The Witch Hunt[‡]

Heejo Lee[*], John Milburn[†], Jong Kim[*]

{heejo, jem, jkim}@postech.ac.kr

Abstract

This report details the story of tracking a cracker who broke into a number of computer systems at the Pohang University of Science and Technology (POSTECH) and at Ewha Women's University. The cracker is someone who had been given a position of trust and responsibility within the Korean Internet community. The attack methods include exploitation of a ypupdated bug and sophisticated IP spoofing, similar to what Mitnick used in the Shimomura attack. This is the first Internet cracking incident in Korea which will result in imprisonment.

Sun. Apr. 7th, 1996

Upon returning from a three-day holiday, Heejo checked his voice mail, which he had neglected to do during his trip. There were 5 messages. Most of them were complaints from Professor Jong Kim about not having been notified about this trip. Professors always seem to complain when their students take a break. While Heejo is grumbling over the unpleasant messages, one strange message from a fellow student is heard: *"Dear Brother Heejo, POSTECH was hacked at dawn on Arbor Day, Friday April 5. Please call me soon."*

Mon. Apr. 8th, 1996

The damage is much larger than expected. Seven major machines of the Electrical Engi-

[*] Heejo Lee and Jong Kim are with the Department of Computer Science and Engineering, Pohang Univ. of Science and Technology, San 31 Hyoja Dong, Pohang 790-784, KOREA.

[†] John Milburn is with the Pohang Accelerator Laboratory, Pohang Univ. of Science and Technology, San 31 Hyoja Dong, Pohang 790-784, KOREA.

[‡] This paper will be presented at the Network Security '96, Washington DC, Nov 4–8 1996. For more information about the conference, look at http://www.sans.org/ns96.html.

neering and Physics departments have been made completely useless. Most machines' file systems were entirely deleted, and some machines, among them POSB, are locked with an unknown EEPROM password. POSB is one of the most popular free BBS services in Korea, having more than 1500 users, and serving about 50 concurrent users. Major projects in two laboratories are stopped dead. Laboratory courses which had used these machines are cancelled. The only obvious track left by the cracker is a console message on POSB.

"Apr. 5 02:25 posb login: ROOT LOGIN from dal2.kaist.ac.kr"

Heejo and the manager of POSB start to trace the cracker.

Since March, Heejo, John Milburn and Prof. Kim (HMK) have been tracing and monitoring a cracker who broke into the network of a large Korean company. HMK suspect that the cracker who broke into POSTECH might be the same person who broke into the company, since the damage patterns in the two places are very similar. HMK also suspect that the cracker who broke into the company was a student of the Korea Advanced Institute of Science and Technology (KAIST). Intuitively, HMK feel that this incident will have some very serious result, and that the cracker is a real bad guy with good cracking skills. Though HMK have no direct responsibility for such incidents at POSTECH, they are interested, and begin to follow the progress.

Fortunately, the manager of POSB has access to a user account on the 'dal2' machine at KAIST. The owner of that account is a KAIST graduate student who did his undergraduate work at POSTECH. He had studied at the laboratory in which the hacked machines are located. The POSB manager copied some of the log files `'(/var/adm/wtmp,pacct)'` from 'dal2' to a safe place. However, checking of the 'wtmp' file revealed that all login records near the time of the incident have been removed.

Tue. Apr. 9th, 1996

The incident is reported to the computer center of POSTECH. In her official capacity, one staff member attempts to contact the manager of the KAIST computing center, which is responsible for the 'dal2' system, and requests cooperation to catch the cracker. The POSTECH staff requests an investigation, and also log data from various KAIST machines near the time of the incident. POSTECH hopes that some helpful information will come from the KAIST investigation.

Wed. Apr. 10th, 1996 thru Thu. Apr. 11th, 1996 Dawn

In the morning, an e-mail message from KAIST is received. They write that after a careful investigation in cooperation with KUS (KAIST Unix Society, a cracking defense group at

KAIST) members, nothing helpful was found, and they suggested that perhaps the cracker had only used the ‘dal2’ machine as a blind, since it has an open account which provides telnet service. None of the requested information, including the log files, is delivered.

If as the KAIST men said there is nothing helpful in ‘dal2’, then further tracing seems near impossible. If so, this incident would be forgotten, and the damaged party would have to endure the pain. One major difficulty is the long delay between the incident and the beginning of back tracing, which allowed plenty of time for the cracker to cover his tracks.

At night, Heejo, John, and Prof. Kim start to probe the ‘dal2’ logs which were copied on Monday. While checking the process accounting file `(/var/adm/pacct)`, HMK find that the cracker used ”slammer”, a program for exploiting an rpc.ypupdated bug in SunOS 4.1.X. Among the things found from the log are:

1. At 2:20am Apr. 5th, the cracker somehow got root privilege on ‘dal2’. After that, he used ftp to copy the slammer source code from somewhere unknown, compiled and ran it to gain access to some machine.

2. Immediately after this, he used the ‘telnet’ program to connect to the target machine. The target machine was probably POSB, since the time of the telnet matches the time of the log entry left on the POSB console.

3. It had taken only 5 minutes from the point he got the root privilege of ‘dal2’ to the point he logged into POSB as root.

After carefully checking the command sequence from the log file, one point becomes apparent. The cracker was not using a normal user account before he got root privilege on ‘dal2’. Also, he was not using the telnet account that was mentioned by KAIST.

This is clear because there was no user processes associated with the same tty which was used by the cracker. This implies that he became root as soon as he logged in ‘dal2’. Figure 1 shows the pacct listing of the last three processes recorded as the cracker terminates his login session on ‘dal2’ at 4:22am Apr. 5th. Note that the accounting information of a process is recorded at its finish time.

In the Figure 1, the two commands, *csh and in.telnetd*, indicate that the cracker logged in the system using ‘telnet’. And, the two commands, *in.telnetd, telnet*, indicate that he did not login to ‘dal2’ from the same machine using ‘telnet’ since the two processes have different start times. The ‘telnet’ process is one used to connect some other system. The ‘X’ in the ‘telnet’ entry indicates that the process was terminated in an abnormal way, probably when the POSB machine died.

```
% lastcomm | less
sendmail  F    root     __         0.02 secs Fri Apr  5 04:27
xdm       F    root     __         0.08 secs Fri Apr  5 04:26
xdm       F    root     __         0.09 secs Fri Apr  5 04:23
xdm       F    root     __         0.11 secs Fri Apr  5 04:22
csh      S     root     __         1.27 secs Fri Apr  5 02:20
in.telne S     root     __        29.95 secs Fri Apr  5 02:20
telnet       X root     ttyp8     35.02 secs Fri Apr  5 02:25
xdm       F    root     __         0.09 secs Fri Apr  5 04:21
xdm       F    root     __         0.08 secs Fri Apr  5 04:20
xdm       F    root     __         0.08 secs Fri Apr  5 04:15
sh       S     root     __         0.08 secs Fri Apr  5 04:15
find           root     __         0.55 secs Fri Apr  5 04:15
rm             root     __         0.03 secs Fri Apr  5 04:15
```

Figure 1: Command list around the cracker's logout.

The cracker logged into 'dal2' as root and used ttyp8. There are two possibilities: The cracker knows the root password of 'dal2', or he had previously made a back door in 'dal2' and used it for the root login. The first possibility is not very likely, since the real root user is a computer center staff member who is unlikely to either give away the password or to be working after midnight.

Also, if the cracker had sniffed the root password and used it to login to the system via normal methods, he should have tried to delete the login records to conceal the fact that the root password was compromised and to reduce the possibility of tracing. However, the process accounting log shows no trace of any such activity.

Hence, the second possibility is more likely. Our three heros log into 'dal2' to check the telnetd and login binaries. While checking 'dal2', HMK find a few things that do not agree with the explanation from KAIST. Although the message from KAIST said that there was nothing suspicious in 'dal2', HMK find that '/bin/login' was changed at 11:24am, Apr 9, all syslog files `(/var/log/syslog,0,1,2,3...)` were modified at 15:36pm, Apr 9, and the process accounting log, *i.e.* pacct, was stopped from 15:44pm, Apr 9. See the file listing shown in Figure . Apr 9. was the very day when the KUS and the computer center manager checked 'dal2'. Why did they stop logging and why was the log modified? And who did it?

```
% ftp -i dal2.kaist.ac.kr
Name (dal2.kaist.ac.kr:user): user
Password:
ftp> cd /var/log
ftp> dir
-rw-rw-r--  1 root     staff           0 Apr  9 17:45 authlog
-rw-r--r--  1 root     staff       58165 Apr 11 01:36 syslog
-rw-r--r--  1 root     staff      161837 Apr  9 15:36 syslog.0
-rw-r--r--  1 root     staff      359596 Apr  9 15:36 syslog.1
-rw-r--r--  1 root     staff      120791 Apr  9 15:36 syslog.2
-rw-r--r--  1 root     staff       35853 Apr  9 15:36 syslog.3
-rw-r--r--  1 root     staff        7078 Apr  9 15:36 syslog.4
-rw-r--r--  1 root     staff        5929 Apr  9 15:36 syslog.5
ftp> dir /bin/login
-rwsr-xr-x  1 root     staff       24576 Apr  9 11:24 login
```

Figure 2: Modified syslogs and /bin/login at Apr. 9th.

While HMK are taking a coffee break, the manager of POSB approaches them. He angrily shouts at them, “The cracker is ‘chester’ at KAIST! We found a log entry that he connected to POSB from ‘baikdu.kaist.ac.kr’ at the time of the cracking, and he made an account at POSB which has SYSOP privilege. The log entry was found after checking 1500 users one by one. Also, the log was left only because one of POSB managers shutdown the machine while the removal of all files was happening.” At this time, HMK cannot believe that the bad guy is ‘chester’, because he is the leader of the KAIST security team KUS, is a very active person in security field, and is one of the major technical support people for assisting CERT-KR (Korea Computer Emergency Response Team). He often was assigned to check machines which have been cracked and reported to CERT-KR. He also setup the security for several government systems.

Fri. Apr. 12th, 1996

In the morning, the professor supervising POSB contacts the POSTECH computer center, to ask how to report this incident to the police. He says that the cracker is ‘chester’ from ‘baikdu.kaist.ac.kr’. However the the computer center person responsible does not believe that the cracker is ‘chester’, and complains to the professor that the machines were hacked because those systems had not been properly protected by the security tools developed and provided by PLUS (POSTECH Laboratory for Unix Security, POSTECH Security Team). Additionally, the same staff member sends an e-mail message to ‘chester’, asking him for the log files of ‘baikdu’, since ‘baikdu’ is managed by KUS members, and ‘chester’ is the leader of KUS. HMK suspect that those logs, like the ones from ‘dal2’, will not be forthcoming.

At this time, HMK are worried that all relevant log files will be deleted by the cracker. If so, tracking the cracker will finish at a dead end. Moreover, HMK are worried that tracking the cracker who attacked the commercial systems will be similarly compromised. This worry creates a sense of urgency.

The logs of ‘baikdu’ should be kept, to find the cracker. After discussing this matter, HMK finally decide to contact the CIC (Computer Crime Investigation Center) at the Seoul District Prosecutor’s Office.

HMK hope that the investigators from the CIC will go to KAIST and save the log files of ‘baikdu’. Instead, the investigators call to inform HMK that they will come to POSTECH early in the morning to investigate the damage POSTECH sustained, and to determine what information HMK have.

Sat. Apr. 13th, 1996

System managers of the EE and Physics departments describe to the prosectorial investigators the damage they suffered due to the cracking incident. The POSB manager explains why he thinks the cracker is ‘chester’. HMK explain what they know about ‘dal2’. After finishing the hearing, the investigators tell HMK that a few detectives are now in KAIST. From now, the difficult investigation begins.

The investigators plan to interrogate the suspect and related people. The investigators arranged to meet them at KAIST. The suspect denies everything, and gives a long, complex alibi for his whereabouts at the time of the incident. Others say that ‘chester’ is not a person who would do such dirty cracking and destruction of data.

The remainder of Apr., 1996

The investigators are facing many difficulties. At first, they copy the log files of ‘dal2’, ‘baikdu’, etc. and check them. However, they fail to find anything related to this cracking incident. For further investigation, they confiscate the system ‘baikdu’. While investigating it, they find that the log files and user directories of ‘baikdu’ were completely deleted just a few minutes before the seizure. Nothing is left on the system which will provide any definitive clues to what happened.

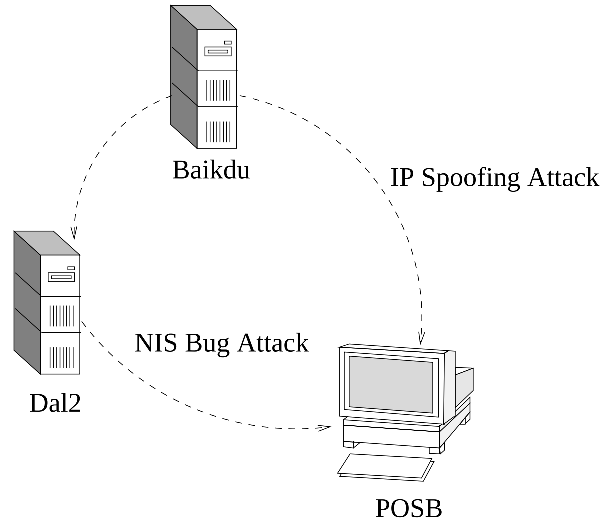

Figure 3: Attacking POSB by the NIS bug and IP spoofing.

Next, they confiscate the backup tapes of 'dal2' and 'baikdu", and several other machines which were frequently used by the suspect. They continue to investigate the suspect, his friends and the confiscated systems.

Mon. May 7th, 1996

Finally, 'chester' confesses his guilt after his alibi is broken by the prosectorial investigation. He and his friend worked together to crack the POSTECH machines using the ypupdated bug of NIS (Network Information System) and IP spoofing. With the two pronged attack, they could get into the POSB machine as shown in Figure 3.

Four persons are arrested. 'Chester' and one of his friends, who deleted the log files and user directories on 'baikdu' while the investigators were confiscating the system, are arrested and held in jail, and two friends who lied to provide the alibi are arrested without detention.

Wed. May 8th, 1996

Every domestic TV news program broadcasts stories about the cracking incident, investigation, and arrests. Also, many newspapers publish novel-like articles, with unknown sources of information. Among them, a few articles are published under the following headlines.

"The security guard hacked a number of machines,"
Choongang Daily Newspaper, May 8th, 1996.

"The end of the hacking war between POSTECH and KAIST,"

Weekly Chosun, May 23rd, 1996.

(This referred to a vernacular novel published last year, describing a "hacking war" between the two universities.)

"286 prosecutors, 586 hackers,"

Hankyure 21, May 23rd, 1996.

(This article glorified the technical prowess of the crackers, and severely criticized the prosecutors abilities. HMK can find little factual information in this article, and consider it a complete work of fiction.)

"Traditional watermelon raid and computer hacking,"

Electronic Newspaper, June 3rd, 1996.

(A "watermelon raid" is in reference to a typical Korean children's prank, which is not to be taken seriously by adults. The slant of this article is that such kind of cracking is definitely a crime and differs from playing.)

Epilog

During the investigation, and after the public announcement of this incident, some people thought that POSTECH people reported this incident to the CIC because the cracker came from POSTECH's rival school, KAIST. Some, including some of the newspapers listed above, complained that the investigation was a "Witch Hunt." However, after the results were fully known, many people were surprised to learn that the cracker was a person who had been believed by everyone, and placed in a position of great trust.

In fact, until now in Korea, most reported computer crimes have been done by employees of financial institutions for their own profit. This kind of cracking incident, data-destructive and through the internet, has been considered to be a highly technical crime with hard to catch criminals, even though such incidents have happened frequently.

This incident has initiated many social and practical changes in domestic security awareness. Many started to think about computer crime and cracking. In many universities, there are new plans to teach incoming students that cracking is a crime. Some universities intend to modify their student's code of conduct to include information related to computer crime. Firewalls and other security tools are receiving heightened attention from academia and industry.

After this incident, POSTECH improved its security by enforcing a policy that each host install the security tools developed by their security team PLUS, adding screening and filtering to the external routers, and increasing logging levels for incoming connections.

The router is programmed to disallow source routing and to drop external packets with a POSTECH source address.

The most definite evidence against ‘chester’ was found in the backup tapes. Even though his friend removed much of the online incriminating data, some useful historical information was found from the backups. This demonstrates, once again, that proper, periodic backups are the most important security tool, not only for data integrity, but also for forensic system and intruder analysis.