CERN
CN/DCI/161

CERN Security Handbook

Practical computer security for CERN users
Version 1.0
2 December 1993

Lionel Cons

Foreword

This guide is intended for end users of computing facilities at CERN. It tries to explain *why* and *how* a user should protect himself. It does not explain how to protect a system, for this purpose please consult one of the many books written on this subject[1].

An up-to-date postscript version of this manual may be obtained via anonymous `ftp` from *asis01.cern.ch*:'`/pub/doc/CERN/us.ps`'. Printed copies are also available from the UCO. An on-line version of this guide is available in the World-Wide Web (CERN Home Page -> UNIX Workstation Support -> Security).

When talking about security several terms are usually misinterpreted:

hacker according to the "official" jargon[2]:

> 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it.

cracker according to the "official" jargon:

> One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of hacker.

attacker a non-ambiguous synonym of cracker, we will use this term here. Note that an attacker does not necessarily try to damage things.

vandal an attacker with bad intentions.

[1] For instance *Practical UNIX Security* by S. Garfinkel and G. Spafford, O'Reilly & Associates.

[2] By "official" jargon I mean "as it appears in the *Jargon File 2.9.9*". This file is a comprehensive compendium of hacker slang illuminating many aspects of hackish tradition, folklore, and humour. It is freely available on the Internet.

1 Security at CERN

Like all other centres exploiting a large number of computers, CERN is obliged to take computer security quite seriously. Our situation is made particularly sensitive given the large variety of operating systems and the prevalent use of network access from outside the laboratory.

1.1 Why should I protect myself?

You should care about security for at least three reasons:

1. **for you**: an attacker may - intentionaly or not - use, modify, corrupt or destroy any of your files; he can waste resources such as CPU time, disk space, tapes, paper...
2. **for your friends, coworkers**: an attacker can use your account to damage other people accounts, he can damage the projects that you work on.
3. **for CERN**: an attacker can waste CERN resources but he can also use CERN as a starting point for further attacks, this can damage CERN's reputation[1].

1.2 CERN is not a bank!

Right. But CERN attracts many potential attackers for several reasons:

- its name contains the word '`nuclear`' and therefore attracts everyone looking for nuclear weapons, nuclear plants, military secrets...
- CERN is seen as a big scientific institute and is as attractive for Europeans as the NASA is for Americans.
- it is well connected to the academic and scientific networks, therefore it's a perfect hopping point to attack other sites, particulary when hopping between network architectures such as X25, DECnet, IP and in the future OSI.

Please note that this is not a myth: CERN main machines (VM, VMS, UNIX) have suffered from several "big" security incidents caused by attackers or worms. The last one occured in July 93 and involved the Geneva police! These incidents cause a waste of manpower to track the intruders and to get rid of them. Most of the time CERN has been lucky in that no important data was lost.

CERN is being attacked now! CERN's firewall (a kind of main entrance for networks) rejects thousands of packets per hour, we believe that a significant number of packets come from attackers. Central systems see several "minor" incidents (for instance intruder using someone else's account) per month. Note that this is only the tip of the iceberg, many attacks remain undetected...

[1] Note that this is not science-fiction, the name of CERN appears in several articles and books about computer breakins which originated at CERN, cf. for instance *The Cuckoo's Egg* by Clifford Stoll.

1.3 Who shall I call in case of problem?

First of all you should contact your local system administrator. In addition, you should also contact the CERN Computer Security Team (Computer.Security@cern.ch) and/or the CERN Computer Security Coordinator, currently John Nigel Gamble (e-mail: John.Gamble@cern.ch, phone: 3105, office: 31 3-030).

2 Passwords

From experience, a significant number of computer breakins (perhaps the majority) can be traced back to a poorly-chosen password. In most of the cases, passwords are the first weakness tried by an attacker.

The password is the most vital part of account security. If an attacker can discover a user's password, he can then log in to the system and operate with all the capabilities of that user. Such an attack is usually hard to detect and can last for months.

Furthermore, as almost all the computers at CERN are connected together, the mis-use of one account on one computer may lead to problems for several accounts on several machines, including critical ones (data handling, beam control...).

2.1 Why should I care?

The answer is easy.

You **must** care because it's written in the Computer Rules that **you have signed** (see Appendix A [Rules], page 14).

> A computer user shall take all reasonable care to protect his or her account and data from unauthorized access, in particular he/she should keep his/her password confidential and should employ non-trivial passwords. He/she should follow the currently recommended methods for choosing a password (see CNL 197, 1989).

You **should** care because if someone uses your account to do bad things you will have no means to prove that it was not you. It's like letting anyone drive your car, you would then be responsible for all the fines...

2.2 What is a good password?

A good password is:

- **private** (it is used and known by one person only)
- **secret** (it does not appear in clear text in any file or program or on a piece of paper pinned to the terminal)
- **easily remembered** (so there is no need to write it down)
- **not guessable** by any program in a reasonable time (less than one week).

Although this seems quite restrictive, it's easy to pick good passwords.

2.3 How can I choose a good password?

Several articles cover this subject, see for instance the CNL articles: [**197**], [**210**], [**211b**]. The following comes mostly from [**210**].

The programs that try to guess passwords (or the attacker of a machine) do not try all existing passwords, they only try a large number (10^8) of "frequently used" passwords. So if you stay out of this search space you are safe; to do so you can follow the following guidelines:

First, here is what you **should not do**:

- **don't** use your login name in any form (as-is, reversed, capitalized, doubled, with a prefix, with a suffix...).
- **don't** use in any form your first or last name and, more generally, any information easily obtained about you. This includes car license plate numbers, telephone numbers, social security numbers, the brand of your car, the name of the street you live on, the name of your spouse or of your children...
- **don't** use a word contained in any dictionary of any language, spelling lists, or other lists of words (acronyms, sequences of letters like 'abcdef' or 'qwerty', place names, car names, cartoon heroes...).
- **don't** use a password shorter than six characters or with only alphabetic characters or only digits.

Then, here is what you **should do**:

- **do** use a password with mixed-case alphabetics, digits, punctuation.
- **do** use long passwords (with more than 6 characters).

Finally, here are some methods of making passwords:

- Choose a line or two from a song or poem, and use the first letter of each word. For example, '`In Xanadu did Kubla Kahn a stately pleasure dome decree`' becomes '`IXdKKaspdd`'.
- Alternate between one consonant and one or two vowels, up to eight characters, do use mixed-case. This provides nonsense words that are usually pronounceable, and thus easily remembered (ex: '`roUtboo`', '`quADpop`', and so on.).
- Choose two short words (or a big one that you split) and concatenate them together with a punctuation character between them (or a digit if you can only use alphanumeric characters). For example: '`dog+F18`' or '`comP7UTer`'. Note that '`dog`', '`F18`' or '`computer`' are in dictionaries but as the passwords use punctuation or digit, mixed-case character, they are really hard to guess.

Remark: if you use mixed-case characters, do not use the following methods (they are tried by most cracking programs):

- all lowercase or all uppercase
- only the first or the last character in uppercase
- only vowels in uppercase
- only consonants in uppercase.

2.4 My good UNIX password is refused on VM!

Remember that each operating system imposes its own restrictions:

- UNIX: you can use all printable characters, case **is** significant and only the first 8 characters will be used, so in the password '`computer+3,Z`' only '`computer`' (an easy-to-guess password) is significant and the remaining characters will be ignored[1].
- VM: you can use only alphanumeric characters, case **is not** significant and the maximum length is 8.
- VMS: you can use all printable characters, case **is not** significant and you can use long passwords (up to 32 characters).
- AFS: you can use all printable characters, case **is** significant and you can use passwords of virtually any length.

In addition, each system manager can impose some other restrictions. The current official restrictions at CERN are described in [**211b**], they contain:

- minimum length is 5, null passwords are forbidden
- new passwords must differ from previous one(s).

In case of doubt, consult the relevant system manager.

2.5 Why should I change my "good" password?

Even if you choose a good password, it can still be discovered: someone may see you typing it, he may capture it by snooping the network... One can also setup a fake machine or terminal and record all the passwords it sees. Another commonly used source of passwords is the "bad login" file, some people do not pay attention and type the password instead of the user name, the log file then contains lines like:

```
joe      ttyp9       Wed Apr 28 09:37
XSecret! pty/ttys0   Fri Feb 26 15:15 - 15:16  (00:00)
fred     pty/ttys0   Fri Feb 26 15:16 - 14:27 (87+22:11)
```

For all these reasons it is wise to change your passwords from time to time, a minimum frequency is twice a year.

2.6 Can I use the same "good" password for all my accounts?

This is delicate to answer. The underlying problem is that if someone finds your password for one account (see Section 2.5 [Why should I change], page 6) he then may be able to use other accounts on other machines with the same password.

[1] On some systems like Ultrix with Upgrade Security you can have passwords with up to 16 characters.

One thing is clear: you should not use trivial rules to generate your passwords. For instance if you've got several accounts on the machines *hplhc01*, *hplhc06*... and the passwords are '`secret01`', '`secret06`'..., this is clearly inefficient. An attacker can easily deduce the passwords you used and the length of the fixed part of the password (in this example '`secret`') is reduced, this implies that you will have less choice to find new passwords.

On the other hand, if an attacker broke into one of your accounts, he has several possibilities to break into other accounts: he can use the autologin facilities (cf. '`.rhosts`' on UNIX), he can install a fake `telnet` program to capture your passwords the next time you use it...

So, in my opinion, the best thing is to have different passwords for all your accounts **with no obvious similarities**. If you can't (for instance because you have too many accounts), it's acceptable to have the same password if it's a really good one **and** if you change it often (for instance once per month)[2].

[2] If you think that it's painful to change a password on many systems, some tools exist to ease this task (cf. the `expect` script called '`passmass`' on UNIX).

3 X Security

The X window system is widely used by workstations, X terminals, PCs with X emulation... It is very convenient and can ease the work. However, this windowing system is usually not well understood and the security implications are, in general, not known.

This chapter describes the security issues of the X window system. If you don't use X you can skip it. If you use X (i.e. you use a workstation, an X terminal or a PC with X emulation) then you should read it.

I will assume that you have a basic knowledge of the X window concepts (X server, X client, display...). If that is not the case please read the appropriate manuals, for instance the man page *X(1)*.

3.1 Why should I protect my display?

If you don't protect your display you are vulnerable to sevaral "attacks"; someone may:

- view the contents of your screen, this is not important unless you've got something to hide.
- create windows on your display, this can be funny for the April's Fool.
- destroy any window on your screen, this can be annoying and even dangerous (imagine a vandal destroying windows that control the accelerators...).
- see everything you do (especially the keys you press), this implies that any password you type can be recorded...[1]

3.2 How can I protect my display?

Two standard mechanisms are available in the X window system.

3.2.1 Host-based access control

The oldest mechanism is a host-based access control list. You list all the hosts (machines) that can access your display[2].

On UNIX systems the list can be viewed and modified with the command *xhost(1)*, on VMS and ULTRIX workstations you can use the Session Manager, menu 'Options -> Security...', on most X terminals you should have a 'Security' or 'Access Control' section in the setup panel.

[1] Please note that if your display is not protected the only way to prevent someone from reading what you type is to use XGrabServer(3X) (`xdm` does this when it prompts for a user name and password), the option 'Secure Keyboard' of `xterm` or `dxterm` that uses XGrabKeyboard(3X) is perfectly useless!

[2] If you use DECnet you can specify a node name **and** a user name.

This mechanism has an obvious limitation: if you allow a machine to access your display it means that you allow all the users of this machine to access it. This is clearly a problem on a server with hundreds of users[3].

3.2.2 User-based access control

Starting with X Version 11 Release 4 (X11R4), a user-based mechanism is now available. When the X server is started with the appropriate option, it reads an authorization file that contains a key (called "magic cookie"). When an X client wants to access the display, it must give this key to the X server.

On UNIX systems, the file containing the key is usually called '`.Xauthority`' and is located in the user's home directory. This mechanism does not exist on VMS or VM. On X terminals you may be able to enter manually the key in the setup panel, otherwise you can do it with `xdm`, (see Section 3.3.2 [XDM], page 10).

Once the display is protected, if you want to run an X client on a remote machine you must transfer the key to this remote machine. On UNIX systems this is usually done with the help of *xauth(1)* and remote shell. The easiest way to handle this is to use `xrsh` (see Section 3.3.1 [xrsh], page 9).

Both mechanisms can run together. In this case the protection is minimum: a connection is accepted if one mechanism accept it. This implies that if you use the user-based access control you must take care of removing all the hosts in the host access control list.

Please note that this mechanism is not bullet proof. If someone can access the key stored on the remote machine he will then be able to use it to start X clients. Also, someone snooping the network may capture these keys...

3.3 Are there some tools to help?

Fortunately several tools exist to ease the use of one of the standard X protection mechanisms. Some other tools can also bring a better level of security.

3.3.1 xrsh

`xrsh` is a shell script that runs any given command on a remote host. It sets up the environment for that command such that it will display its windows on the current server's screen by propagating the DISPLAY environment variable. `xrsh` automatically handles authentication so that the remote client will be allowed to open windows on the server; it understands the host-based and the user-based mechanisms.

[3] This mechanism has also a non-obvious limitation: every user of a workstation will be able to access the local display, think of it if you use NIS (the yellow pages).

For instance:

```
# to run xbiff on dxcern using xhost
xrsh -auth xhost dxcern xbiff
# to start a new terminal on parcb with user name fred using xauth
xrsh -auth xauth -l fred parcb xterm
```

Note that `xrsh` uses the remote shell to start the command on the remote machine. The user must be authorized via the '`.rhosts`' file. See *hosts.equiv(4)* for more details.

`xrsh` is part of the X11R5 distribution and should run on any UNIX system. It may be partially ported to VMS but this requires some work.

`xrsh` is available on ASIS under '`/usr/local/bin/X11`', for information on how to use it, see the man page: *xrsh(1)*. Please note that the ASIS version of `xrsh` has been modified to work well with `mxconns`.

3.3.2 XDM

`xdm` manages local and remote X displays. It provides services similar to those provided by `init`, `getty` and `login` on character terminals: prompting for login/password, authenticating the user, and running a session. It manages your complete X environment (it sets the display, starts programs...).

`xdm` can be configured by the system administrator to use the user-based protection mechanism[4]. In this case, it creates the "magic cookie" for you; all you need to do is propagate the cookie, with `xrsh` for instance.

`xdm` runs on all UNIX systems, it does not exist for VMS or VM. It can be used from any workstation or X terminal. For more information please consult the manuals (especially *xdm(1)*) or the relevant system administrator.

3.3.3 mxconns

`mxconns` is a public domain tool that can be used to secure your display. You will be prompted for each new connection to your display asking whether the connection should be authorized or not.

`mxconns` should run on all UNIXes and is available on ASIS under '`/usr/local/bin/X11`'. For more information, see *mxconns(1)*.

[4] Cf. the resource '`authorize`'.

3.4 So what should I do?

Here is what you should do to protect your display:

3.4.1 on a workstation

If you use a workstation, you should use `xhost` and `xauth` to secure your display, use `mxconns` to filter the connections to your display and `xrsh` to start remote X clients.

For this, the easiest solution is to use XDM and to follow the instructions of the next section (see Section 3.4.2 [on an X terminal], page 11). If you don't use XDM, you'll have to play with your vendor specific session manager. For instance, on a HP workstation:

3.4.1.1 HP (VUE)

To enable user-based authentication mechanism, set the resource '`Vuelogin*authorize`' to '`true`' in the file '`/usr/vue/config/Xsession`'.

To start `mxconns` for all users, modify '`/usr/vue/config/Xsession`'; to start it for one user, modify '`$HOME/.vue/sessions/sessionetc`':

```
/usr/bin/X11/xhost -
/usr/local/bin/X11/mxconns -dispno 1 -geometry +0-0 -xrm \*workspaceList:\ all &
```

For ASIS' `xrsh`, set the variable XDISPLAY to the display created by `mxconns`: <local_host>:1. Modify '`/usr/vue/config/Xsession`' for all users or '`$HOME/.vueprofile`' for one user.

3.4.2 on an X terminal

If you use an X terminal (or a PC with X emulation, or a workstation configured as an X terminal), **you should use XDM** with user-based access control.

For this, check that the machine where you usually log in runs XDM[5] and is configured properly[6]; if not, ask the system manager on this machine to configure it. Note that only UNIX machines support XDM...

For a better security **you should use** `mxconns`. To do so, just add the following lines to your '`$HOME/.xsession`' file:

```
mxconns=/usr/local/bin/X11/mxconns
tmp=/tmp/tmp.$$
# mxconns stuff for use with xrsh
xhost -
```

[5] To do so, just start an XDM session on this machine to see if it replies.

[6] To do so, log in via XDM and check with `xauth` that you have a new "cookie".

```
if [ -f $mxconns ]; then
   $mxconns -verbose -hunt -dispno 2 > $tmp &
   while [ ! -s $tmp ]; do
      sleep 1
   done
   XDISPLAY=`cat $tmp`; export XDISPLAY
   rm $tmp
fi
```

When all this is done, use `xrsh` to start a program on a remote machine. Et voila, your X terminal is safe...

References

CERN Computer Newsletter (CNL) articles:

[**197**] David Lord: *Advice on the Choice and Use of Passwords*

[**210**] Lionel Cons: *How to choose a good password*

[**211a**] Lionel Cons: *Crack, a password checking system service at CERN*

[**211b**] John Gamble: *CERN's password security policy*

Man pages:

X(1) a portable, network-transparent window system

Xserver(1) X Window System server

mxconns(1) an X11 connection monitor

passwd(1) change login password

xauth(1) X authority file utility

xdm(1) X Display Manager with support for XDMCP

xhost(1) server access control program for X

xrsh(1) start an X program on a remote machine

Appendix A CERN's Computing Rules

Note that any user of the CERN computing facilities **must have signed** the 'CERN Computer Center User Registration' form (DD/US/REG) that contains:

> I, the undersigned, agree to use the CERN computing facilities in accordance with the User's Rules [...] which have been notified to me [...].

Revised Rules for the use of Computing Facilities at CERN

CSP/91/05

A.1 Introduction

The computing facilities at CERN, both in its Computer Centre and on the rest of its site, including mainframes, work stations, networks both on- and off-site, support services, program libraries, etc. are provided exclusively for the work of the Laboratory as set out in The Article II of the CERN basic Convention of the 1st July 1953, as amended 17th January 1971.

Almost all computers and workstations at CERN are connected directly or indirectly to a communication network. Hence mis-use or lack of adequate security on any of these systems can lead to problems for other systems at CERN. Furthermore for many of these systems, the maintenance support and the software licenses are provided under contracts made between CERN and their suppliers or other companies.

As a consequence these Rules including the above opening statement apply to all who make any use of computers, including work stations or personal computers, on the CERN site unless they are not connected directly or indirectly to a communication network and are not subject to any contract or license agreement entered into by CERN.

The computing facilities at CERN are not available for public access and use: they are subject to specific rules as set out herein.

CERN reserves the right to: refuse registration and authorization to use any system that is its property; refuse permission to install a computer on the CERN site; disconnect any computer from the networks or exclude it from any contract, agreement or license between CERN and a third party.

A.2 Use in General

1. The computing facilities, including networks, must not be used other than for their intended purpose in connection with the CERN official programme of work, unless subject to a special agreement.

   In particular, access to CERN's or third parties' computing facilities resulting in acts or omissions prejudicial to property and legitimate interests is strictly forbidden.
2. The operational procedures in force and the instructions of the staff in charge must be followed.

A.3 Account Codes, Passwords, Data and their Protection

1. Account codes and passwords must be used in a manner compatible with the official purpose for which they have been allocated.
2. A computer user shall take all reasonable care to protect his or her account and data from unauthorized access, in particular he/she should keep his/her password confidential and should employ non-trivial passwords. He/she should follow the currently recommended methods for choosing a password (see CNL 197, 1989).
3. Any evidence of unauthorized access to an account or to data shall be reported immediately by the user concerned to the staff responsible.
4. A computer user shall not engage in unauthorized access to other accounts or the data of other users.
5. The search for the passwords of other users or system accounts, or any attempts to find and exploit any security weakness of computing facilities at CERN, or to make use of any of these facilities in attempts to attack computing facilities outside of CERN, are deemed to be abusive.
6. The confidential nature of any data or other material that may become available to a user, either in the normal course of his or her work, or inadvertently, shall be respected.
7. CERN's external network connections must not be used to make transfers of technical data, not in the public domain, that would violate any export regulations.

A.4 Privileged Use and Protection

1. Special services or arrangements and exceptional allocations of time or permanent file space must be requested from the staff appointed for that purpose.
2. When a computer user has been entrusted with a privileged account, it must be used only for the purpose for which it was intended; those privileges must not be abused.
3. For all users who have been given access to privileged use of a system, the level of their password protection must be increased appropriately .
4. If as a result of, for example, departure or change of project, a user no longer has the right to access privileged resources, then he or she must immediately inform the appropriate staff and return any material connected with that privilege.

A.5 Budgetary and Resource Control

1. A computer user must comply with the instructions in force or notified to him or her by the group or divisional administrator or other staff responsible for the control of resource usage.
2. He or she shall inform the appropriate administrative staff of any change in his or her status which would affect his or her eligibility for computer access, in particular departure or change of project.

A.6 Intellectual Property of the Organization and of External Holders

1. As CERN holds the intellectual property rights associated with its own computer hardware, software and documentation; neither a computer user nor any other person may reproduce them by any means, market them or make them otherwise publicly available, without obtaining the formal permission in advance from the Organization.
2. For certain CERN-written products the permission to reproduce is given by specific mention thereon.
3. The intellectual property rights of programs and associated material supplied by outside organizations, are held externally. Such programs an material may only be used on those machines for which they are licensed and no unautho- rized copies may be made for use on-site or off-site. Users may not reveal to a third party any information about such programs or material that would infringe on these property rights or about any security mechanisms incorporated in them.
4. In case of doubt, advice should be obtained from the Program Library office on questions of external property rights. If these rights are infringed through deliberate abuse or gross negligence, personal liability of the person involved may be involved according to the applicable laws.

A.7 Sanctions

1. In the case of duly established breach of one of the above rules or of any abuse of the computing facilities at CERN, the Organization may take action against the person concerned.

   In the case of CERN Staff Members, the provisions for disciplinary measures of the CERN Staff Rules & Regulations will apply.

   In the case of other persons, they would be subject to the authority of the Director General of CERN, who may take action ranging from a simple warning to immediate exclusion from further use of the CERN facilities.
2. In the case of acts and damage directed against CERN or its computing facilities, the Organization formally reserves all rights of civil and penal proceedings.

Table of Contents