Introduction and Security Trends

Chapter 1

Background

- Why people should be concerned about computer and network security.?
- What are the issues involved in securing computers and networks from a variety of threats utilizing different attacks?

The Security Problem

- **Fifty years ago:**
    - Computers and data were uncommon.
    - Computer hardware was a high-value item and security was mainly a physical issue.

- **Now:**
    - PC's- Ubiquitous and portable, making them much more difficult to secure physically.
    - Computers are often connected to the Internet.
    - The value of the data on computers often exceeds the value of the equipment.

3

The Security Problem

- Networks are used to transfer vast amounts of information
    - Money in the form of bank transactions or credit card purchases.

    - Today, companies rely on the Internet to operate and conduct business
    - Information transferred via networks

- Some people try to take advantage of the environment to conduct fraud or theft.
    - Take advantage of what has made shopping, banking, investment, and leisure pursuits a matter of "dragging and clicking" for many people.
    - Identity theft is common today

4

The Security Problem (*continued*)

- Two basic categories of electronic crime   hacking ,malware ,Denial-of-Service (DoS) Attacks
    1. Crimes in which the computer was the target
    2. Incidents in which a computer was used to perpetrate the act

    Phishing,Identity Theft

    carry out or commit (a harmful, illegal, or immoral action):

Using the internet to stalk, harass, or threaten individuals. This can include sending threatening emails or messages, spreading false information, or using social media to intimidate.

Child Exploitation: Using computers and the internet to exploit children, including the distribution of child pornography

5

Sample of Security Incidents

- The Morris Worm (November 1988)
- Citibank and Vladimir Levin (June–October 1994)
- Kevin Mitnick (February 1995)
- Omega Engineering and Timothy Lloyd (July 1996)
- Worcester Airport and "Jester" (March 1997)
- Solar Sunrise (February 1998)
- The Melissa Virus (March 1999)

- The Love Letter Virus (May 2000)
- The Code Red Worm (2001)
- Adil Yahya Zakaria Shakour (August 2001–May 2002)
- The Slammer Worm (2003)
- U.S. Electric Power Grid (1997–2009)
- Conficker (2008–2009)
- Fiber Cable Cut (2009)

6

- Morris worm
  - Viewed as first Internet Worm to have caused significant damage and to have brought the Internet down

- Kevin Mitnick
  - Convicted of various computer crimes and was known for his ability to conduct successful social engineering attacks
  - FBI described as 2.5 yrs computer hacking spree
  - Gained unauthorized access to computers belonging to Motorola, Novell, Fujitsu, Sun

verdict of jury

A social engineering attack is a type of cyber attack that relies on human interaction and psychological manipulation to deceive individuals into divulging confidential information, performing actions, or granting access to restricted systems. Instead of exploiting technical vulnerabilities, social engineering targets human vulnerabilities.

disclose of private sensitive informations

7

- Melissa Virus
  - Best known early macro-type virus that attach themselves to documents for programs that have limited macro programming capability
  - Attached to MS Word 97 & 2000 docs- Clogged network by sending itself to first 50 addresses in the individual's email address book
- Slammer Worm
  - Credited with reaching global proportions in less than 10 minutes
  - Exploited a buffer overflow vulnerability in computers running Microsoft SQL server

8

Malware

- The term "malware" comes from "malicious software."
- Malware is software that has an evil purpose, designed to cause problems to an individual (for example, identity theft) or system.
- Viruses and worms are just two types of *malware* threats.

9

Threats

Structured threats are well-organized, often originating from skilled and sophisticated attackers.

State-Sponsored Cyberattacks
Insider Threats

- Unstructured
- Structured

Unstructured threats are less organized and may involve opportunistic attackers with varying levels of technical skills. They are often characterized by spontaneity and may lack a clear plan or objective

Malware Infections

10

Unstructured Threats

- Unstructured threats :
    - Attacks by individuals, small groups of attackers
    - Conducted over short periods of time (lasting at most a few months)
    - Do not involve a large number of individuals,
    - Little financial backing
    - Accomplished by insiders or outsiders who do not seek collusion with insiders.

hacker
script kiddie

Viruses and Worms

- *Have no* useful purpose.
- The most common problem that an organization faces.
- Generally are non-discriminating threats.
- Easily detected and generally not the tool of choice for highly structured attacks.
- Released on the Internet in general and are not targeted at a specific organization.
- Antivirus software and system patching can eliminate the largest portion of this threat.

- **Cause- Unaware employees and users**

Intruders

- Hacking
  - The act of deliberately accessing computer systems and networks without authorization.
- **Hackers are individuals who conduct this activity.**
- Intruders need
  - Persistence
  - Patience
  - Determination

13

Types of Intruders

Unauthorized persons

exploit

taking advantage of a security flaw in an operating system, piece of software, computer system, Internet of Things (IoT) device or other security vulnerability

- Script kiddies
  - Do not have the technical expertise to develop scripts or discover new vulnerabilities.
  - Have enough understanding of computer systems to download and run scripts that others have developed.

- Script writers
  - People who are capable of writing scripts to exploit known vulnerabilities
  - Much more technically competent than script kiddies and account for an estimated 8 to 12 percent of malicious Internet activity.

- Elite hackers
  - Highly technical individuals
  - Have the ability to write scripts that exploit vulnerabilities and discover new ones
  - Smallest of the lot, and is responsible for, at most, only 1 to 2 percent of intrusive activity.

High

Elite
1–2%

Script Writers
8–12%

Technical Expertise

Script Kiddies
86 to 91%

Low

14

7

Insiders

Insiders:

- More dangerous than outside intruders.
- <mark>Have the access and knowledge necessary to cause immediate damage to an organization.</mark>
- Besides employees, insiders also include a number of other individuals who <mark>have physical access to facilities</mark>

- <mark>Most security is designed to protect against outside intruders and thus lies at the boundary between the organization and the rest of the world.</mark>
- Attacks by insiders are often the result of employees who have become disgruntled with their organization and are looking for ways to disrupt operations.

angry or dissatisfied:

- It is also possible that **an "attack" by an insider may be an accident and not intended as an attack at all.**

15

Criminal Organizations

- As financial transactions over the Internet increased, criminal organizations followed the money.
- Fraud, extortion, theft, embezzlement, and forgery all take place in an electronic environment.

a person who produces fraudulent copies or imitations:

- A *structured threat* is characterized by a greater amount of planning, longer time to conduct the attack, and more financial backing than in an unstructured attack.

- A difference between criminal groups and the "average" hacker is the level of organization that criminal elements may employ in their attack.

16

Structured Threats

Attacks by criminal organizations can fall into the structured threat category, which is characterized by:

- Planning.
- Long period of time to conduct the activity.
- More financial backing.
- Corruption of or collusion with insiders.
- May not only include attempts to subvert insiders, but also include attempts to plant individuals inside potential targets before an attack.
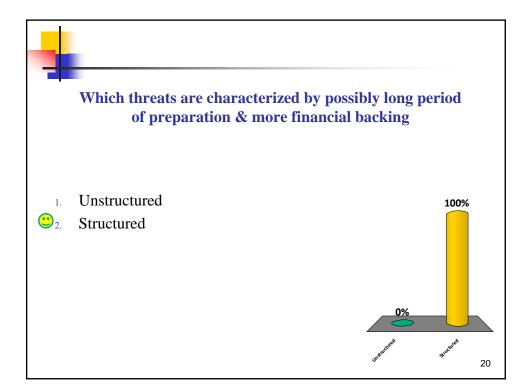
17

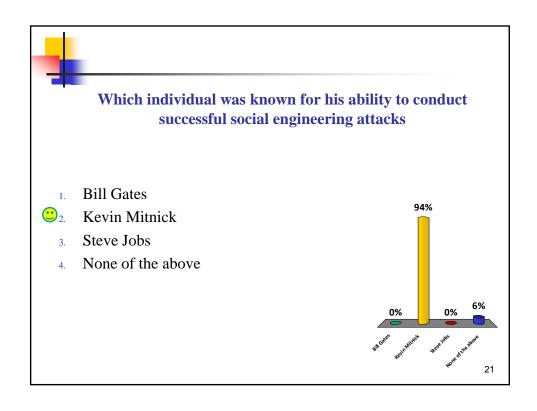## Terrorists and Information Warfare

- Information warfare — Overloading an adversary's servers with traffic to disrupt services.
  - Warfare conducted against information and the information-processing equipment used by an adversary. → rival
  - A highly structured threat.

- Many nations today have developed to some extent the capability to conduct information warfare.
  - Computer systems are important assets that nations depend upon. As such, they are now targets of unfriendly foreign powers.
  - During warfare, nations may choose targets other than the opposing army.
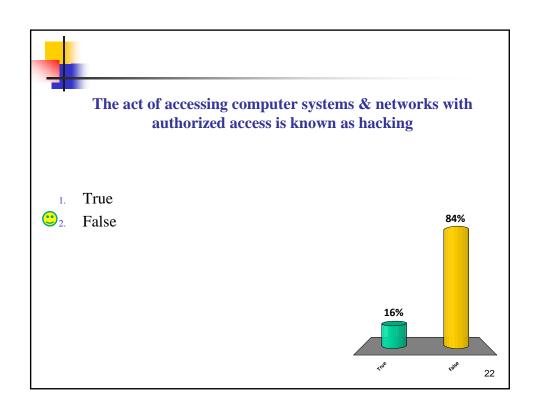
18

9

Critical Infrastructure

- Critical infrastructures are those infrastructures whose loss would have a severe detrimental impact on a nation.
- Examples:
    - Water
    - Electricity
    - Oil and gas refineries and distribution.
    - Banking and finance
    - Telecommunications.

19

Which threats are characterized by possibly long period of preparation & more financial backing

1. Unstructured
2. Structured

100%

0%

Unstructured   Structured

20

Which individual was known for his ability to conduct successful social engineering attacks

1. Bill Gates
2. Kevin Mitnick
3. Steve Jobs
4. None of the above

94%

0%   0%   6%

Bill Gates   Kevin Mitnick   Steve Jobs   None of the above

21

The act of accessing computer systems & networks with authorized access is known as hacking

1. True
2. False

84%

16%

True   False

22

11

Security Trends

- The trend has been away from large mainframes to smaller personal computers.
- Large mainframes are replaced by highly interconnected networks of much smaller systems.
- Security has switched from a closed environment to one in which computer can be accessed from almost anywhere.
- As the level of sophistication of attacks has increased, the level of knowledge necessary to exploit vulnerabilities has decreased.

This trend highlights the decentralization of computing power, with individuals and organizations increasingly relying on smaller, more accessible devices like personal computers, laptops, and mobile devices.

Despite the increasing complexity of cyber attacks, the barrier to entry for would-be attackers has lowered. This is primarily due to the availability of exploit kits, hacking tools, and online resources that provide step-by-step instructions for carrying out attacks.

23

Security Trends (*continued*)

- The percent of organizations experiencing security incidents has declined
- Four types of attacks are on the rise
    - Unauthorized access
    - Theft/loss of proprietary information
    - Misuse of web applications
    - DNS attacks

They commonly aim to render the DNS unavailable or alter the answers provided by the DNS, directing unsuspecting users to malicious websites

24

Profile of Individuals

- The type of individual who attacks a computer system or a network has also evolved over the last 30 years.
  - The rise of non-affiliated intruders, including "script-kiddies," has greatly increased the number of individuals who probe organizations looking for vulnerabilities to exploit.

- Another trend :
  - As the level of sophistication of attacks has increased, the level of knowledge necessary to exploit vulnerabilities has decreased.

25

Avenues of Attack

- There are two general reasons a particular system is attacked:

  - **Specifically targeted** by the attacker
    - Choice based on for example, political reason.
    - A *hacktivist* is a hacker who uses their skills for political purposes
    - An example - A person who defaces the web site of a fur coat company in protest of animal cruelty

  - or it is **an opportunistic target**.
    - Conducted against a site that has hardware or software that is vulnerable to a specific exploit.
    - The attackers are not targeting the organization.

verb

To exploit something means to make full use of a resource, opportunity, or situation for one's own benefit, often in a way that may be perceived as unfair or unethical.

26

13

Avenues of Attack (*continued*)

- Targets of opportunity
  - Attacks are conducted against a site that has software vulnerable to a specific exploit.
  - In these instances, the attackers are not targeting the organization, instead they are targeting a vulnerable device that happens to belong to the organization.
  - Relies on the fact that with any piece of widely distributed software, there will almost always be somebody who has not patched the system.

- Targeted attacks
  - Specifically targeted attacks generally are more difficult and take more time than targets of opportunity.
  - More difficult and take more time than attacks on a target of opportunity.

27

Which of the following is an attempt to find and attack a site that has a software that is vulnerable to a specific exploit

1. Target of opportunity
2. Targeted attack
3. Vulnerability scan attack
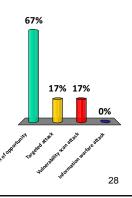4. Information warfare attack

67%

17% 17%

0%

Target of opportunity
Targeted attack
Vulnerability scan attack
Information warfare attack

Scanning for Vulnerabilities: The attacker uses automated tools or scripts to scan the internet for websites running software with known vulnerabilities. These vulnerabilities could be in web applications, content management systems (CMS), server software, or other components.
Identifying Target Sites: Once the attacker identifies a site that appears to be running vulnerable software, they may further analyze it to confirm the presence of the vulnerability and assess its potential impact.
Exploiting the Vulnerability: With knowledge of the specific vulnerability present on the target site, the attacker crafts or obtains an exploit code that can take advantage of it. This exploit code could be a piece of malware, a script, or a payload designed to exploit the vulnerability and gain unauthorized access to the target system.
Launching the Attack: The attacker then launches the attack against the vulnerable site by sending the exploit code to the target system. This could be done through various means, such as sending a specially crafted HTTP request to a web server or injecting malicious code into a web form.

28

14

The Steps in an Attack

Step		
1 Profiling	Gather information on the target organization	Check the SEC EDGAR web site (www.sec.gov/edgar.shtml), whois look up, google
2	Determine systems available	Ping sweep with nmap or superscan
3 Finger printing	Determine the OS and open ports	Nmap or superscan, banner grab
4	Discover applicable exploits	Search web sites for vulnerabilities and exploits that exist for the OSes and services discovered
5	Execute exploit	Systematically execute exploits

29

Sources of Information

- There are numerous web sites that provide information on vulnerabilities in specific application programs and operating systems.

- In addition to information about specific vulnerabilities, some sites may also provide tools that can be used to exploit vulnerabilities.

- An attacker can search for known vulnerabilities and tools that exploit them, download the information and tools, and then use them against a site.

30

Minimizing Possible Avenues of Attack

- Administrative Mistake
  - The attack may be successful if the administrator for the targeted system has not installed the correct patch.
- The attacker will move on to the next possible vulnerability if the patch has been installed.

Minimizing Possible Avenues of Attack

System hardening	Involves reducing the services that are running on the system
Patching	Ensures that your operating system and applications are up-to-date
Limiting information	Makes it more difficult for an attacker to develop the attack by limiting the information available about your organization

31

Disable Unnecessary Services: Only enable services that are essential for the system's intended functionality. Unnecessary services can provide additional entry points for attackers.
Remove Unneeded Software: Uninstall software applications and packages that are not required. Each installed application increases the system's attack surface.

ethical hacking

The General Process

- There are different ways in which a system can be attacked.
  - Gathering as much information as possible about the target (using both electronic and non-electronic means).
  - Gathering information about possible exploits based on the information about the system, and then systematically attempting to use each exploit.

- If the exploits do not work, other, less system-specific, attacks may be attempted.

The general process for conducting an attack on a system, particularly in the context of ethical hacking or penetration testing, involves several distinct steps. Each step is designed to methodically uncover vulnerabilities and exploit them to assess the security of the system

32

Electronic Means:
Network Scanning: Use tools like Nmap to discover active devices, open ports, and services running on the network.

Non-Electronic Means:
Social Engineering: Collecting information through interactions with people, often by impersonating trusted entities to extract confidential details.

Types of Attacks

- If successful, an attack may produce one or more of the following:
  - Loss of confidentiality
    - Information is disclosed to individuals not authorized to see it.
  - Loss of integrity
    - Information is modified by individuals not authorized to change it.
  - Loss of availability
    - Information or the system processing it are not available for use by authorized users when they need the information.

More in Chap. 15

33

Maintaining Information Assurance Over Time

- Ensures that the information assurance system continues to be appropriate to the environment
- A disciplined and systematic process is used to guarantee that the protection will be maintained
- A continuous process based on continuous feedback from operations

34

Ensuring a Disciplined Process: Establishing the Culture

- Only way to assure security is by demanding disciplined performance of assigned duties
    - Requires a high degree of disciplined practice by people responsible for carrying out the tasks
        - The managers
        - The workers
        - Humans are the weakest link in the security chain
    - Requires the right level of information assurance and security practice

35

Humans are the weakest link in the security chain

1. True
2. False

100%

0%

True   False

36