

Computer Systems Security Incidents at JPL (1997)

Joseph S. Sherif, R. Brent Mead, and Tom G. Dearmond

**The Jet Propulsion Laboratory, California Institute of Technology
Pasadena, CA. 91109**

and

California State University Fullerton, Fullerton, CA. 92634

Abstract

This paper puts forward an analysis of security incidents at JPL Computer Systems for the year 1997. The analysis includes computer systems affected, date and origin of incident, vulnerability type and previous incident dates. The paper also gives the cost of search, correction and lost time due to these incidents.

Introduction

Every organization, business, or government establishment should assume that it will be the target of an intruder of some kind and as many barriers as possible should be implemented to thwart intrusions. As companies connect to the Internet, and allow some of its employees to work at home with dial-up access privileges, the threat of unauthorized intrusion will increase. Security problems on the network arise due to the following: (1) Resources and workload is shared between networks, (2) Interconnected networks may have different operating systems and security standards, (3) Rigor of authentication may differ between various networks, and (4) Fast expansion of network systems makes access monitoring and protection more difficult and costly.

Information Security and Hacking

The main components of information security are: (1) confidentiality- The data should not be made available or disclosed to persons who are not authorized to have access to it, (2) Integrity- the data once accessed must not be modified, altered or destroyed in any unauthorized manner, and (3) Availability- computer systems assets must be accessible, present and attainable and immediately capable of use for a purpose by persons authorized to access it.

Attacks on computer systems may include the following: (1) Interruption- this is an attack on availability such as the disabling of the file management system, (2) Interception- this is an attack on confidentiality such as illegal copying of files or programs, (3) Modification- this is an attack on integrity such as changing values in a

data file, and (4) Fabrication- this is an attack on authenticity such as the addition of records to a file or the insertion of fake messages in a network.

Hackers describe transgressors who roam the electronic corners of cyberspace exploring its frontiers and disregarding no trespassing signs. Although hacker was originally intended as a compliment meaning a highly skilled computer user, recently it has come to mean unscrupulous computer users who wreak havoc on networks and databases.

Vulnerability of Computer Systems

Most conventional computer operating systems do not have rigorous security requirements. This is due to the high cost of implementing ideal and comprehensive security measures especially when specific security needs are not fully specified by users.

Vulnerabilities are weaknesses in the security systems, which if exploited will cause damage, harm (loss of secrecy, integrity and availability) and loss of productive time. Vulnerabilities of computing systems may include: (1) Hardware (accidental or intentional damage), (2) Software (utility programs, application programs, the operating system) modified, destroyed, deleted, replaced, or copied, and (3) Communication links between hosts.

Major and minor vulnerabilities at JPL Computer Systems were identified in the year 1997. There were at least twenty computer security incidents recorded, searched, identified and corrected (vulnerability fixed). Table 1 shows these incidents at the JPL Computer Systems, classified by date of incident, operating system involved, origin of incident, vulnerability identified and previous incident dates. Table 2 identifies the vulnerability types identified at JPL, and Table 3 shows the vulnerability types, their level of risk, and the corrective actions to be taken for each vulnerability. Table 4 shows the total computer systems incident cost which is the sum of the cost of search and identification of the incident by the Network and Computer Security Group, and the cost of lost time and correction time (fixing the vulnerability) by the section involved with the incident.

Analysis

Computer systems incidents at JPL did cause harm and loss of productive time valued at about half a million dollars. Damage to software was almost minimal since most of the operating systems, utility programs, application programs and data were not seriously tampered with. Also the systems that were affected were not high risk systems or contained sensitive information. The vulnerabilities that were exposed by hackers with their percentage of occurrence are shown in Table 5. It can be seen that the vulnerabilities that were exposed the most are number 11- The Phone File (PHF) program in the Common Gateway Interface Cgi-bin directory; and number 12- Acquiring a password during legitimate use of a valid account by a password sniffer running on a

remote system. Also the percentage of incidents originating from various countries is shown in Table 6. Most hacking originated from the USA, then Canada, and Sweden. The site with the most persistent hacking is T10O11P4. TELIA .com, an Internet Service Provider (ISP) that is also known as a hacker problem site located in Forsta, Sweden. Usually the intruder uploaded the Internet Relay Chat (IRC) software Robot Eggdrop, which enables real-time chat connections to other systems that are also running Eggdrop.

Conclusion

Computer systems and network security has become of vital importance due to the increased growth of computer systems and their connectivity to the Internet. This has prompted management information systems personnel to increase awareness to protect data and resources from disclosure, to ensure the authenticity of data and messages and to safeguard these systems from Network based attacks.

Vulnerabilities are threats to computer systems and networks and include the following: wiretapping, violations of confidentiality and integrity of communications, code integrity, and denial of service. This may be due to impersonation of a legitimate user, hacking, lack of security audit, and malicious code threats such as Viruses, Trojan Horses, Worms and Message Flooding. All security incidents detected at JPL were identified and corrected.

Acknowledgments

This work was carried out by the Jet Propulsion Laboratory, California Institute of Technology under contract with the National Aeronautics and Space Administration (NASA). The authors would like to thank Ron Holland, Michael Flores, David Gilliam and Behshad Sedighi for their help and interest in this work.

Bibliography

1. Harasim, L. (Editor) Global Networks, The MIT Press, Mass., 1994
2. Internet Security Systems (ISS) Publications, 1997
3. JPL Reports (1997)
4. Pfleeger, C.P., Security in Computing, Second Edition, Prentice Hall, NJ. 1997
5. Stallings, W., Network and Internetwork Security, Prentice Hall, NJ. 1995
6. Computer Incident Advisory Capability (CIAC) Publications 1997.

Table 1. Computer systems Incidents at JPL (1997)

| Inc. # | Inc. Date | Systems Affected | Incident Origin | Vulnerability Type | Previous Incident Date |
|--------|-----------|---------------------------------|-----------------|--------------------|-------------------------|
| 1 | 1/10/97 | HP-710, HP-UX 9.03 | USA | 12 | 9/23/96 |
| 2 | 1/21/97 | INDIGO, IRIX 5.03 | AUSTRALIA | 11 | 9/23,24/96 |
| | | | USA | | 11/10,23/96 |
| | | | CANADA | | 12/7,19/96 |
| | | | SWEDEN | | |
| 3 | 2/18/97 | SUN SPARC 20, SOLARIS 2.5.1 | CANADA | 12 | 2/12/97 |
| | | | BRAZIL | | |
| 4 | 3/10/97 | SUN SPARC SERVER/1000 | ITALY | 5 to 11 | |
| | | SOLARIS 2.5 | SWEDEN | | |
| | | SUN ULTRA SPARC, SOLARIS 2.5.1 | GERMANY | | |
| | | SPARC STATION 20, SOLARIS 2.3 | USA | | |
| | | SPARC STATION 20, SOLARIS 2.5 | CANADA | | |
| | | SPARC STATION 20, SOLARIS 2.5.1 | | | |
| | | SUN ULTRA SPARC, SOLARIS 2.5.1 | | | |
| | | SPARC STATION 5, SOLARIS 2.5 | | | |
| | | SUN ULTRA SPARC, SOLARIS 2.5.1 | | | |
| | | SUN ULTRA SPARC, SOLARIS 2.5.1 | | | |
| 5 | 3/28/97 | SUN SPARC SERVER | CANADA | 12 | |
| | | 670 MP, SUN OS 4.1.3 | USA | | |
| 6 | 4/27/97 | SUN SPARC, STATION 2 | USA | 4, 8 to 12 | 02/18,22/97, 4/23,24/97 |
| | | SUN OS 4.1.3 | | | 12/29/96, 10/5,15/96 |
| 7 | 5/29/97 | SUN SPARC 2, SUN OS 4.1.3 | USA | 1 to 4 | |
| | | SUN SPARC IPC | | | |
| | | SUN SPARC 2 | | | |
| | | HP 725 | | | |
| | | SUN SPARC 10 | | | |
| 8 | 6/3/97 | DEC 3000, DIGITAL OSF/1 2.0 | GERMANY, USA | 5,6 | 5/27/97 |
| | | | ISRAEL | | |
| 9 | 7/1/97 | SUN ULTRA SPARC 1, SOLARIS 2.5 | SWEDEN | 12 | |

| | | | | | |
|----|----------|----------------------------------|-------------|----------|----------------|
| 10 | 7/11/97 | GRAY J90, UNICOS | USA | 12 | 6/29/97 |
| 11 | 7/14/97 | SUNSPARC 10, SUN OS 4.1.3 | FINLAND | 5,6,7,9 | 7/2,7,12,13/97 |
| | | | SWEDEN | 11,14,15 | 6/25,30/97 |
| 12 | 8/23/97 | GRAY J90, UNICOS | USA | 12 | |
| 13 | 8/18/97 | SUN SPARC 20, SOLARIS 2.5.1 | USA | 11 | |
| 14 | 8/12/97 | SGI, IRIX 4D, IRIX 4.1.5 | BRAZIL | 11 | |
| 15 | 8/8/97 | SUN SPARC, SOLARIS 2.6 | USA | 11 | |
| 16 | 10/14/97 | SUN ULTRA 2, SOLARIS 2.5 | USA | 11 | |
| 17 | 10/17/97 | SGI, ONYX 6.2, IBM AS400 | USA | 10,14 | |
| 18 | 10/12/97 | STI, IRIX; SUN IPC, SUN OS 4.1.4 | USA | | |
| 19 | 11/13/97 | X.500, SUN SPARC | USA | 13 | |
| 20 | 12/10/97 | SGI, ONYX, IRIX 6.2 | USA, BRAZIL | 5 | |

Table 2. Vulnerability Types Identified at JPL

| Type # | Explanation of Vulnerability Types |
|--------|---|
| 1 | Open System Display(ability to capture users keystrokes) |
| 2 | Send Mail (older version) |
| 3 | Unix to Unix Copy Protocol, UUCP (contains security vulnerability) |
| 4 | Anonymous FTP (Writable directories allow for unauthorized use) |
| 5 | Easily Guessed Password_Logins |
| 6 | Easily Guessed Password_FTP |
| 7 | X-Windows accessible by the world |
| 8 | Host. Equiv. File Open to world access |
| 9 | HTTP (WWW) Server (older version of software) |
| 10 | Remote Shell (Rsh) Open to world access. When the /etc/hosts.equiv.file contains an entry with a+ in it by default. |
| 11 | Phone File (PHF) program in Common Gateway Interface Cgi-bin directory. This vulnerability allows the system password file to be exported to another computer system where the intruder could use the password guessing program "crack" to extract readable passwords. |
| 12 | Acquiring a password during legitimate use of a valid account by a password sniffer running on a remote system. |
| 13 | Forged E-Mail: Previous employee knowledge of JPL mail systems, address structure, and mail list format. |
| 14 | Open Default Accounts (found through Telnet) |
| 15 | finger, Finger Bomb (gives intruder information such as login accounts and trusted hosts) Finger Bomb allows redirecting the finger to remote sites while covering their tracks. |

Table 3. Vulnerability, Risk Level and Corrective Actions

| Vulnerability Type | Risk | Corrective Actions |
|--------------------------------------|--------|--|
| Open System Display | High | Make your system access protected. |
| Send Mail | Low | Do not set your X server to xhost+ Upgrade |
| UUCP | Medium | Hosts that do not need to allow access should disable it by placing a # at the beginning of the UUCP Line in the file/etc/inetd. Conf and then sending the SIGHUP signal to the inetd process to restart the process |
| Anonymous FTP | Low | If an anonymous login is permitted, the scanner attempts to copy/etc/password. If the FTP server is chrooted, etc/password is not available. |
| Easily guessed passwords- login, FTP | Low | Use stricter password construction. Use TCP wrapper software. use onetime password mechanism |
| Host. Equiv. File open access | High | Use TCP wrappers |
| Rsh open access | High | Remove the + from Hosts.equiv |
| PHF program in Cgi-bin directory | High | Remove the PHF program from the /Cgi-bin |
| Acquiring a password by a sniffer | High | Encrypt login session. Use a one-time password mechanism |
| Forged E-mail | Medium | Correct TCP sequence prediction |
| Open Default Accounts | High | Use TCP wrappers, disable accounts by placing * in the password field and the string/bin/false in the shell field in the /etc/password. |
| Finger Bomb | Medium | Disable Fingered. Configure Firewalls properly. Use Finger daemons for disabling redirections. |

Table 4. Total (Penetration) Incident Cost (Search, lost time and Correction)

| Penetration Incident # | Network and Computer Security Group (Search) (\$) | Section Involved with Incident (lost time and correction) (\$) | Total Cost (\$) |
|------------------------|---|--|-----------------|
| 1 | 600 | 200 | 800 |
| 2 | 400 | 200 | 600 |
| 3 | 200 | 800 | 1000 |
| 4 | 7,600 | 376,992 | 384,592 |
| 5 | 1,300 | 750 | 2,150 |
| 6 | 2,000 | 1,200 | 3,200 |
| 7 | 1,200 | 600 | 1,800 |
| 8 | 2,800 | 2,275 | 5,075 |
| 9 | 1,600 | 0 | 1,600 |
| 10 | 450 | 150 | 600 |
| 11 | 2,500 | 400 | 2,900 |
| 12 | 600 | 0 | 600 |
| 13 | 100 | 0 | 100 |
| 14 | 500 | 0 | 500 |
| 15 | 250 | 0 | 250 |
| 16 | 2,000 | 400 | 2,400 |
| 17 | 2,400 | 0 | 2,400 |
| 18 | 450 | 0 | 450 |
| 19 | 0 | 0 | 0 |
| 20 | 2,000 | 0 | 2,000 |

Table 5. Percentage of Vulnerabilities Occurrence by Type at JPL (1997)

| VulnerabilityType | Occurrence (%) |
|-------------------|----------------|
| 1 | 2.3 |
| 2 | 2.3 |
| 3 | 2.3 |
| 4 | 4.5 |
| 5 | 9.0 |
| 6 | 7.0 |
| 7 | 4.5 |
| 8 | 4.5 |
| 9 | 7.0 |
| 10 | 7.0 |
| 11 | 20.0 |
| 12 | 18.0 |
| 13 | 2.3 |
| 14 | 7.0 |
| 15 | 2.3 |
| | 100.00 |

Table 6. Percentage of Incidents Originating from Various Countries

| Country | Occurrence (%) |
|-----------|----------------|
| USA | 50.0 |
| Canada | 13.0 |
| Sweden | 10.0 |
| Germany | 6.7 |
| Brazil | 6.7 |
| Australia | 3.4 |
| Finland | 3.4 |
| Italy | 3.4 |
| Israel | 3.4 |

100