UNIT 6 TECHNOLOGICAL VULNERABILITIES

Structure

6.1 Introduction

6.2 Objectives

6.3 Computer Hacking

6.4 Intrusion Techniques

6.5 Vulnerabilities and Exploitation of Vulnerabilities

6.6 Controls against Malicious Software

6.7 Latest Update on Technological Vulnerabilities

6.8 Definition of Common Attacks and Vulnerabilities

6.9 Summary

6.10 Terminal Questions

6.11 Answers and Hints

6.12 References and Suggested Readings

6.1 INTRODUCTION

Individuals and organizations across the world are increasingly using computers, Internet and computer networks (collectively hereinafter referred to as "Information Systems") in almost all spheres of life from personal use to launch of spacecrafts. This dependence on Information Systems has made them critical to the very survival of business, economy and infrastructure of the world. As the criticality of Information Systems increases so do the vulnerabilities that increasingly face them. Some vulnerabilities are due to human interference and some others are due to obsolete technology or the usual wear and tear during usage. This paper aims to provide a basic understanding of some of the more critical technological vulnerabilities that Information Systems may face today. The paper also explores some basic concepts of ensuring that Information Systems are protected from these technological vulnerabilities.

6.2 OBJECTIVES

After studying this unit you should be able to:

- describe technological vulnerabilities of Information Systems;
- know the concept of hacking;
- describe effective security measures that may be implemented to prevent exploitation of the vulnerabilities of Information Systems;
- know the latest update on technological vulnerabilities; and
- give definitions of common attacks and vulnerabilities.

6.3 COMPUTER HACKING

In order to understand the technological vulnerabilities of the Information Systems it is first imperative to understand the information security sphere. Hackers make use of the vulnerabilities and gain access to Information Systems. Computer hacking is also referred to technically as "intrusion" which may be defined as an attempt to break into or misuse a computer system. Misuse of the computer system may be a simple act of sending prank messages from the user's e-mail system to a potentially damaging act of stealing confidential information from the user. Computer hackers are also of many ranges and types; some hack for intellectual highs while other hack for money. There is no absolute or foolproof method to prevent hacking or safeguard your computer system against hacking. However IT professionals need to be aware of the range and risk of hacking and should take reasonable precautions to safeguard their computer systems.

6.4 INTRUSION TECHNIQUES

The following are some of the most prevalent ways by which hacker can get into a computer system:

Physical Intrusion: This is the most basic of the techniques- and most often the most overlooked in information security procedures adopted by IT professionals. If the hacker has physical access such as access to the console or the keyboard then it is very simple for him or her to get into the machine and take the machine apart. The disk may be removed and read/ write on another machine. Data can be transferred from the machine to a disk or another machine. With the advent of blue tooth and wireless communication, intrusion has become easier.

System Intrusion: This is common where the hacker has access to the system as a low privilege user on the computer system and uses his low privilege account to gain additional administrative privileges. In this scenario the hacker uses security loopholes if the computer system does not have the latest security patches.

Remote Intrusion: Here, the hacker has no physical or user access to the computer system and attempts to hack the computer system remotely across the network. The network may be an internal company intranet or through the Internet.

6.5 VULNERABILITIES AND EXPLOITATION OF VULNERABILITIES

Hackers do not magically get into the computer system or information systems, they exploit the technological vulnerabilities present in a computer system, information system or networks and then gain access to the computer system. The following paragraphs attempt to provide a brief understanding of the various technological vulnerabilities:

Software bugs are one of the most important ways, which the hackers exploit to gain access into the computer systems. Software bugs can be broadly classified into buffer overflows, unexpected combinations and race conditions. A typical example is a programmer who sets aside 256 characters to hold a login username. However, if an attacker tries to enter in a false username longer than the actual you might have a problem. All the attacker has to do is send 300 characters, including code that will be executed by the server, and thus gain access. Hackers find these bugs in several ways. First, the source code for a lot of services is available on the net. Hackers routinely

look through this code searching for programs that have buffer overflow problems. Secondly, hackers may look at the programs themselves to see if such a problem exists. Thirdly, hackers will examine every place the program has input and try to overflow it with random data. If the program crashes, there is a good chance that carefully constructed input will allow the attacker to gain access[1]. Unexpected combinations are scenarios where hackers send input that is meaningless to one layer, but meaningful to another layer. The program is usually constructed using many layers of code and therefore by trial and error method the hacker talks to one of the layers of the software and setting off a chain reaction in other layers, which provides him with the access. Race conditions are scenarios where one program accesses data and the same data is accessed by another program being run by another person which enables the person to access the data. Race conditions work because most computers are designed to handle more than one program at a time. In yet another kind of intrusion, the hacker just feeds random inputs into the system hoping to elicit a response from the system and at times this works.[2]

System configuration bugs are security holes, which develop in the system due to the way the system has been configured for use usually by the administrator. Default configurations (configurations in which the system is shipped to the customer) in a system is the most vulnerable and can be hacked in easily. If the administrator fails to set up a root/administrator password in a system it becomes easy for the hacker to gain access. Also in systems, which have been interconnected with a pool of other systems, then the security loopholes in one unsecure system can be used to hop to other systems in the pool, thereby endangering the entire network.

Internet Browsers and Operating Systems also have security holes, which are regularly exploited by hackers to install bugs, viruses and trojans or for them to be downloaded through various infected sources. This includes URL, HTTP, HTML, and JavaScript, Frames, Java and ActiveX attacks. Regular patches are available which need to be used in order to plug these loopholes. The section at the end of this paper provides a list of the most active vulnerabilities, which may be used as a reference. By sending illegal or strange ICMP or TCP packets, a hacker can identify the OS on the target system. Standards usually state how machines should respond to legal packets but omit to instruct the machine how to respond to invalid inputs. Therefore each reply to an invalid input can be used by the hacker to determine and identify the system OS and plan the attack.

Password Access is the key to any computer system or in fact networks. Therefore control over password access is perhaps most crucial in ensuring information security and also easiest for the hacker to exploit as a vulnerability. The first major flaw in password access is weak or easy to guess passwords. These passwords are where people use names of pets, loved ones, nick names as passwords thereby enabling the hacker to guess the password easily. Too many passwords are easily guessed, especially if the hacker knows something about their target's background. It's not unusual, for example, for office workers to use the word "password" to enter their office networks. Other commonly used passwords are the computer user's first, last or child's name, secret, names of sports teams or sports terms, and repeated characters such as AAAAAA or bbbbbb[3]. Another method of intrusion exploiting the computer system is 'dictionary attack' on the system. The hacker will use a program, which will try every possible word in the dictionary. Similar to the dictionary attack is the 'brute force' attack where the hacker tries combinations of the password characters in order to break in. A simple five-letter password using English characters may be easy to break

in. Sniffing programs on servers or switched networks may prove to be effective in tapping into the users password when he/she logs onto the system. There are other sophisticated methods of gaining password control such as encrypted sniffing and replay attack.

Another interesting mechanism used to gain access to passwords is through *Social Engineering.* 'Social engineering' is hackerspeak for conning legitimate computer users into providing useful information that helps the hacker gain unauthorized access to their computer system[4]. Some of the more common social engineering scenarios are[5]:

1. The attacker pretends to be a legitimate end-user who is new to the system or is simply not very good with computers. The attacker may call systems administrators or other end-users for help. This "user" may have lost his password, or simply can't get logged into the system and needs to access the system urgently. The attacker may sound really lost so as to make the systems administrator feel that he is, for example, helping a damsel in distress. This often makes people go way out of their way to help.
2. The attacker pretends to be a VIP in the company, screaming at administrators to get what he wants. In such cases, the administrator (or it could be an end-user) may feel threatened by the caller's authority and give in to the demands.
3. The attacker takes advantage of a system problem that has come to his attention, such as a recently publicized security vulnerability in new software. The attacker gains the user's trust by posing as a system administrator or maintenance technician offering help. Most computer users are under the mistaken impression that it is okay to reveal their password to computer technicians.
4. The attacker posing as a system administrator or maintenance technician can sometimes persuade a computer user to type in computer commands that the user does not understand. Such commands may damage the system or create a hole in the security system that allows the attacker to enter the system at a later time.

Insecure modems are another gateway for a hacker to gain access to a computer system. War dialers are used by hackers to identify the modems of a target. A war-dialer is a computer program that automatically dials phone numbers within a specified range of numbers and chances are that if an organization has one number, it will have a few other numbers in same range for all telecommunications. By dialing all numbers within the targeted range, the war-dialer identifies which numbers are for computer modems and determines certain characteristics of those modems. The hacker then uses other tools to attack the modem to gain access to the computer network. Effective war-dialers can be downloaded from the Internet at no cost. The problem is that a modem is a means of bypassing the "firewall" that protects your network from outside intruders. A hacker using a "war-dialer" to identify the modem telephone number and a password cracker to break one weak password can gain access to the system. Due to the nature of computer networking, once a hacker connects to that one computer, the hacker can often connect to just about any other computer in the network[6]. Of course it is now possible to incorporate safeguards to prevent easy access through modems, which is beyond the scope of this paper.

Cookies are another security threat that the user of a computer system faces. A cookie is a small program that may be placed on a computer. The cookie enables the site that has deposited the cookie to recognise when the user visits it the next time. It maintains a database of the users visits to the site and also in some instances other websites. Cookies raise substantial privacy issues, which are again beyond the scope of this

paper. Suffice to say that cookies do raise issues of profiling of individuals, illegal tracking on the Internet etc. Cookies per se do not damage or hack the system but are often used by hackers to gain information on a target and his/her Internet surfing habits prior to hacking. It is possible to ensure that the user's computer systems do not accept cookies from any site and settings on the system and special software installation will achieve this goal.

Denial of Service attacks are another variety of system compromises which are designed to overload network links, the processing unit of the user system or the disk of the system thereby crashing the service. The hacker aims to make the computer system deny providing services to the user. The increased degree of automation in the recent years has enabled a single hacker to control thousands of compromised systems for use in the attacks. A simple example may be to flood the user's (in most case an entire organization's) mail inbox with a host of messages thereby making the server to crash.

In the recent past attacks on Internet Domain Name System (DNS) is on the rise. The hacker may create a bogus DNS resembling a legitimate Internet site. Therefore information intended for the legitimate site may flow into the hacker's site. In some other cases hackers compromise poorly protected DNS servers which give them the ability to modify the data passing through the server. By leveraging insecure mechanisms used by customers to update their domain registration information, attackers can co-opt the domain registration processes to take control of legitimate domains[7]. Another issue which has cropped up recently is web spoofing which is a kind of electronic con game in which the attacker creates a convincing but false copy of the entire World Wide Web. The false Web looks just like the real one: it has all the same pages and links. However, the attacker controls the false Web, so that all network traffic between the victim's browser and the Web goes through the attacker. The key to this attack is for the attacker's Web server to sit between the victim and the rest of the Web. This kind of arrangement is called a 'man in the middle attack' in the security literature. Since the attacker can observe or modify any data going from the victim to Web servers, as well as controlling all return traffic from Web servers to the victim, the attacker has many possibilities. These include surveillance and tampering[8].

Attacks against routers are another vulnerability that may be exploited by hackers to crash information systems. Intruders use poorly secured routers as platforms for generating attack traffic at other sites, or for scanning or reconnaissance. Further, routers are designed to pass large amounts of traffic through them; they often are not capable of handling the same amount of traffic directed at them. Intruders take advantage of this characteristic attacking the routers that lead into a network rather than attacking the systems on the network directly. Another method of intrusion into routers is to exploit the trust relationships that the routers have. For routers to do their job, they have to know where to send the traffic they receive. They do this by sharing routing information between them, which requires the routers to trust the information they receive from their peers. As a result, it would be relatively easy for an attacker to modify, delete, or inject routes into the global Internet routing tables to redirect traffic destined for one network to another, effectively causing a denial of service to both (one because no traffic is being routed to them, and the other because they're getting more traffic than they should). Although the technology has been widely available for some time, many networks (Internet service providers and large corporations) do not protect themselves with the strong encryption and authentication features available on the routers[9].

Viruses and Trojans are possibly the most damaging vulnerabilities that a computer system may face today. Viruses and trojans have the ability to damage computer systems to a great extent. A virus is a small, self-contained piece of computer code hidden within another computer program. Like a real virus, it can reproduce, infect other computers, and then lie dormant for months or years before it strikes. A virus is only one of several types of 'malicious logic' that can harm your computer or your entire network. Worms, logic bombs, and trojan Horses are similar 'infections' commonly grouped with computer viruses. A computer worm spreads like a virus but is an independent program rather than hidden inside another program. A logic bomb is a program normally hidden deep in the main computer and set to activate at some point in the future, destroying data. A trojan horse masquerades as a legitimate software program. It waits until triggered by some pre-set event or date and then delivers a payload that may include destroying files or disks[10]. Through Trojans on the user's systems a remote hacker can control the activities of the user's computer whenever the user is on the Internet. When you interact with another computer, the virus may automatically reproduce itself in the other computer. Once a virus infects a single networked computer, the average time required to infect another workstation in the same network is from 10 to 20 minutes — meaning a virus can paralyse an entire organization in a few hours[11]. Since viruses and Trojans have such a huge potential adverse impact on an organization's security, the following paragraphs have been included to provide a brief overview of the possible controls that an organization should adopt to counter viruses and Trojans.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are some of the most common techniques adopted by hackers to exploit to vulnerabilities in Information System?

.....

.....

.....

.....

.....

.....

6.6 CONTROLS AGAINST MALICIOUS SOFTWARE

The detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented. The protection against malicious software should be based on security awareness, appropriate system access and change management controls. To protect the integrity of information and the information systems from modifications, disclosures or destruction by malicious software, the following steps should be taken:

1. To establish a virus detection and protection procedure, to be continuously reviewed and revised, conforming to the emerging requirements and to implement the same across the organization.

2. All software acquired by the organization should be checked by the virus detection procedure prior to installation and use.
3. To establish the management procedures and responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks.
4. To distribute instructions on the detection of viruses to all the users.
5. Evidence such as sluggish performance or mysterious growth of files should alert the users to a problem that must be reported to the information system security manager immediately on occurrence thereof.
6. To establish a written policy on downloading, acceptance and use of freeware and shareware including the flexibility to prohibit this practice, if deemed necessary.
7. To establish a formal policy requiring compliance with software licences and prohibiting the use of unauthorized software.
8. To authenticate software for highly critical applications using digital signature. Failure to verify would indicate potential problem/problems and the software should not be used until the source of the problem is identified and properly dealt with.
9. To establish a formal policy to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken.
10. To install and regularly update the anti-virus detection and repair software to scan computers and media, either as a precautionary control or on a routine basis.
11. To conduct regular reviews of the software and data content of systems supporting critical business processes. The presence of any unapproved files or unauthorized amendments should be formally investigated.
12. To establish a policy and procedure for checking the diskettes and other such media, brought in from outside the organization's normal purchasing programme. To check any files on electronic media of uncertain or unauthorized origin or files received over untrusted networks for viruses before use.
13. To check any electronic mail attachments and downloads for malicious software before use. This check may be carried out at different places e.g. at electronic mail servers, desktop computers or when entering the network of the organization.
14. To establish appropriate business continuity plans for recovering from virus attacks, including all necessary data and software backup and recovery arrangements.
15. To establish procedures to verify all information relating to malicious software and ensure that warning bulletins are accurate and informative. The Information Systems Security Managers should ensure that qualified sources, e.g. reputed journals, reliable Internet sites or anti-virus software suppliers are used to differentiate between hoaxes and real viruses. The users of the information systems should be made aware of the problem of hoaxes and the action to be taken on receipt thereof.

To ensure recovery of the processing capabilities following a virus infection, the following steps should be taken:

1. To retain the original back-up copy of all software and hold the same until such time as the original software is no longer in use; and
2. All data is backed up regularly.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 4 Min.*

Can Information Systems be protected against malacius software? What control measures may be adopted?

.....

.....

.....

.....

.....

.....

.....

.....

6.7 LATEST UPDATE ON TECHNOLOGICAL VULNERABILITIES

Four years ago, the SANS Institute and the National Infrastructure Protection Center (NIPC) at the FBI released a document summarizing the Ten Most Critical Internet Security Vulnerabilities. The latest list of SANS Top-20 2005 has been released and contains in addition to Windows and UNIX categories, Cross-Platform Applications and Networking Products. The list indicates critical vulnerabilities in the past year and a half and can be an effective tool to check preparedness of Information Systems against technological vulnerabilities[12].

6.8 DEFINITION OF COMMON ATTACKS AND VULNERABILITIES

Backdoor: A change made to a violated system to make future re-entry easier for the hacker.

Bacteria: A program that quickly allocates system resources and reproduces instances of itself to deny service to other processes (also known as hogs).

Buffer overrun: An attack that forces a processor to execute foreign code in privileged mode by passing a lengthy string parameter containing the code to a subroutine that does not have the buffer space to receive it.

Compromised system utilities: Common system commands or programs altered by a hacker so that the systems extend unintended privileges to unauthorized users, provide a backdoor for later re-entry, or fail to report hacker activities.

DNS hijack: An attack that alters the Domain Name System (DNS) so that a DNS lookup for a computer name returns an unintended IP address.

E-mail forgery: An attack that constructs e-mail messages to appear as if originating from another person or source.

E-mail relay: An attack that bounces messages into spam-filtering mail system through an unsuspecting, third-party mail system that is not on the filtering list.

IP spoofing: A form of masquerading in which the sender of an Internet data packet forges the originating IP address so that the packet appears to have been sent by another system.

Keystroke monitoring: Using a hardware or software mechanism to capture user keyboard strokes and report the strokes to a hacker.

Logic bomb: Clandestine code triggered by a certain set of conditions, such as a particular date or a combination of inputs.

Mail bombing: Overloading an e-mail system by sending large volumes of messages (also known as e-mail flooding).

Masquerading: Posing as an authorized entity.

Networking scanning: Using standard network protocols to determine topology and service access points of a target network.

Packet sniffing: Copying data in transit on a network link, usually with a network transceiver in 'promiscuous mode'.

Password cracking: Trying words from a dictionary to ascertain a user password.

Ping flooding: Sending a large number of Internet Control Message Protocol (ICMP) 'echo' requests to target system, causing it to divert significant resources to handling them.

Reply attack: An attack in which network transmissions, usually authentication sequences such as user login information, are recorded (see packet sniffing) and later re-sent by a masquerader.

Script kiddies: Inexperienced hackers who use prepackages software to conduct attack against well-known vulnerabilities.

Security audit tools: Software tools that probe systems to discover vulnerabilities so that attackers can quickly identify easy targets (also used as a defense).

Shell escapes: User input, usually to a web-based forms processor supported by a Common Gateway Interface (CGI) scripting utility, that contains OS commands to be executed unintentionally by a command interpreter.

Shoulder surfing: Acquiring data by observing user interaction with computer I/O devices, such as monitors or touch screens (often accomplished using magnification devices from a distance).

Smurfing: Combination of IP spoofing and ping flooding in which ICMP echo requests and the target subnet address are sent to a group of unsuspecting accomplice systems, which then generate replies to broadcast addresses to the target sub network.

Social engineering: Using human relationship and interactions to obtain unauthorized access or confidential information.

SYN flooding: Beginning Transmission Control Protocol (TCP) sessions with a target system by sending initial synchronization requests but not acknowledging responses, causing the number of open connections on the target system to increase and consume resources.

Traffic analysis: Observation of network traffic patterns to deduce confidential information, such as communication habits and frequency (also used as a defense).

Trapdoor: Undocumented program behaviour triggered by a secret input sequence to give a perpetrator special privileges.

Trojan horse: A software program that is advertised to fulfill a useful function but is actually malicious.

Van Eck attack: The use of sophisticated reception equipment to capture and decode electromagnetic signals from computer output devices at a distance.

Virus: Code fragment inserted into a legitimate program (a process called infection) to steal processor cycles during which new programs are found and infected.

War dialing: Automated dialing of every telephone number on a common exchange for the purpose of finding numbers that are connected to computer systems.

Worm: A self-replicating program or virus that uses network connections to propagate to new systems.

Let us now summarize the points covered in this unit.

6.9 SUMMARY

- Hacking is a serious problem and a consistent one for which no permanent solution has been derived.
- Back ups are an essential and integral process of securing information.
- The most prevalent ways by which a hacker can get into a computer system are physical intrusion, system intrusion and remote intrusion:
- Software bugs, system configuration bugs, Internet browsers and operating Systems, password access, Insecure modems, cookies, Denial of service, Attacks on Internet Domain Name System, Attacks against routers, Viruses and trojans are some of vulnerabilities, that are exploited by hackers.
- software bugs can be classified into buffer overflows, unexpected combination and race conditions.
- *System configuration bugs* are security holes, which develop in the system due the manner in which the system has been configured for use usually by the administrator.
- *Internet Browsers and Operating Systems* also have security holes, which are regularly exploited by hackers to install bugs, viruses and trojans or for them to be downloaded through various infected sources. This includes URL, HTTP, HTML, and JavaScript, Frames, Java and ActiveX attacks.
- *Password Access* is the key to any computer system. The first major flaw in password access is weak or easy to guess passwords.
- Social engineering is also used to gain access to passwords, it is hacker-speak for conning legitimate computer users into providing useful information that helps the hacker gain unauthorized access to their computer system.
- A cookie is a small program that may be placed on a computer.
- A virus is a small, self-contained piece of computer code hidden within another computer program, it can reproduce, infect other computers, and then lie dormant for months or years before it strikes.

- A virus is only one of several types of "malicious logic" that can harm your computer or your entire network. Worms, logic bombs, and trojan horses are similar "infections" commonly grouped with computer viruses.
- The detection and prevention controls to protect against malicious software and appropriate user awareness procedures should be implemented.

6.10 TERMINAL QUESTIONS

1. Explain in simple terms, the concept of hacking and the techniques used for such hacking?
2. What vulnerabilities usually occur in software, computer systems, Internet Browsers and operating systems? Explain in brief.
3. Why is Password Access Control a key vulnerability and in what ways can you improve security of passwords?
4. Define the concept of "Social Engineering" in simple terms?
5. Explain the following security vulnerabilities in brief:
   a. Insecure Modems
   b. Cookies
   c. Man in the Middle Attacks
6. Explain what Malicious Software means and what controls need to be established to protect computer systems against Malicious Software?

6.11 ANSWERS AND HINTS

Self Assessment Questions

1. Hackers and intrusionists use technological vulnerabilities to hack or intrude Information Systems through physical intrusion, system intrusion and remote intrusion techniques.
2. Yes, Information Systems may be prevented from malicious software by undertaking a series of technological security measures, ongoing awareness and system audits.

Terminal Questions

1. Refer to section 6.3 of the unit.
2. Refer to section 6.5 of the unit.
3. Refer to section 6.5 of the unit.
4. Refer to section 6.5 of the unit.
5. Refer to section 6.5 of the unit.
6. Refer to section 6.6 of the unit.

6.12 REFERENCES AND SUGGESTED READINGS

1. Zachary Wilson. "Hacking: The Basics". Giac.org. 4 April. 2001. 4 April. 2006 <http://www.giac.org certified_professionals/practicals/gsec/0608.php>.

2. Ibid.

3. "Computer Vulnerabilities". rf-Web.Tamu.edu 8Mar.2007<http://rf-web.tamu.edu/security SECGUIDE/V1comput/Intra.htm>.

4. Ibid.

5. Erik Guttman, Lorna Forey, & G. Malkin. Users' Security Handbook. Internet Engineering Task Force. July. 1998 draft.

6. Ira Winkler. Corporate Espionage: What it is, why its' Happening in Your Company, What you Must Do About it. Rocklin, CA: Prima Publishing. 1997.

7. Overview of Attack Trends. CERT.org.2002. Carnegie Mellon University, 8Mar.2007< http://www.cert.org/archive/pdf/attack_ trends.pdf>.

8. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. "Web Spoofing: An Internet Con game". Dec. 1996. Technical Report. Department of Computer Science, Princeton University, Feb. 1997: 540-96.

9. Supra n 6.

10. Supra n 1.

11. D. L. Carter & A.J. Katz. "Trends and experiences in computer-related crime: Findings from a national study". Paper presented at the Annual Meeting of the Academy of Criminal Justice Sciences. Las Vegas. NV, 1996.

12. SANS Institute. "The SANS Top 20 Internet Security Vulnerabilities". Sans.org.9Mar.2007<http:/ www.sans.org /top20/#w1>.

13. J. Craig Lowery. "Computer System Security: A Primer". Dell.com. Mar.2002. 9Mar.2007<http:// www1.us.dell.com/content/topics/global.aspx/power/en pslq_lowery?c=us&1=en&s=gen>.