**Class Note 3**

**The Need for Security**

Business need: Information security performs four important functions for an organization:

* Protecting the organization’s ability to function
* Enabling the safe operation of applications running on the organization’s IT systems
* Protecting the data the organization collects and uses
* Safeguarding the organization’s technology assets

**Protecting the organization’s ability to function**: Each of an organization’s communities of interest must address information security in terms of business impact and the cost of business interruption, rather than isolating security as a technical problem.

**Enabling the safe operation of applications running on the organization’s IT systems**:

**Protecting Data that Organizations Collect and Use:** Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. The value of data motivates attackers to steal, sabotage, or corrupt it. An effective information security program implemented by management protects the integrity and value of the organization’s data.

**Safeguarding Technology Assets in Organizations:** To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise. For instance, a small business may get by using an e-mail service provided by an ISP and augmented with a personal encryption tool. When an organization grows, it must develop additional security services. For example, organizational growth could lead to the need for public key infrastructure (PKI), an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

**Threats**

In the context of information security, a **threat** is an object, person, or other entity that presents an ongoing danger to an asset.



**Deliberate Software Attacks**

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or **malicious software**, or sometimes **malware**. Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors.

On Malware – check note on malware

**Espionage or Trespass**

When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass. When foreign governments are involved, these activities are considered espionage and a threat to national security. The classic perpetrator of espionage or trespass is the hacker. **Hackers** are “people who use and create computer software [to] gain access to information illegally.

**Expert hacker**, or **elite hacker**, who develops software scripts and program exploits used by those in the second category, the novice or **unskilled hacker.** The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and exhibits mastery of the technical environment of the chosen targeted system.

A much more sinister form of hacking is **cyberterrorism**. Cyberterrorists hack systems to conduct terrorist activities via network or Internet pathways.

**Information Extortion**

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft.

**Sabotage or Vandalism**

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization.

**Attacks**

It is accomplished by a **threat agent** that damages or steals an organization’s information or physical asset. A **vulnerability** is an identified weakness in a controlled system, where controls are not present or are no longer effective.

Malicious Code: The **malicious code** attack includes the execution of viruses, worms, Trojan horses, and active Web scripts with the intent to destroy or steal information.

Back Doors: Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door. Sometimes these entries are left behind by system designers or maintenance staff, and thus are called trap doors.

Password Crack: Attempting to reverse-calculate a password is often called **cracking**. A cracking attack is a component of many dictionary attacks. It is used when a copy of the Security Account Manager (SAM) data file, which contains hashed representation of the user’s password, can be obtained. A password can be hashed using the same algorithm and compared to the hashed results. If they are the same, the password has been cracked.

Brute Force: The application of computing and network resources to try every possible password combination is called a **brute force attack**. Since the brute force attack is often used to obtain passwords to commonly used accounts, it is sometimes called a **password attack**.

Dictionary: The **dictionary attack** is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations. Organizations can use similar dictionaries to disallow passwords during the reset process and thus guard against easy-to-guess passwords.

**Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS)**: In a denial-of-service (DoS) attack, the attacker sends a large number of connection or information requests to a target (see Figure 2-11). So many requests are made that the target system becomes overloaded and cannot respond to legitimate requests for service. The system may crash or simply become unable to perform ordinary functions.

A **distributed denial of-service (DDoS)** is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time. Most DDoS attacks are preceded by a preparation phase in which many systems, perhaps thousands, are compromised. The compromised machines are turned into **zombies**, machines that are directed remotely (usually by a transmitted command) by the attacker to participate in the attack. To use a popular metaphor, DDoS is considered a weapon of mass destruction on the Internet.36 The MyDoom worm attack of early 2004 was intended to be a DDoS attack against *www.sco.com* (the Web site of a vendor of a UNIX operating system) that lasted from February 1, 2004 until February 12, 2004.

**Spoofing**: Spoofingis a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host. To engage in IP spoofing, hackers use a variety of techniques to obtain trusted IP addresses, and then modify the packet headers to insert these forged addresses. Newer routers and firewall arrangements can offer protection against IP spoofing.

**Man-in-the-Middle**: **TCP hijacking attack**, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network. This type of attack uses IP spoofing to enable an attacker to impersonate another entity on the network. It allows the attacker to eavesdrop as well as to change, delete, reroute, add, forge, or divert data.39 A variant of TCP hijacking, involves the interception of an encryption key exchange, which enables the hacker to act as an invisible man-in-the-middle—that is, an eavesdropper—on encrypted communications.



**Spam**: spamis unsolicited commercial e-mail. It can be used as a means of enhancing malicious code attacks. The most significant consequence of spam, however, is the waste of computer and human resources. Many organizations attempt to cope with the flood of spam by using e-mail filtering technologies.

**Mail Bombing**: Another form of e-mail attack that is also a DoS is called a **mail bomb**, in which an attacker routes large quantities of e-mail to the target. This can be accomplished by means of social engineering or by exploiting various technical flaws in the Simple Mail Transport Protocol (SMTP). The target of the attack receives an unmanageably large volume of unsolicited e-mail.

**Sniffers**: snifferis a program or device that can monitor data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information. Unauthorized sniffers can be extremely dangerous to a network’s security, because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite

weapon in the hacker’s arsenal. Sniffers often work on TCP/IP networks, where they’re sometimes called **packet sniffers.**

**Social Engineering**: social engineeringis the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

Pharming: **Pharming** is “the redirection of legitimate Web traffic (e.g., browser requests) to an illegitimate site for the purpose of obtaining private information. Pharming often uses Trojans, worms, or other virus technologies to attack the Internet browser’s address bar so that the valid URL typed by the user is modified to that of the illegitimate Web site.

**Timing Attack**: A timing attackexplores the contents of a Web browser’s cache and stores a malicious cookie on the client’s system. The cookie (which is a small quantity of data stored by the Web browser on the local system, at the direction of the Web server) can allow the designer to collect information on how to access password-protected sites.

References

[1] Principle of Information Security by Michael E. Whitman, 5th Edition, Herbert J. Mattord.

[2] Network Security Essentials: Applications and Standards, 4th Edition, William Stallings.