

Microsoft has been sent a copy of this advisory, and I would expect a hotfix from them at some point in the near future.

Example :

I wrote up a trojan to test exploitability, and it was a simple 'forwarder' DLL that had the same exported names as KERNEL32.DLL, but a different 'DllMain()' function, to be called when the DLL is loaded. The function calls in my trojan, simply forward o ff to the real KERNEL32.DLL calls located in a copy of the kernel that you make in REALKERN.DLL' in the c:\temp directory.

To try out this vulnerability, obtain an account as a low-privilege guest user (referred to as 'Dick') and do the following:

1. Log in as Dick at the console.
2. Start up two "cmd.exe" shells. Do the following in one of them.
3. Copy c:\winnt\system32\kernel32.dll to c:\temp\realkern.dll (The egg dll is hard coded to use the c:\temp directory to find this file. If you can't put it in c:\temp, then modify the source '.def' file to point to a different location and recompile eggdll.dll)
4. Copy the provided hackdll.exe and eggdll.dll to c:\temp
5. Ensure that there is no file named c:\lockout. If there is, delete it. The exploit uses this file as a lockfile.
6. Delete the KERNEL32.DLL file-mapping object from the system cache:

```
c:\> cd\temp
 c:\temp> hackdll -d kernel32.dll
```

7. Insert the new file-mapping object with:

```
 c:\temp> hackdll -a kernel32.dll c:\temp\eggdll.dll
```

   Don't hit a key in this window after hitting enter.
8. Now move to the other cmd.exe window that you started.
9. Run a POSIX subsystem command. A good way to start it is:

```
c:\temp> posix /c calc
```

   (if you have calculator installed. If not, pick some other program)
10. Now the EGGDLL.DLL will prompt you with a few message boxes:
    Say no to the "User is DOMAIN\DICK, Spawn Shell?" box.
    Say no to the "User is \[garbage], Spawn Shell?" box.
    Say YES to the "User is NT AUTHORITY\SYSTEM, Spawn Shell?" box.
    Say YES to the "Winsta0" window station message box.
    Say YES to the "Desktop" window desktop message box.

You will now see a "System Console" command.com shell open up.
(saying yes to the next 'winlogon' box will give you something funny when you log out, btw :P)

11. Now go back to your first cmd.exe window and hit a key to unpoison the DLL cache.
12. In the System Console window, run the User Manager program, and modify Dick's account (or anyone else's for that matter) to your hearts content.
    (NT Server) c:\winnt\system32> usrmgr
    (NT Workstation) c:\winnt\system32> musrmgr

Source and Compiled Code:

Exploit code can be downloaded from L0pht's website at http://www.l0pht.com/advisories.html. It is available in compiled form, and in pure source form as two zipfiles. The L0pht patch for this advisory is also available in both source form and compiled form from the same URL.

dildog@l0pht.com

L0PHT
HEAVY INDUSTRIES

A BAD CASE OF BO:
A NEW USERS GUIDE TO
BACK ORIFICE

by
ShaGGy^C

Have you ever wanted an easy-to-use Windows-based program that allows you to quietly (or not, depending on your style) manipulate someone else's Windows95/98 machine, for revenge, for convenience, or just for fun? Well there is such a program. It is called Back Orifice, more commonly referred to as BO. A creation of the Cult of the Dead Cow, you may or may not have heard of/used this program before.

"Back Orifice is a client/server application which allows the client software to monitor, administer, and perform other network and multimedia actions on the machine running the server. To communicate with the server, either the text based or gui client can be run on any Microsoft Windows machine. The server currently only runs in Windows 95/98."

In case you're wondering what that means.. There are two parts to this program.. the server, which runs on the manipulated system; and the client, which the user runs.

To set up the server on the system, the server file (boserve.exe) must be executed while Windows is running. You can rename this file if necessary. Once executed on the system, the file disappears, setting up the server in the \Windows\System\ directory as a file with no icon, no name.. only the file extension .exe . The server automatically runs while windows is running.

The client (bogui.exe {the one i use} or boclient.exe) is run on your machine. I'm not quite sure how to use the boclient.exe, so this article is based on my knowledge of the bogui.exe . To use the various commands, the system's IP number needs to be put in the top-left blank (labeled Target Host). The port should be set to 31337. The following is a guide for users of the GUI client:

(** means I've never used the command before.. so i wouldn't know anything about it other than what's in the BO text file)

****APP ADD-** Spawn a text based application on a tcp port. This allows you control a text or dos application (such as command.com) via a telnet session.

****APP DEL-** Stops an application from listening for connections.

****APPS LIST-** Lists the applications currently listening for connections.

DIRECTORY CREATE- Create a directory, perhaps? just put the name of the directory you want to create (i.e. c:\progra~1\folderofshit) for val1 (the first blank) and click Send

DIRECTORY LIST- put the name of a directory using a wildcard (i.e. c:\balls\*.*) for val1, and click Send.. it will bring back a listing of everything in the directory (files, folders) {A little tip-- most computers have an a: drive, though it usually doesn't show up in the System info.. just do a Directory list on a:\*.* to check if there's anything in the a: drive.. also gives people a scare if you do it repeatedly..}

DIRECTORY REMOVE- put the name of a directory (i.e. c:\ballsack) for val1, and click Send.. deletes the directory (can only be done to an empty directory, i still haven't figured out a way to delete a directory with files in it :P)

****EXPORT ADD-** Creates an export on the server. The exported directory or drive's icon does not get overlaid with the shared hand icon.

****EXPORT DEL-** Deletes an export.

****EXPORTS LIST-** Lists current share names, the drive or directory that is being shared, the access for that share, and the password for the share.

FILE COPY- put the name of the file you want to copy for val1 (i.e. c:\shizzack.exe) and put the name of the new file for val2 (i.e. c:\kcazzihs.exe) and click Send

FILE DELETE- put the name of the file you want to delete for val1 (i.e. c:\sack.nut) and click Send

FILE FIND- finds a file.. for val1, put the file mask, which may contain wildcards (i.e. *scrotum*.jp*) and put the search path for val2 (i.e. c:)

FILE FREEZE- freezes (compresses) a file.. put the original filename for val1 (i.e. a:\shiz.ack), and the compressed filename for val2 (i.e. d:\compres.sed) and click Send

FILE MELT- melts (decompresses) a frozen/compressed file.. put the compressed filename for val1 (i.e. d:\compres.sed), and the new file's name for val2 (i.e. a:\shiz.ack) and click Send

FILE VIEW- views the contents of a text file, just put the name of the file for val1 (i.e. c:\shit.txt) and click Send

HTTP Disable- Disables the HTTP server.

HTTP Enable- Enables the HTTP server.. for val1, you put the port (i.e. 80) and put the root directory thing for val2 (i.e. c:).. click Send.. then to connect, run http://IP:Port/ in your browser (like, if their IP is 252.151.152.25 and you set the port to 80, it would be http://252.151.152.25:80/)

Keylog begin- Logs keystrokes on the server machine to a text file. The log shows you the name of the window the text was typed into. put the name of the file you want to log the keystrokes to (i.e. c:\shat.txt) for val1.. and if you wanna view the file, just do a File view on the file you're logging to

Keylog end- Disable the keylog.

****MM Capture avi-** Captures video and audio (if available) from a video input device to an avi file... put the name of the avi file you want to create for val1 (i.e. d:\screen.avi), and fill in the parameters for val2 (not sure what to put there)

****MM Capture frame-** Captures a frame of a video to a bitmap image.. put the bitmap image's name for val1 (i.e. c:\crap.bmp) and fill in val2's parameters (not sure what goes here)

MM Capture screen- takes a picture of the screen, puts it in a bitmap file.. specify the filename for val1 (this never works for me..)

****MM List capture devices-** lists video input devices.. i guess:P

MM Play sound- plays a .wav file on their system.. put the wav filename (i.e. c:\dookie\toilet.wav).. gives them a scare

****Net connections-** lists incoming and outgoing net connections..

****Net delete-** disconnects machine from a network source

****Net use-** connects machine to a network source

****Net view-** Views all network interfaces, domains, servers, and exports visible from the server machine.

Ping host- Pings the host machine. Returns the machine name and the BO version number... if you put wildcards in the IP (i.e. 222.111.35.*), it will search every IP matching that for a BO infection.. very useful

**PLUGIN EXECUTE- Executes a Back Orifice plugin. Executing functions that do not conform to the Back Orifice plugin interface may cause the server to crash.

**PLUGIN KILL- tells a specific plugin to shutdown

**PLUGINS LIST- Lists active plugins or the return value of a plugin that has exited.

PROCESS KILL- Kills a running process.. use the Process ID (specified when you do a process list) for val1

PROCESS LIST- Lists the all the running processes

PROCESS SPAWN- Opens a file/program that you specify in val1.. but i think you hafta put something in val2, im not sure..

**REDIR ADD- redirects incoming tcp connections/udp packets to another IP address.. never used it before, not sure how it works :P

**REDIR DEL- stops a port redirection

**REDIRS LIST- lists active port redirections

**REG CREATE KEY- Creates a key in the registry. NOTE: For all registry commands, do not specify the leading \\ for registry values.

**REG DELETE KEY- Deletes a key from the registry.

**REG LIST KEYS- Lists the sub keys of a registry key.

**REG LIST VALUES- Lists the values of a registry key.

**REG SET VALUE- Sets a value for a registry key. The values are specified as a type followed by a comma, then the value data. For binary values (type B) the value is a series of two digit hex values. For DWORD values (type D) the value is a decimal number. For string values (type S) the value is a text string.

****RESOLVE HOST-** Resolves the ip address of a machine name relative to the server machine. The machine name can be an internet host name, or a local network machine name.

SYSTEM DIALOGBOX- FUN :).. just put a message for val1, and put a title for val2, and click Send.. it pops up a dialog box on their screen with the message and title, with an OK button.. do as many as you want, they cascade in front of the previous box

SYSTEM INFO- Displays system information for the server machine. Information displayed includes machine name, current user, cpu type, total and available memory, Windows version information, and drive information, including drive type (Fixed, cd-rom, removable, or remote) and for fixed drives, the size and free space of the drive.

SYSTEM LOCKUP- it locks up the machine

SYSTEM PASSWORDS- Displays cached passwords for the current user and the screen saver password. Displayed passwords may have garbage data at their end.

SYSTEM REBOOT- reboots the system :P

****TCP FILE RECEIVE-** Connects the server machine to a specific ip and port and saves any data recieved from that connection to the specified file.

****TCP FILE SEND-** Connects the server machine to a specific ip and port and sends the contents of the specified file, then disconnects. NOTE: For tcp file transfers, the specified ip and port must be listening before the tcp file command is sent or it will fail. A useful utility for transfering files this way is netcat, which is available for both unix and win32.

Back Orifice is a product of the cDc (http://www.cultdeadcow.com). All of the above was based on version 1.20, which can be downloaded at the cDc's homepage. Let me know if a new version is posted.. I don't feel like looking often. :)

-ShaGGy^C

Crawling for 411: Improving your Internet Searches

Article sub'd by

FORENSIC

You've just posted to a newsgroup for the first time, wondering if anyone has such and such phile. You were immediately flamed so hard, you closed your news reader with your head spinning like a HDD's magnetic disk. What happened?

One of the major ethos of the community is DIY: Do It Yourself. Go over every info outlet before looking to others for help. Not that the members of EUA don't mind questions, but it's a good idea to try to get it yourself in order to learn where much of the information is stored.

The first thing you should do is keep up with the news. I don't know how many times I've talked to other h/p/c/v/a-ers only to find out that they had no clue a major virus had been released over the Internet. If you don't know what the media is saying about you, how can you protect yourself? How can you have a springboard to find other information? Get into the habit of visiting these sites, if not on a daily basis, then at least every two days:

http://www.cnn.com: CNN

http://www.zdnet.com: ZDNet

http://www.zdnet.com/zdtv/cybercrime/:
ZDNet's Cybercrime section. Interesting because an ex-hacker writes for them.
http://www.news.com: CNet's daily news.

http://www.newslinx.com: Extensive. This one rocks.

http://www.hackernews.com:
You must visit this site very very often. Great 411.

http://www.bikkel.com/~demoniz/:
100% Pure Bikkel. More great 411.

http://www.angelfire.com/nt/slackware/mainp.html:
C-R-I-M-E-O-N-L-I-N-E. An other incredible 411 site.

Okay, so you are the guru of the news now. These sites are a good start in getting links to good information, but there still might be some files that you can't find. First off, throw away the major search engines. Yahoo, Altavista, Lycos, and the like are not necessarily bad. However, they are inappropriate for the kind of broad sweeping searches that are needed when seeking out arcane texts. Your best bet is a meta engine, or one that uses a combination of search engines to pool results.

Why are meta engines better? One reason is that search engines like Yahoo! are getting so flooded with URL submissions that they have resorted to taking money under the table from companies that want a better list ranking. When you're not original enough to come up with a new logarithm for your bot, money is your last stop. This doesn't make these engines undesirable just on an ethical level, but also because a great deal of content is being excluded when you use them to find information.

Another reason why meta engines are better is that you get a better sampling of sites from the Internet. Let's face it, the Internet is extremely huge, and you don't really want to sift through 20000 search results off of Lycos. Meta engines compile results across a broader scale, and are pickier about keyword relevance, thereby saving you a great deal of time.

The next step in better info gathering is getting to know those little-known search engines. These are engines that the little guy will submit his site to, and the little guy might have more interesting 411 than the larger guys.

Next step: use of keywords. Don't do a search for "hacking", "hack", "hackers" or anything like that. Obviously you're going to come up with a huge amount of results, and most of them will probably be from T50, an online adult entertainment company that likes to use hackish, crackish keywords in their meta tags. If you come across one of their sites, run like hell. Not only will you have ten windows pop up for every link you click from on sites, but you will never get the info you want. Unless the info you want somehow involves teenage blonde vixens.

Be specific in your keyword usage. If you are looking for the DoD's Rainbow series, use "DoD Rainbow series." If you do not get the results you needed, think for a moment. Who releases the info? What keywords would they use? How would they title the documents? Plug those into the search field and you will have better results.

Last, but not least, if you know the name of the specific file you need, plug it into the search field including the extension (for example: patch.exe). The file should be in the first five results. I especially like to do this for image file searches (if I'm looking for a picture of a gear, I'll plug in "gear.gif") because then the engine will link directly to the site's directory.

If you still haven't found what you need, it's time to hit the library. Before you turn up your nose and snort, remember that before there was an Internet, there were libraries. If you are looking for a particularly old piece of information, chances are you will find it at the library. If you don't know how to search through a library, ask the librarian. This article is already running a little long to go into the finer points of the Dewey Decimal System.

A few forensic-approved search engines:

http://www.dogpile.com/: so far that I've seen, simply the best.

http://www.metacrawler.com/: I think this might even be the first meta engine ever developed.

http://www.isleuth.com/: This would be the most kickass engine if it weren't so damn slow.

http://www.aj.com/: Not too bad. Uses a natural language search.

http://ahoy.cs.washington.edu:6060/: Home page engine. You'll never know what you'll find.

http://www.filez.com/: just another one to try.

http://www.diysearch.com/: underground search engine.

http://www.inference.com/infind/: really hits those keywords hard.

What's your favorite search engine? Drop me a line at DanteInfo@yahoo.com.

by Daem0n Zer0

<*> AIM: *Have you ever wanted to go on IRC under your friend or enemy's nick but didn't know their password? Today my friend you can learn how to change that.*

Obtaining The Password File

Your victim must be using pirch either v 32 or 98. The password and other info that pirch uses is stored in a .ini file in the pirch dir i.e c:\pirch98\pirch98.ini.

There are many ways in which you can obtain this file the ones i can think of off the top of my head would be go to the victims house and copy the file on a disk and tell him/her some bullshit excuse why you need it OR you could use NetBus or Back Orifice to get it or you could try some social engineering and try to get him/her to dcc it or whatever.

Finding The Encrypted Password

Open The .ini File and look under [user] here you will see there nick, email address etc. look for the line beggining with "pw=" here is where the Encrypted password is in my example below it would look like:

pw=çäëëî

copy this line in the .ini and move on.

Encryption

Below is a list of all characters and its Pirch Encrytption:

lowercase alphabet

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
à	á	â	ã	ä	å	æ	ç	è	é	ê	ë	ì	í	î	ï	ð	ñ	ò	ó	ô	õ	ö	÷	ø	ù

```
UPPERCASE ALPHABET
--------------------------------------------------
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù
--------------------------------------------------
```

Other Characters, note: the ! character is a space when encrypted into (pirch language) ie its just a blank space in the encrypted password field in the .ini file.

```
-------------------------------------------------------
!"£$%^&* ( ) _ + < , > . ? / : ; @ ' ~ # { [ } ] \ - ` |

 ¡"£¤Ý¥© § ¨ Þ ª » « ½ - ¾ ® ¹ º ¿ ¦ ý ¢ ú Ú ü Ü Û ¬ ß û
-------------------------------------------------------
```

```
Numbers
-------------------------------------------------------
1 2 3 4 5 6 7 8 9 0

° ± ² ³ ´ µ ¶ · ¸ -
-------------------------------------------------------
```

Cracking The Password

Ok so now you have the encrypted password all you have to do is compare each encrypted character to the ones beneath the english characters and from there match up the english character, so if the encrypted password is çäëëî then I will match them up.

ç = h
ä = e
ë = l
ë = l
î = o

So the real password is "hello", its not that hard. From past experience i have noticed that alot of people use the same password for everything like IRC, E-mail, ISP account etc. I managed to log into my freinds e-mail and ISP using his IRC password, so experiment.

Thats it for just now if you have any problems e-mail me at:

mike@rainz.freeserve.co.uk

--Daemon0

DEPARTMENT OF DEFENSE
DEFENSE SWITCHING NETWORK
MILITARY PHONE SYSTEMS -- PART TWO

BY Archive

THE DSN WORLDWIDE NUMBERING AND DIALING PLAN

INTRODUCTION

C4.1 General. This chapter introduces the DSN Worldwide Numbering and Dialing Plan (DSN WNDP) to DSN users. The WNDP is a standard numbering system that will serve all DSN users in a uniform manner. The plan provides network numbering and dialing requirements for intraswitch dialing and establishes standard (mandatory) information which must be passed between DSN switches. All new switches introduced into the DSN must have the capability to operate with the DSN WNDP. This plan has been generally accepted as the global calling format to be used in the DSN. It allows the user to access any subnetwork using a single dialing plan. This plan also contains user feature codes that have been assigned globally to ensure compatibility in selecting user features and services.

C4.2 Objectives. The primary objectives of the DSN WNDP were to be interoperable with the worldwide AUTOVON Numbering Plan and the European Telephone System (ETS) Numbering Plan, and to provide sufficient capability and flexibility to accommodate new DSN features without major numbering plan changes. The DSN WNDP provides for the following:

C4.2.1 Capability to customize local dialing (intraswitch) plans by offering four-, five-, or seven-digit options.

C4.2.2 Capability for all users to dial precedence service.

C4.2.3 Capability to incorporate modern features including abbreviated dialing of local service and emergency codes.

C4.2.4 Establishment of the standard for interswitch exchange of information relative to call establishment.

C4.2.5 Use of authorization codes.
C4.2.6 Direct dial access to and from North Atlantic Treaty Organization (NATO) and U.S. tactical telephone systems.

C4.2.7 Local and remote dial service assistance operator service.

C4.2.8 Direct dial access to local and long-distance public telephone systems for the purpose of establishing:

C4.2.8.1 Local, national, and international calls through the commercial telephone system.

C4.2.8.2 Local, national, and international voice and data calls through the leased private line and software defined portions of the DSN.

C4.2.9 Incorporation of the present AUTOVON and ETS Numbering Plans.

C4.2.10 Direct dial access to and from other Government, commercial, and special common carrier services and networks.

NETWORK NUMBERING PLAN

C4.3 General. This section contains information which DSN switches use to establish network calls. Each switch involved in a network call must conform strictly to the Switch Outpulsing Format and the assignment of digits contained therein.

C4.4 Numbering Plan Parts and Formats. The DSN WNDP consists of eight basic parts. A subset of these basic parts is used by the customer in conveying information to the switch in the Customer Dialing Format. Another subset is used by the DSN switches in establishing interswitch calls. The DSN WNDP parts are:

C4.4.1 Access Digit.

C4.4.2 Precedence Digit or Service Digit.

C4.4.3 Route Code.

C4.4.4 Route Control Digit.

C4.4.5 Area Code.

C4.4.6 Switch Code.

C4.4.7 Line Number.

C4.4.8 Traveling Class-of-Service Digit.

C4.5 Switch Outpulsing. Switch outpulsing information is described in table T4.1. Digits shown in parentheses are not required on all calls, and a digit shown in brackets is never dialed by the customer. When this digit is required by the routing plan, it will be inserted by the switch.

C4.6 Precedence Digit. Precedence digit assignments are:

0 DSN - FLASH OVERRIDE Prece

1 DSN - FLASH Precedence.

2 DSN - IMMEDIATE Precedence.

3 DSN - PRIORITY Precedence.

4 DSN - ROUTINE Precedence.

C4.7 Route Digit. Route digit assignments are:

0 Voice or data grade trunking may be used.

1 Data grade trunking required.

2 Unassigned.

3 Unassigned.

4 Unassigned.

5 Hot line (offhook) voice grade.

6 Hot line (offhook) data grade.

7 FTS Numbering Plan.

8 Unassigned.

9 CONUS Commercial Numbering Plan.

C4.8 Route Control Digit. When required, the route control digit is generated by the switch. The route control digit is required in a polygrid network to prevent backhauling, shuttling, and "ring-around," and to assure that a call advances toward its destination.

C4.9 Address Digits. Address digits are used to identify and to route calls to a user in any part of the world. Address digits include the area code, the switch code, and the line number.

NETWORK DIALING PLAN

C4.10 User Dialing.

C4.10.1 The DSN user dialing format shown in table T2.1 and the component parts of the User Dialing Plan Format for dialing DSN 4-, 5- and 7-digit addresses are described in this section. In table T2.1, the codes shown in parentheses are not required for all calls. For interarea calls the user must also dial the area code. This requires dialing 10 digits to establish a ROUTINE interarea call.

C4.10.2 The worldwide numbering plan shown in table T2.1 permits access to commercial and other Government networks using the full range of address digits indicated. Within DSN, however, a subset of address digits will be used to preclude the first dialed digit's being interpreted as an access code when an access code is not needed or intended. The address subsets are as follows where K, L, N, X are defined in figure F2.1:

(1) For 7-digit dialing within DSN: (KYX) KNX XXXX.

(2) For 5-digit dialing: LXXXX.

(3) For 4-digit dialing: LXXX.

C4.11 Authority for Intraswitch Dialing Options. For overseas theaters the responsibility for selecting which of the intraswitch dialing options (four, five, or seven digits) described below rests with the appropriate unified commander (CINCEUR or CINCPAC) in consultation with DISA. For the Western Hemisphere, DISA will select the intraswitch dialing option. Components having particular end office requirements that may differ from the CINC-stated or DISA-stated intraswitch dialing policy must negotiate any exceptions with the appropriate CINC and DISA. CINCEUR and CINCPAC have directed that seven-digit intraswitch dialing be used. Employing other onbase optional features, such as speed calling or abbreviated dialing and special feature and service codes will be at the discretion of the local base, post, camp, or station commander.

C4.12 Intraswitch Dialing Options. The DSN Worldwide Dialing Plan permits the selection of four-, five-, or seven-digit intraswitch dialing. Four-digit intraswitch dialing may be used when projected switch growth is less than 6000 lines. Five-digit dialing may be used when the projected growth is above 6000 lines. For growth beyond 10,000 lines, two or more switch codes must be assigned. Additional limitations on four- or five-digit intraswitch dialing are described below. Seven-digit intraswitch dialing provides uniform interswitch and intraswitch dialing within a DSN number plan area. DSN numbering plan areas generally correspond to the military theaters.

C4.12.1 Four-Digit Intraswitch Dialing. Four-digit intraswitch dialing uses the four-digit line number for establishing intraswitch calls. Line number assignments must be of the form LXXX where L is any digit 2 through 7, and X is any digit 0 through 9. Access to the local operator is obtained by dialing

0. Access to DSN for ROUTINE or higher precedence calls or otherGovernment or commercial service is obtained by dialing 9, followed by the appropriate precedence or service digit.

Intraswitch precedence calls above ROUTINE are made by dialing the appropriate access code or pressing the appropriate precedence key in the case of 15- or 16-button DTMF keyset telephones.

C4.12.2 Five-Digit Intraswitch Dialing. Five-digit intraswitch dialing uses the last digit of the switch code and the four-digit line number. Number assignments for this plan must be of the form LXXXX, where L and X are as defined previously. Procedures for dialing the local operator, DSN, and other Government or commercial services, as well as intraswitch precedence calls above ROUTINE, are identical to those described above for four- digit dialing.

C4.12.3 Seven-Digit Intraswitch Dialing. Seven-digit intraswitch dialing uses the digits of the switch code and line number to establish either interswitch or intraswitch calls.

Number assignments for this plan must be of the form KNX XXXX where K and N are as defined above. DISA will assign the specific KNX of each switch to preclude conflicts with other switch codes. Access to the local operator is obtained by dialing 0. DSN ROUTINE calls are initiated by dialing the appropriate sequence of (KYX) KNX XXXX where the digits and the parentheses are as defined above. DSN calls above ROUTINE precedence are initiated by the appropriate sequence of 9P (KYX) KNX XXXX, where P is the appropriate digit (0, 1, 2, 3) for the level of precedence desired and the other digits and parentheses are as defined above. Access to other Government or commercial services is obtained by dialing 9 followed by the appropriate service digit. For 15- or 16-button DTMF keyset telephone instruments, use of the appropriate precedence key replaces dialing of precedence access code 9P.

C4.13 Access Code. The access code consists of the access digit, 9, followed by a precedence digit or a service digit.

C4.13.1 The access digit, 9, informs the switch that the digit which follows indicates a precedence call, an offnet call for service on another system, or a special features call, such as an individual trunk test.

C4.13.2 The precedence digit 0, 1, 2, 3, or 4 permits a DSN user to dial an authorized DSN precedence level from either a properly class-marked rotary dial or a 10- or 12-button telephone instrument. The FO, F, I, and P keys of a 16-button DTMF keyset replace the precedence access codes 90 through 93 when precedence calls are originated at levels above ROUTINE. When the seven-digit intraswitch dialing is used, it is not necessary to dial or key the precedence access code for ROUTINE calls. When four- or five-digit local dialing is used, the DSN user is required to dial the access code and precedence digit 4 when placing DSN ROUTINE precedence interswitch calls.

C4.13.3 The service digits 5 through 9 provide information to the switch to connect calls to Government or public telephone services or networks that are not part of the DSN. In order to distinguish between access codes and two-digit abbreviated dialing codes, the DSN switch will receive the access code and all routing and address digits before attempting to route a call.

C4.14 Precedence and Service Access Code Assignments.

C4.14.1 The assignment of precedence and service access codes is presented below. DISA assigns service access codes.

C4.14.1.1 Assignments for rotary dial and 10- and 12-button DTMF keyset telephones are:

Access Digit

Precedence Digit

9	0	DSN - FLASH OVERRIDE Precedence
9	1	DSN - FLASH Precedence
9	2	DSN - IMMEDIATE Precedence
9	3	DSN - PRIORITY Precedence
9	4	DSN - ROUTINE Precedence (four- or five- digit plan only)

C4.14.1.2 Assignments of precedence access codes for 15- or 16-button DTMF keyset telephone instruments are:

FO	DSN - FLASH OVERRIDE Precedence
F	DSN - FLASH Precedence
I	DSN - IMMEDIATE Precedence
P	DSN - PRIORITY Precedence
94	DSN - ROUTINE Precedence (four- or five-digit optional local plans only)

C4.14.1.3 Assignments for service access codes are:

Access Digit	Service Digit	
9	5	To be determined
9	6	To be determined
9	7	To be determined
9	8	To be determined

9 9 Local Public Telephone Network

C4.14.2 The access code 8N, where N is any digit 2-9, is reserved for future assignment to include access to the Federal Telecommunications System (FTS), the Nationwide Emergency Telecommunications System (NETS), and the DCTN.

C4.15 Route Code.

C4.15.1 The route code is a special-purpose DSN code that permits the customer to inform the switch of special routing or termination requirements. At the present time, the use of the route code is limited to the DSN (including AUTOVON) to determine whether a call will use data or voice grade trunking or to indicate that the number to be dialed is either an FTS or WESTHEM commercial number. The route code may be used to disable echo suppressors or cancelers and override satellite link control when these features are incorporated into the DSN.

C4.15.2 It is not necessary to dial a route code for voice calls, as no special features are required. The first digit of the route code is the part of the dialing plan that informs the switch that the next digit gives network instructions for specialized routing. The route code assignments are in table T4.2.

C4.16 Address Digits. The address digits are used to identify and to route calls to a user in any part of the world. There are three parts as indicated below.

C4.16.1 Area Code. The DSN area code indicates the geographical part of the world or tactical unit (Call Area) in which a called party is located. It is a three-digit code of the form KYX and is used only when calling a user outside of the originator's own call area. There are normally 160 area codes available for use worldwide. Because of the assignment of the access digits 9 and 8, only 130 area codes are available in the DSN. Fifty area codes have been reserved for tactical systems, and the AUTOVON uses over 20 area codes. DISA Code D362 (formerly B520) will make DSN area code assignments.

(1) Assignable area codes (including tactical):

200 - 219

300 - 319

400 - 419

500 - 519

600 - 619

700 - 719

800 - 809

(2) Area codes reserved for tactical use numbers:

200 - 209

300 - 309

400 - 409

700 - 709

800 - 809

(3) Nonassignable area codes are:

810 - 819

900 - 919

C4.16.2 Switch Code. The DSN switch code directs a call to a specific switching center within a call area. It is a three-digit code of the form KNX. There are normally 640 switch codes available in each calling area; however, because of the use of the access codes, only 480 switch codes are available in each calling area. All theaters, except CONUS, have converted to the KNX formats, but in CONUS, the NNX format is still required due to the large demand. This code must be dialed to reach another switch in the same calling area. DISA Code D362 (formerly B520) will make DSN switch code assignments.

(1) Assignable switch codes:

220 - 299

320 - 399

420 - 499

520 - 599

620 - 699

720 - 799

(2) Nonassignable switch codes:

820 - 899

920 - 999

C4.16.3 Line Number. The line number is the unique user identification. It is of the form XXXX and can be reused from switch to switch, but not within a switch code. The four-digit line number can identify as many as 10,000 users in each switch. The line number groups cannot be assigned arbitrarily for each switch. The line number group assignments must be coordinated with the DISA and with the local connecting telephone company or the host nation PTT.

SPECIAL FEATURES AND SERVICES

C4.17 General.

C4.17.1 A goal of the DSN is to provide access to many features and services through a single-line instrument. As the number of features increases and the methods of providing these features become more diverse, it becomes necessary to provide standard methods of accessing the features to avoid retraining when a user moves from one call area to another.

C4.17.2 Certain features and codes to be used in the DSN are shown below. All features will not be available in all switches; however, where they are available, the number assignments shown in this section are to be used. The format and restrictions for each feature must be adhered to in order to maintain network uniformity and allow for network expansion.

C4.18 Feature Codes. Feature codes, except abbreviated dial codes, for DTMF telephones will be of the form *NX or #NX. The switch will decode first digits "12" as equivalent to "*" and "13" as equivalent to "#" when received from a rotary dial or a 10- or 15-button DTMF telephone. Current recommended assignments are in table T4.3.

C4.18.1 Abbreviated Dialing (Speed Calling). Abbreviated dialing is a feature code subset. The codes prescribed in table

T4.4 are recommended for use in the DSN.

C4.18.2 Special Services - Abbreviated Numbers. The format 10X is recommended where conflicts between DSN route codes (1X) and special service number (1XX) exist. The generally accepted special service numbers of 11X may be continued in use with the four- and five-digit intraswitch dialing option. If the seven-digit intraswitch dialing option is used, the switch must be programmed so that after the 11X code is received, and no additional digits are received within approximately 4 seconds, the call will be treated and processed as a Special Service call. If additional digits are received within 4 seconds, the call will be treated and processed as a DSN call. The recommended 10X format assignments are shown in table T4.5.

C4.18.3 Special Services. Access to special services (e.g., dictation, paging, station ringer test) should be accomplished using the format of the common list of abbreviated dial numbers. Specific number assignments are left to the discretion of the local base commander.

C4.18.4 Attendant Assisted Precedence Calling. The DSN Worldwide Numbering Plan includes provision for DSN stations to dial calls exceeding their authorized maximum precedence and calling area class-mark by dialing a 0 followed by the complete DSN number, including access code. The call will be routed to the serving DSN attendant who will permit or deny the call in accordance with established procedures. The complete dialed number will be displayed on the attendant's console to expedite the handling of the call. The specific dialing formats from rotary dial and DTMF telephone instruments are outlined below:

(1) Rotary Dial and 10- and 12-Button Telephone

Formats.

0 + 90 + DSN Number	Attendant Assisted (FLASH OVERRIDE)
0 + 91 + DSN Number	Attendant Assisted (FLASH)
0 + 92 + DSN Number	Attendant Assisted (IMMEDIATE)
0 + 93 + DSN Number	Attendant Assisted (PRIORITY)
0 + DSN Number	Attendant Assisted (ROUTINE)

(2) 15- and 16-Button DTMF Telephone Instrument

Formats.

0 + FO + DSN Number	Attendant Assisted (FLASH OVERRIDE)

0 + F + DSN Number	Attendant Assisted (FLASH)
0 + I + DSN Number	Attendant Assisted (IMMEDIATE)
0 + P + DSN Number	Attendant Assisted (PRIORITY)
0 + DSN Number	Attendant Assisted (ROUTINE)

C4.18.5 Standard Directory Numbers. Standard directory numbers for the following services shall adhere to the format and assignments specified if the service is provided at a centralized location where a network call is required to reach that service.

(1) Standard Directory Numbers (Four-Digit).

Call Type	Rotary Dial, 10- or 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Attendant Assistance	KNX-L110	KNX-L110
Chief Operator	KNX-L311	KNX-L311
Weather Announcer	KNX-L381	KNX-L381
Time	KNX-L391	KNX-L391
Trouble Reporting	KNX-L611	KNX-L611

(2) Standard Directory Numbers (Five-Digit).

Call Type	Rotary Dial, 10- or 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Attendant Assistance	KNL-1110	KNL-1110
Chief Operator	KNL-1311	KNL-1311
Weather Announcer	KNL-1381	KNL-1381
Time	KNL-1391	KNL-1391
Trouble Reporting	KNL-1611	KNL-1611

(3) Standard Directory Numbers (Seven-Digit).

Call Type	Rotary Dial, 10- or 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Attendant Assistance	KNX-1110	KNX-1110
Chief Operator	KNX-1311	KNX-1311
Weather Announcer	KNX-1381	KNX-1381
Time	KNX-1391	KNX-1391
Trouble Reporting	KNX-1611	KNX-1611

C4.18.6 Standard Test Numbers. Standard test numbers for the test and maintenance capabilities shall adhere to the format and number assignments specified below if a DSN centralized test and maintenance capability is desired and a network call is required.

(1) Standard Test Numbers (Four-Digit).

Call Type	Rotary Dial, 10- or 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Milliwatt Test	KNX-L021	KNX-L021
Supervisory and Signal Test	KNX-L031	KNX-L031
Far End Transmission and Noise Test	KNX-L041	KNX-L041
Dial Speed Test	KNX-L351	KNX-L351
DTMF Test	KNX-L361	KNX-L361
Ringback Test	KNX-L371	KNX-L371
Line Test Check (Commercial)	KNX-L301	KNX-L301
Loop-Around Termination	KNX-L061	KNX-L061
Preemption Test	KNX-L071	KNX-L071

(2) Standard Test Numbers (Five-Digit).

Call Type	Rotary Dial, 10- or 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Milliwatt Test	KNL-1021	KNL-1021
Supervisory and Signal Test	KNL-1031	KNL-1031

Far End Transmission and Noise Test	KNL-1041	KNL-1041
Dial Speed Test	KNL-1351	KNL-1351
DTMF Test	KNL-1361	KNL-1361
Ringback Test	KNL-1371	KNL-1371
Line Test Check (Commercial)	KNL-1301	KNL-1301
Loop-Around Termination	KNL-1061	KNL-1061
Preemption Test	KNL-1071	KNL-1071

(3) Standard Test Numbers (Seven-Digit).

Call Type	Rotary Dial, 10- or 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Milliwatt Test	KNX-1021	KNX-1021
Supervisory and Signal Test	KNX-1031	LNX-1031
Far End Transmission and Noise Test	KNX-1041	KNX-1041
Dial Speed Test	KNX-1351	KNX-1351
DTMF Test	KNX-1361	KNX-1361
Ringback Test	KNX-1371	KNX-1371

Line Test Check (Commercial)	KNX-1301	KNX-1301
Loop-Around Termination	KNX-1061	KNX-1061
Preemption Test	KNX-1071	KNX-1071

C4.18.7 Sample Dialing Formats. The following sample dialing formats are presented to illustrate user dialing procedures under the three local dialing options. These abbreviations are used in the options given below: Direct Distance Dialing, (DDD); Federal Telecommunications System, (FTS); and Public Telephone Network, (PTN).

(1) Four-Digit Intraswitch Dialing Option.

Call Type	Rotary Dial, 10- 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Intraswitch Call	LXXX	LXXX
DSN IMMEDIATE Precedence Voice Grade	I-(KYX)KNX-LXXX	92-(KYX)-KNX-LXXX
DSN IMMEDIATE Precedence Data Grade	I-11-(KYX)-KNX-LXXX	92-11-(KYX)-KNX-LXXX
DSN ROUTINE Precdence Voice Grade	94-(KYX)-KNX-LXXX	94-(KYX)-KNX-LXXX
DSN ROUTINE Precedence Data Grade	94-11-(KYX)-KNX-LXXX	94-11-(KYX)-KNX-LXXX

FTS Number, ROUTINE Precedence Within DSN	94-17(NYX)-NNX-XXXX	94-17-(NYX)-NNX-XXXX
FTS Number, IMMEDIATE Precedence Within DSN	I-17(NYX)-NNX-XXXX	92-17-(NYX)-NNX-XXXX
CONUS DDD Number, ROUTINE Precedence Within DSN	94-19-(NYX)-NNX-XXXX	94-19-(NYX)-NNX-XXXX
CONUS DDD Number, IMMEDIATE Precedence Within DSN	I-19-(NYX)-NNX-XXXX	92-19-(NYX)-NNX-XXXX
LOCAL PTN Number	99 plus PTN Number	99 plus PTN Number

(2) Five-Digit Intraswitch Dialing Option.

Call Type	Rotary Dial, 10- 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Intraswitch Call	L-XXXX	L-XXXX
DSN IMMEDIATE Precedence Voice Grade	I-(KYX)KNX-XXXX	92-(KYX)-KNX-XXXX

DSN IMMEDIATE Precedence Data Grade	I-11-(KYX)-KNL-XXXX	92-11-(KYX)-KNL-XXXX
DSN ROUTINE Precedence Voice Grade	94-(KYX)-KNL-XXXX	94-(KYX)-KNL-XXXX
DSN ROUTINE Precedence Data Grade	94-11-(KYX)-KNL-XXXX	94-11-(KYX)-KNL-XXXX
FTS Number, ROUTINE Precedence Within DSN	94-17(NYX)-NNX-XXXX	94-17-(NYX)-NNX-XXXX
FTS Number, IMMEDIATE Precedence Within DSN	I-17(NYX)-NNX-XXXX	92-17-(NYX)-NNX-XXXX
CONUS DDD Number, ROUTINE Precedence Within DSN	94-19-(NYX)-NNX-XXXX	94-19-(NYX)-NNX-XXXX
CONUS DDD Number, IMMEDIATE Precedence Within DSN	I-19-(NYX)-NNX-XXXX	92-19-(NYX)-NNX-XXXX
LOCAL PTN Number	99 plus PTN Number	99 plus PTN Number

(3) Seven-Digit Intraswitch Dialing Option.

Call Type	Rotary Dial, 10- 15- or 16-Button DTMF Keysets	12-Button DTMF Keysets
Intraswitch Call	KNX-XXXX	KNX-XXXX
DSN IMMEDIATE Precedence Voice Grade	I-(KYX)-KNX-XXXX	92-(KYX)-KNX-XXXX
DSN IMMEDIATE Precedence Data Grade	I-11-(KYX)-KNX-XXXX	92-11-(KYX)-KNX-XXXX
DSN ROUTINE Precedence Voice Grade	(KYX)-KNX-XXXX	(KYX)-KNX-XXXX
DSN ROUTINE Precedence Data Grade	11-(KYX)-KNX-XXXX	11-(KYX)-KNX-XXXX
FTS Number, ROUTINE Precedence Within DSN	17-(NYX)-NNX-XXXX	17-(NYX)-NNX-XXXX
FTS Number, IMMEDIATE Precedence Within DSN	I-17(NYX)-NNX-XXXX	92-17-(NYX)-NNX-XXXX
CONUS DDD Number, ROUTINE Precedence	19-(NYX)-NNX-XXXX	19-(NYX)-NNX-XXXX

Within DSN		
CONUS DDD Number, IMMEDIATE Precedence Within DSN	I-19-(NYX)-NNX-XXXX	92-19-(NYX)-NNX-XXXX
LOCAL PTN Number	99 plus PTN Number	99 plus PTN Number

VOICE PRECEDENCE SYSTEM

C5.1 General. The initial AUTOVON had four levels of precedence: FLASH, IMMEDIATE, PRIORITY, and ROUTINE. The initial AUTOVON network included many commercial type electromechanical switches. These switches also had override capabilities which could override the four levels of precedence. This override capability (FLASH OVERRIDE) was used to provide very important persons (e.g., the President) with the ability to override all calls and to prevent others from overriding the important persons. The DSN will consist of digital software-controlled switches, which use software to handle precedences.

The distinction between FLASH OVERRIDE and the four precedences is no longer germane. These switches treat FLASH OVERRIDE as a fifth, non-preemptible, level of precedence. Reference 4.2 was written for the AUTOVON network which included the electromechanical switches. Reference 4.3 written for the DSN network eliminates the distinction. The precedence criterion for FLASH OVERRIDE was taken from various sources. The precedence criteria for FLASH, IMMEDIATE, PRIORITY, and ROUTINE were taken from reference 4.2.

C5.2 Precedence Designator: FLASH OVERRIDE.

C5.2.1 Order of Precedence and Preemption. Telephone calls designated FLASH OVERRIDE shall take precedence over and preempt all calls on the DSN. FLASH OVERRIDE calls are not preemptible.

FLASH OVERRIDE calls shall be handled ahead of all other calls.

C5.2.2 Application (FLASH OVERRIDE). FLASH OVERRIDE is reserved for:

C5.2.1 The President of the United States.

C5.2.2 The Secretary of Defense.

C5.2.3 Chairman of the Joint Chiefs of Staff.

C5.2.4 Chiefs of Military Services.
C5.2.5 Commanders of Unified and Specified Commands.

C5.2.6 Others as specified by the President.

C5.3 Precedence Designator: FLASH.

C5.3.1 Order of Precedence and Preemption. Telephone calls designated FLASH shall take precedence over and shall preempt calls designated ROUTINE, PRIORITY, or IMMEDIATE. FLASH calls may be preempted by application of the FLASH OVERRIDE capability. FLASH calls will be handled as fast as possible.

C5.3.2 Application (FLASH). FLASH precedence is reserved generally for telephone calls pertaining to:

C5.3.2.1 Command and control of military forces essential to defense and retaliation.

C5.3.2.2 Critical intelligence essential to national survival.

C5.3.2.3 Conduct of diplomatic negotiations critical to the arresting or limiting of hostilities.

C5.3.2.4 Dissemination of critical civil alert information essential to national survival.

C5.3.2.5 Continuity of Federal governmental functions essential to national survival.

C5.3.2.6 Fulfillment of critical U.S. internal security functions essential to national survival.

C5.3.2.7 Catastrophic events of national or international significance.

C5.3.3 Examples (FLASH). Calls pertaining to:
C5.3.3.1 Initial enemy contact.

C5.3.3.2 Recall or diversion of friendly aircraft about to bomb targets unexpectedly occupied by friendly forces or emergency action to prevent conflict between friendly forces.

C5.3.3.3 Extremely important and perishable intelligence.

C5.3.3.4 Major strategic decisions of great urgency.

C5.3.3.5 Imminent large-scale attacks.

C5.3.3.6 Preattack shutdown of facilities which if damaged would pose a significant hazard to public health and safety.
C5.3.3.7 National security information requiring the immediate attention of the President or the Secretary of State.

C5.3.3.8 Presidential action notices essential to national survival during attack or preattack conditions.

C5.4 Precedence Designator: IMMEDIATE.

C5.4.1 Order of Precedence and Preemption. Telephone calls designated IMMEDIATE shall take precedence over and shall preempt calls designated ROUTINE or PRIORITY. IMMEDIATE calls will be handled as fast as possible.

C5.4.2 Application (IMMEDIATE). IMMEDIATE precedence is reserved generally for telephone calls pertaining to:

C5.4.2.1 Situations which gravely affect the security of national and allied forces.

C5.4.2.2 Reconstitution of forces in a postattack period.

C5.4.2.3 Intelligence essential to national security.

C5.4.2.4 Conduct of diplomatic negotiations to reduce or limit the threat of war.

Borrowed from our friendly

DEPARTMENT OF DEFENSE

UNITED STATES OF AMERICA

HACKER NEWS NETWORK

The Electronic Underground Affiliation is proud to be one of the new digi-publisher affiliates of HNN, the Hacker News Network. The staff of the EUA thanks the staff at HNN for allowing us these rights. The following articles are some of the highlights from past couple of weeks. We hope you enjoy. -editor.

ProMail 1.21 is still a Trojan

contributed by Code Kid

A story that HNN reported on last week has finnally made it to the mainstream. MSNBC is now reporting that Aeon Labs has discovered that ProMail is indeed a Trojan that will steal information from your system and secretly mail it to free account email address.

Aeon Labs
MSNBC

Billionaire CEOs vulnerable

contributed by Code Kid

Bill Gates, Paul Allen, Gordon Moore, and Ted Waitt, among others, have all had their social security numbers exposed through an official Security and Exchange Commission online database called EDGAR. The database, which is no longer used according to C|Net, is still accessible from the web and is still spewing out CEO social security numbers.

C|Net

Encryption Tutorial?

contributed by Eric

Want to know why IT executives are clueless when it comes to security concepts? This tutorial from CIO Magazine creates confusion rather than clarity. It would be funny, if your CIO wasn't reading it.

CIO Magazine

Australian Man Arrested for Unlawful Computer Use

contributed by _GryPhoNN_

Charged with 37 counts of 'unlawfully operating a computer' a man from Perth Australia has not yet entered a plea and has requested legal assistance. Christopher Thomas Daniels, 20, was allegedly in possession of 350 passwords of which he supposedly used 37 and might have caused a whopping $50(Aus) in fraud. All of the compromised accounts where from ViaNet in Western Australia.

Australia Technology News
Via Net

Hacking Contest

contributed by ju

PC Intern, a german Computer magazine is sponsoring a contest to draw attention to web server security. They have set up a WindowsNT and a Linux system with a hidden file. First person to get the file wins an IBM Netfinity-server. Try your skillz.

PC Intern

Federal Prosecutors Leak Info on Mitnick

contributed by Space Rogue

Numerous mainstream media outlets are reporting that Kevin Mitnick has pleaded guilty to computer related crimes. It is believed that this plea of guilty is in exchange for reduced charges and a sentence of mostly time served. The real story is not that Kevin pleaded out as only 4% of federal cases actually go to trial, the real story is how the press got notified of the contents of a _sealed_ federal court document.

If the Honorable Mariana Pfaelzer declines the plea agreement Kevin will still be headed for trial on April 20. If that happens Kevin's defense hopes to introduce a motion that will dismiss most of the evidence against him on the grounds of illegal search and seizure. It would appear the the information used to provide probable cause to issue a search warrant for Mitnick's apartment was itself illegally obtained. The defense is claiming that Tsutomu Shimomura, while a private citizen, was in fact acting as a government agent and therefore subject to the laws regarding illegal search and seizure.

We urge you to visit the Free Kevin site and learn more about what is not being said by the mainstream media.

Free Kevin

AOL Cracker Busted

contributed by ju

Jay Satiro an 18-year old New York resident has been charged with computer tampering after breaking into the systems on America Online. AOL has claimed that it will cost $50,000 to repair the damage done to its data. AOL spokesmen have refused to give out details in the case such as how the intruder gained access, how long he went undetected and exactly what damage was caused. (Ed Note: Would sure be interesting to know how they justify that fifty grand figure. How much can it cost to restore from backup?)

Washington Post

HACKING ARAPANET PART 3

BY

THE SOURCE

STRAIGHT FROM THE
CATACOMBS OF ARCHIVE COMES
AN OLDIE BUT GOODIE

ARPANET can't be faulted for the amount of information it is willing to disclose to anyone who knows the number of a dial-up and knows enough to type in "@N" and then follow directions. But the EXEC is, after all, limited to managing inter-computer phone calls. Even more interesting material is available once you get onto what is known as one of the network's "server" computers.

OPENING THE DOOR

Once you have reached the Exec on a TIP, getting the door to a server machine to open to you is no problem. At the "@" prompt type "O" for open followed by a space and then by two numbers separated by a comma. The numbers represent the address of a computer system. The first number may be from 0 to 3, and the second number may range from 0 to 15:

```
@O 0,11
<the Exec responds:>
TCP Trying...SU-AI WAITS 9.17/H Assembled 06/17/84
.Open
```

The ".Open" shows that you're in. There is a great deal you can do at this level, and you don't even have a password yet -- as far as the system knows, you're still "anonymous guest"! Most server systems operate under the UNIX operating system, so any good manual on UNIX should tell you more than you need to know. But now that we've reached Stanford University's Artificial Intelligence Lab (having been switched there by SRI, formerly Stanford Research Institute), let's take a look at what's available. First, list the HELP files:

```
.HELP
```

```
Job 3   SU-AI WAITS 9.17/H  Assembled
06/17/84
Type HELP followed by any of the following, then carriage return:

ACCESS  COMPIL  EDITOR  HOSTS   MICROS  PPK     SORT
UNDELE  ACCOUN  COPY    EDKEY   HOWBIG  MIDAS   PPSAV
SOS     UNPROT  ACRONY  CPRINT  EFTP    IIIPOX  MLISP
PRESS   SOUP    VERIFY  ADA     CRDIR   EKL     ILISP
MLISP2  PRINT   SPASM   WEAVE   ADAEDT  CRE     EMACLS
IMPRIN  MONCOM  PRLISP  SPINDL  WEB     AL      CREF
ESC     INTERN  MOORE   PROLOG  SPOOL   WHEN    ALIAS
CRYPT   ESCAPE  JARGON  MUSIC   PROTEC  SRCCHK  WHERE
ARKTEX  CSD     ET      KILL    NCOMPL  PROVE   SRCCOM
WHO     ARM     D       ETEACH  KJOB    NET     PRUNE
STICKY  WHOLIN  ARPA    DART    ETV     KRL     NETDOC
PTYJOB  SUTIP   WHOPHN  ARPANE  DDFONT  EVENT   L
NETWRK  PUMPKI  SYMBOL  WL      ASSIGN  DDKEY   EXT
LATER   NEWIO   PUPTIM  SYSTEM  XGP     ATSIGN  DDQ
FAIL    LATEX   NEWS    RCV     TALK    XGPSYG  ATTACH
DED     FASBOL  LAWS    NOEKEY  REMIND  TANGLE  XGPSYN
BAIL    DFTP    FCOPY   LEDIT   NOTEBK  RENAME  TECO
XGPTYP  BATCH   DIAL    FELT    LIFE    NSL     RESOLV
TELNET  XIP     BBOARD  DIALNE  FILES   LIFXGP  OPTION
RESTOR  TEMPER  XPART   BIBOP   DIR     FIND    LINGO
P       RETRY   TERMINK10       PAM     SAIL    TEX78
YUMYUM  BMP     DISPLA  FONT    LISP    PASCAL
SAVE    TEX82   Z80     BOISE   DM      FORWAR  LIST
PASSWO  SCHEME  TFM     ZERO    BOOK    DMKEY
FRAID   LOADAV  PC      SCIP    TIP     370     BOYER
DO      FTP     LOGIN   PCP     SCRIBE  TTY     6500
CANCEL  DOC     GEOMED      LOGOUT  PHONE   SD
TTYCMD  6800    CANON   DOVER   GRIPE   MACLIS  PHONES
SEND    TTYESC  8080    CC      DRAW    GRUMP   MACLSP
PIX     SERVIC  TTYSET  CHARGE  DRD     GUEST   MAIL
PK      SIMPLE  TVFONT  CHRMAC  DSKSIZ  H19KEY  MAP
PLAN    SLAC    TYPE    CKMAIL  DTN     HELP    MAXTEX
POLL    SLR1    TYPREL  COLIST E HELPER METAFO
PONY    SNAIL   UDPUFD  COMBIN  ECL     HOST    MF
```

Type "HELP HELPER" for one-line descriptions of most of the HELP messages.

MORE HELP

If you'd like, try "HELP HELPER" for yourself. Meanwhile more detailed listings of some help files follow.

.HELP GUEST

There is no general guest account on this system. There are some commands that can be given without an account, as listed below. If you need to know more about any of these, type "HELP <topic><carriage return>". For information on special control characters and commands, type "HELP TTY". WHO, FINGER, WHERE, WHEN provide information about people and jobs currently running. MAIL, SEND, GRIPE permit you to send messages and converse with people on the system. (You can use SEND to ask someone who is logged in to form a two-way link with you.) DIR lists the files in specified directories.

TYPE lets you type out the contents of text files. FIND searches text files and prints those paragraphs that contain specified keywords.

If you need to do more than the above programs permit, say "HELP LOGIN".

.HELP NETDOC
Job 5 SU-AI WAITS 9.17/H Assembled

06/17/84 (Much network information is available from the Network Information Center at SRI-NIC. Please consult the network liaison, Martin Frost (ME), for more information about the network or the resources available to you at the NIC.) A large library of source and documentation files about the network, NOT including the host table, live on the [S,NET] directory. Even more hardcopy documentation is available in the bookshelf in ME's office for the general SAIL community (please ask ME before borrowing anything). The host table files can be found on [HST,NET]. The NETWRK library of network subroutines can be found in NETWRK.FAI[S,NET]and NETWRK.MID[S,NET]. Some interesting files are: HOSTS.TXT[HST,NET] The source of the host table SUAI.TXT[S,NET] Our write-up in the Arpanet Resource Handbook.

Most of the network user-level documentation is contained in the Monitor Command Manual, which can be found online by giving the monitor command READ MONCOM<cr>. Large online directories of network documetation exist at SRI-NIC as <NETINFO> and MIT-DMS as NETDOC;.

Type HELP NETWRK for information on programming for the network.

Kjob+

...HELP HOST
Job 5 SU-AI WAITS 9.17/H Assembled 06/17/84 The HOST command is used to look up information in the host table about a particular host name or host number.

This information includes the official name of the host if the name is a nickname, all host numbers known for that host, whether the host is a user or a server, the host machine and the host operating system.

To use HOST, type HOST followed the host name (or any abbreviation) you want to look for, or the host number, and return. The program will print all hosts (and nicknames) which match the input specification. A null specification will type out the entire host table, but only if you are logged in. For example:

```
HOST MIT-MC            (describe MIT-MC)
HOST CMU               (describe all CMU sites)
.HOST 36.40.0.194      (describe Internet host 36.40.0.194)
.HOST 50#302           (describe SU Ethernet host 50#302)
.HOST                  (print out the host table)
```

Note that even non-unique abbreviations are accepted. For example "SU" will print out ALL of the Stanford University hosts. This is different from TELNET, etc., which only accept abbreviations which are unique to a single host. Kjob

(In Hacking ARPANET Part IV we'll report on some more important help files.) Example "SU" will print out ALL of the Stanford University hosts. This is different from TELNET, etc., which only accept abbreviations which are unique to a single host.

DECLASSIFIEDS

The products, software, and/or merchandise mentioned in these is advertiesed free of cost.
The EUA Monthly only publishes these for their readers and makes no claims/profits.

What is TechAds? TechAds is a online classified site that caters to the desires of the hacker community. The site is run and operated by the 719 group, you can peruse the links bellow to see if you can find what you need or want or you can place your ad for that old Comodore 64 you have in the attic.

For Sale	Wanted
Computers	**Computers**
Hardware	**Hardware**
Software	**Software**
Books	**Books**
Miscellaneous	**Miscellaneous**

Submit your ad!

This site is copyrighted 1999 SON

The full Harmless Strategies members website on CD-ROM

All the files and texts from the Members website in one place! Three years of accumulating the best software and tutorials for beginners and experts alike. Learn to use trojans like back orifice and masters paradise! Adult site passwords! Control viruses, make them and kill them!

Incredible collection of software!

Included on this cd is the latest software programs which will allow you to crack, hack ,reverse engineer, and more! These are mostly shareware programs!

You do not need to buy the cd in order to obtain these programs. Simply send me an email with the program or text file you want and i will send it to you through email or send you the url! They are included on the cd for people who do not want to be tracked or spend hours downloading from their service provider.

SoftIce *Used by the best crackers in the world!*

UltraEdit *Must have editor for crackers and reversers*

NukeNabber *Detect people trying to access your machine through your modem!*

Windows Washer *Automate the cleansing of your cache and history files and more!*

NeoTrace *Find out exactly where your packets are sent*

Dll Show *Know when a trojan is planted in your machine!*

Type it in *Automates filling out forms. Use it to attack password programs.*

The Cleaner 2 *Detects all known trojans on your machine.*

Directory Snoop *Find files that are supposed to be erased! Unerase data easily!*

EnCase *Software used by law enforcement agencies to get private data.*

BC Wipe *Use this program with encase (above) to insure your data is gone forever!*

BlowFish *Encrypt your data with military strength*

WWWHack *Make ur own passwords for any adult or password protected site on the net!*

Glide *Another great password buster*

Nag Buster *Get rid of annoying nag screens on shareware*

Oscar 10.3 *Thousands of serials and cracks for the latest shareware.*

Romeo *Hundreds of serial numbers in an easy to use program.*

*Texts **

ICQ Hacking utilities
The famous Jolly Roger Cookbook
Serials- more than 9,000 in one searchable text!
The MIT complete guide to lockpicking
Anarchist Cookbook
Harmless Strategies Anyone Can do
Phreaking Telephones
Universal Product Codes
How to Nuke people, How to Mailbomb!

** These tutorials and software are offered on the cd but are also available freely on the internet! If you have trouble collecting any of the above articles please send me an email and they will be provided to you free of charge through email or I will send you the URL where they can be located. The purpose of providing them on the cd is to avoid tracking and save you time charges through your service provider. (Do not request more than three at one time!)*

Your purchase will include one year of website access in the Harmless Strategies Member Site! As well as the weekly newsletter!

Everything is contained on a CD-Rom delivered anywhere in the world for the ridiculously low price of only $45.00 (US) $60.00 Canadian funds
This price includes shipping anywhere in the world!

FAQ

Is the cd rom update able?

Yes. The website will provide updates as well as new programs and texts.

I'm already a member. Do I have to pay full price?

No. As a member, you can discount the cost of the members payment from the cd.

You must send your payment along with your address and present membership details.

I live outside North America? Can i still get delivery?

Yes. Anyone can order from almost every country. You must send me details of any different instructions I may have to make in order to ship to your particular country. Postage to anywhere in the world is included in the price!

Can I get immediate access to the members website?

Sure. If you pay by credit card, you can get instant access. The delivery of the cd-rom may take several weeks. (depending on where you live) After you have paid using your credit card you must send me details of your mailing address to my email address. Thomas@Yeomans.com

What is the most private method of payment?

Snail mail is the most discreet method of payment. You will be sent the cd-rom in an unmarked cd mailer with only my name and mailing address, along with your name and address written by hand in ink. When you send your payment make sure you have included a written note with complete address details!

What is your mailing address?

Make your payment payable to me, Thomas Yeomans. My address is
RR#3, New Germany
Nova Scotia, Canada
B0R 1E0

Is there a refund or guarantee?

I will not refund the cd for any reason other than defects. Too many people will burn their own copy and then try to return it. Each cd has been tested and run before I send them out. I know how frustrating it is to get defective stuff !

Are cracks available on the cd as well?

No. The law states very explicitly that I can not put cracks on the same website, cd-rom or disk as shareware. Another thing about cracks is that they age very quickly. Everyone who becomes

DO YOU
HAVE AN AD OR CLASSIFIED
YOU WANT RUN IN THE EUA MONTHLY?

If you have a advertisement or classified that you want to run in the EUA Monthly Zine, contact email **archive** subject: AD/CLASS. Ensure that the document gives your email address, description of ad/class to be run, cost, etc. pic’s of products are welcome. Thats it.

About Subscriptions

We want to take this time to thank people who have read our little zine up for the straight, unadulterated, 411. Remember, throw the zine up as hard copy, post it to a bbs, give a copy to your boss. We want to provide as many subscriptions as we can. If you want to subscribe to the zine all you need to do is email archive_@hotmail.com subj: Subscribe Monthly Zine. We work on trying to get in touch with each and everyone that signs up for the Zine. But if you do not hear from us a while, do not get depressed, keep checking the EUA Monthly Zine site and download it once it hits the street.

Hope that you are all doing well.

Do you want to carry a copy of the EUA Monthly Zine on your BBS or website? Contact archive by email and let me know where to send the copy of the zine to and we'll get it to you. If you have a site that wants to carry it just let us know and link it to our website. If you run a bbs, we'll upload at our cost.

l8r - *The EUA Staff*

Electronic Underground Affiliation

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

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**
Northern IL Digital Publishing	**Highlander**
Chicagoland Digital Publishing	**Subhuman**
	Fringe & Enigma
NC Digital Publishing	**Lord Apathos**
PA Digital Publishing	**CyberMonk**
OR Digital Publishing	**Phrack Wolf**
Canadian Digital Publishing	**Zarkov**
Australian Digital Publishing	**DuRab**

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.:

ShaGGy^C	— Bad Case of BO
Forensic	— Logo & Design Work
Dildog	— L0pht WinNT 4.0 Advisory
Daemon0	— Pirch 32/98

Visit our website @
http://www.freespeech.org/eua

So come on already! tell us!

What’s coming next month?

Well the next edition of EUA Monthly will be out and that is about all that we can say. This comes from having to go on tour around europe. Expect to see the next edition of EUA Monthly around the middle of April. Raven and myself will be keeping the zine going while I am working abroad.

Micro$oft Exchange $erver Information

by Lord Apathos
(pending information from him)

DEFENSE SWITCHING NETWORK
PART THREE

by Archive
(last of this series)

NetTrash 4.0

by Anonymou$
(a log of an actual hack of a system)

IRC tips and ‘ploits

by Gigsaw
(some things that can help you on irc)