FUNDAMENTALS OF INFORMATION SYSTEM SECURITY

CHAPTER ONE: OVERVIEW OF THE COMPUTER SECURITY

Introduction to Computer Security

1.1 Motivation:

Scenario

a) Institutions targeted in a large-scale attack against computers worldwide

- *A massive cyber-attack that locks files in a computer until the owner pays ransom that has been infecting computers around the world*
- *The 'Wannacry' malware was behind a massive disruption of medical services in England and Scotland after attacking the servers of the National Health Service (NHS) in the UK, sometime back (2017)*
  - In May 2017, the MCA21 system was subjected to **WannaCry ransomware attack**. The **attack** was in the nature of a 'zero day **attack**' and was first noticed on May 7, the document said. Zero day **attack** refers to hackers exploiting a flaw in a software system that is not known to the vendor itself.Jun 19, 2017

Introduction to Computer Security

1.1 Motivation:

Scenario

a) Institutions targeted in a large-scale attack against computers worldwide

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. In response, Colonial Pipeline Company halted all of the pipeline's operations to contain the attack. With the assistance of the FBI, Colonial Pipeline paid the requested ransom (75 bitcoin or $4.4 million) within several hours after the attack.The hackers then sent Colonial Pipeline a software application to restore their network, but it operated very slowly.
- The Federal Motor Carrier Safety Administration issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May 9. It was the largest cyberattack on an oil infrastructure target in the history of the United States. The FBI and various media sources identified the criminal hacking group Dark Side as the responsible party. The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack

Introduction to Computer Security

1.1 Motivation:

Scenario

a) Institutions targeted in a large-scale attack against computers worldwide

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline. In response, Colonial Pipeline Company halted all of the pipeline's operations to contain the attack. With the assistance of the FBI, Colonial Pipeline paid the requested ransom (75 bitcoin or $4.4 million) within several hours after the attack.The hackers then sent Colonial Pipeline a software application to restore their network, but it operated very slowly.
- The Federal Motor Carrier Safety Administration issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open on May 9. It was the largest cyberattack on an oil infrastructure target in the history of the United States. The FBI and various media sources identified the criminal hacking group Dark Side as the responsible party. The same group is believed to have stolen 100 gigabytes of data from company servers the day before the malware attack

1.1 Motivation: Scenario Cont……

- b) **A story from Computerworld**
  - *A story about a programmer employee of a company who allegedly launched a denial-of-service attack against his own company, a provider of on-line stock trading services. Apparently, this programmer was in negotiations with the company for more compensation. He became frustrated with the progress of the negotiations and decided to demonstrate to the company its vulnerability by launching an attack on its systems from the Internet. He was intimately familiar with the company's systems and software, and his inside knowledge enabled him to hit the firm in a manner that shut it down. In fact, the attack disrupted stock trading services at the company for three days. The U.S. Secret Service was eventually employed, and the attack was traced to the employee, who was subsequently arrested.*
  - Every organization should monitor its systems for possible unauthorized intrusion and other attacks. This needs to be part of the daily routine of every organization's IT unit, as it is essential to safeguarding a company's information assets.

1.1 Motivation: Scenario Cont……

- b) ***four scenarios you should train for and be ready to respond to in the event of a cyber security incident:***

1. **Phishing Emails –**
   - The frequency of phishing emails and overall business email compromise (BEC) has gained momentum, especially as ransomware attacks have been on the rise. According to a study conducted by Malwarebytes,;
     - *47 percent of U.S. companies experienced a ransomware attack in the some year, with 50 percent of those incidents resulting from someone clicking on a malicious link in emails.*
   - Educating employees to practice due diligence is a first step, and conducting faux phishing exercises can be a valuable teaching tool.
2. **Malicious Attachments –**
   - It's just as important for your security team to know when malicious attachments make their way onto the network as it is to avoid opening them.
   - If malicious attachments make it through your filters and into your employee's in-boxes, you need a plan in place – one that has been practiced – to be able to respond quickly and limit the damage. .

1.1 Motivation: Scenario Cont……

b) four scenarios you should train for and be ready to respond to in the event of a cyber security incident:

3. Password and Other Suspicious Requests

– Cybercriminals can pose as employees, contractors, or third-party vendors to bait employees into divulging sensitive passwords and other access controls. Your security personnel should be trained on how to respond.

- *You can test your incident response teams and employees by running exercises to simulate password requests from familiar sources such as the help desk or even executives, who are often spoofed.*

4. Unauthorized Computers and Devices on Network –

- *Computers and devices that haven't gone through proper authentication processes before joining your corporate network are perfect targets for attackers.*
  - *response teams should not only identify attempts to connect to a network, but block them?*

These are just a few of the scenarios you can use to test your incident response team's readiness for a cyber incident. Practicing these on a regular basis can help your team be better prepared and identify any weaknesses before you're in the midst of a crisis, saving you time, money, and peace of mind

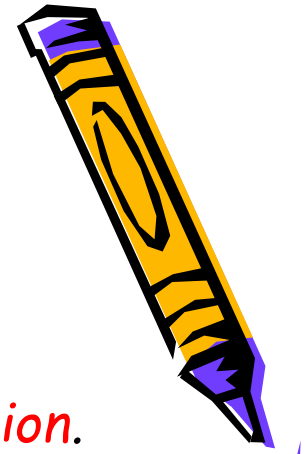
2. Basic Security Concepts

- **Definitions and terminologies**
  - **Security:**
  - Freedom from risk and danger.
    - Originally, computers security meant physical security and confidentiality.
    - Integrity and access control then became important with multi-tasking computers.
    - In recent years availability is a big issue.
  - *Further,*
    - ***Security*** *is the ability of a system to protect information and system resources with respect to confidentiality, integrity, and availability.*

2. Basic Security Concepts

- **Definitions and terminologies Cont.……**
  - **Computer Security**
    - Refer to the collection of tools designed to protect data and to thwart hackers.
    - *is protection of computing assets and computer network(communication assets) against abuse, unauthorized use, unavailability through intentional or unintentional actions, and protection against undesired information disclosure, alteration, or misinformation.*
  - today's environment:-
    - *the subject encompasses*
      - *computers ranging from supercomputers to microprocessor-based controllers and microcomputers, software,*
      - *peripheral equipment (including terminals, printers),*
      - *communication media (e.g., cables, antennas, satellites),*
      - *people who use computers or control computer operations, and networks (some of global extent) that interconnect computers, terminals, and other peripherals.*

2. Basic Security Concepts



- **Definitions and terminologies Cont.……**

❑ **Network Security**

- *Involves measures to protect data during their transmission.*
- *It is the protection of networks and their services that ensure that the network performs its critical functions correctly and without harmful side effects. It prohibits unauthorized modification, destruction, or disclosure.*
  - *(**Network Security Officer is** the individual in charge of network security. He is also referred to as Information System Security Officer).*

❑ **Internet Security**

- Measures to protect data during their transmission over a collection of interconnected networks

2. Basic Security Concepts

- **Definitions and terminologies Cont…….**

❑ **Vulnerabilities**

- is a weakness in the security system,
  - for example, in procedures, design, or implementation that might be exploited to cause loss or harm.
    - *For instance, a particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.*
- ***Vulnerability*** is a known or suspected flaw in the hardware or software designer operation of system that exposes the system to penetration of its information to accidental disclosure.

•

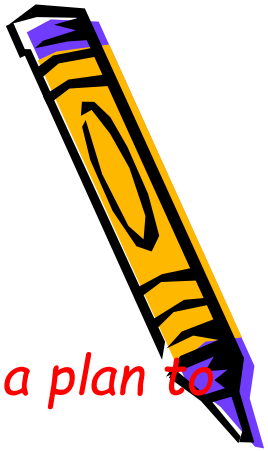
2. Basic Security Concepts

- **Definitions and terminologies Cont……**
- **Threats** to a computing system
  - is a set of circumstances that has the potential to cause loss or harm.
  - There are many threats to a computer system, including human-initiated and computer-initiated ones.
    - *We have all experienced the results of inadvertent human errors, hardware design flaws, and software failures. But natural disasters are threats, too; they can bring a system down when the computer room is flooded or the data center collapses from an earthquake, for example.*

a) A ***threat*** is a potential possibility of a deliberate unauthorized attempted to:

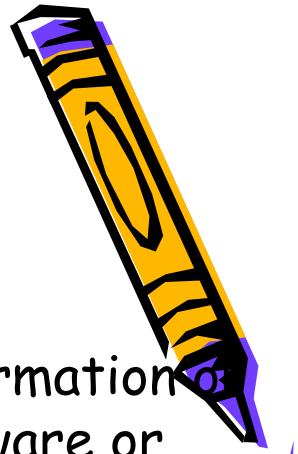
- *Access information,*
- *Manipulate information*
- *Render a system unreliable or unusable*

2. Basic Security Concepts



- **Definitions and terminologies Cont…….**
  - **b) Attacks**
    - *An attack is a specific formulation or execution of a plan to carry out a threat.*
    - A human who exploits a vulnerability perpetrates an **attack** on the system.
    - An attack can also be launched by another system, as when one system sends an overwhelming set of messages to another, virtually shutting down the second system's ability to function.
      - » Unfortunately, we have seen this type of attack frequently, as denial-of-service attacks flood servers with more messages than they can handle.

2. Basic Security Concepts



- **Definitions and terminologies Cont…….**

c) Risk

– A risk is an accidental and unpredictable exposure of information or violation of operations integrity due to malfunction of hardware or incomplete or incorrect software design.

d) Penetration

– Is a successful attack; the ability to obtain unauthorised (undetected) access to files and programs or the control state of a computer system.

3. Security issues

- The world before computers was in some ways much simpler. Why
  - *Signing, legalizing a paper would authenticate it*
  - *Photocopying easily detected*
  - *Erasing, inserting, modifying words on a paper document easily detectable*
  - *Secure transmission of a document: seal it and use a reasonable mail carrier (hoping the mail train does not get robbed)*
  - *One can recognize each other's face, voice, hand signature, etc.*

- Electronic world: the ability to copy and alter information has changed dramatically
  - *No difference between an "original" file and copies of it*
  - *Removing a word from a file or inserting others is undetectable*
  - *Adding a signature to the end of a file/email: one can impersonate it – add it to other files as well, modify it, etc.*
  - *Electronic traffic can be (and is!) monitored, altered, often without noticing*
  - *How to authenticate the person electronically communicating with you*

3. Security issues

- ***Possible adversaries***
  - Student: to have fun snooping on other people's email
  - Cracker: to test out someone's security system, to steal data
  - Businessman: to discover a competitor's strategic marketing plan
  - Ex-employee: to get revenge for being fired
  - Accountant: to embezzle money from a company
  - Stockbroker: to deny a promise made to a customer by email
  - Convict: to steal credit card numbers for sale
  - Spy: to learn an enemy's military or industrial secrets
  - Terrorist: to steal germ warfare secrets
- **Note**
  - *Making a network or a communication secure involves more than just keeping it free of programming errors. It involves outsmarting often intelligent, dedicated and often well-funded adversaries.*

3. Security issues

- ***Security issues: Some practical situations***
  - ***A sends a file to B: E intercepts it and reads it***
    - *How to send a file that looks gibberish (nonsense) to all but the intended receiver?*
  - ***A sends a file to B: E intercepts it, modifies it, and then forwards it to B***
    - *How to make sure that the document has been received in exactly the form it has been sent*
  - ***E sends a file to B pretending it is from A***
    - *How to make sure your communication partner is really who he/she claims to be*
  - ***A sends a message to B: E is able to delay the message for a while***
    - *How to detect old messages*
  - ***A sends a message to B. Later A (or B) denies having sent (received) the message***
    - *How to deal with electronic contracts*
    - E learns which user accesses which information although the information itself remains secure. E prevents communication between A and B: B will reject any message from A because they look unauthentic.

3. Security issues

- ***Security issues: Some practical situations cont….***
  - ***A sends a message to B. Later A (or B) denies having sent (received) the message***
    - *How to deal with electronic contracts*
    - E learns which user accesses which information although the information itself remains secure. E prevents communication between A and B: B will reject any message from A because they look unauthentic.

5. Goals of Security

- Given a policy that specifies what is "secure" and what is "non-secure", the goal of security is to put in place mechanisms that provide:
  - ***Prevention,***
  - ***Detection and***
  - ***Response,*** and
  - **the basis for network security**.
- The security trinity should be the foundation for all security policies and measures that an organization develops and

Figure 1: The security trinity.

5. Goals of Security Cont…

- **Prevention**
  - involves implementing mechanisms that users cannot override and are trusted to be implemented in correct and unalterable ways.
  - To provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities.
  - In developing network security schemes, organizations should emphasize preventative measures over detection and response: It is easier, more efficient, and much more cost-effective to prevent a security breach than to detect or respond to one. Remember that it is impossible to devise a security scheme that will prevent all vulnerabilities from being exploited, but companies should ensure that their preventative measures are strong enough to discourage potential criminals-so they go to an easier target.
- **Detection**
  - The goal of detection is to determine that an attack is underway, or has occurred and report it. Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches, in the event preventative measures fail. It is very important that problems be detected immediately. The sooner a problem is detected the easier it is to correct and cleanup.

5. Goals of Security Cont…

- **Response**
  - *Organizations need to develop a plan that identifies the appropriate response to a security breach. The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation.*
  - ***Recovery***
    - ***is the** resuming the correct operation either after an attack or even while an attack is underway.*

6. Why Is Computer and Network Security Important?

- Computer and network security is important for the following reasons.

a) To protect company assets:

- One of the primary goals of computer and network security is the protection of company assets.
- By "assets,"
  - *it means the hardware and software that constitute the company's computers and networks. The assets are comprised of the "information" that is housed on a company's computers and networks. Information is a vital organizational asset. Network and computer security is concerned with the protection, integrity, and availability of information.*

b) ***To gain a competitive advantage:***

- *Developing and maintaining effective security measures can provide an organization with a competitive advantage over its competition.*
- *Network security is particularly important in the arena of Internet financial services and e-commerce. It can mean the difference between wide acceptance of a service and a mediocre customer response. For example, how many people do you know who would use a bank's Internet banking system if they knew that the system had been successfully hacked in the past? Not many. They would go to the competition for their Internet banking services.*

6. Why Is Computer and Network Security Important?

- Computer and network security is important for the following reasons.
- ***c) To comply with regulatory requirements and fiduciary responsibilities:***
  - *Corporate officers of every company have a responsibility to ensure the safety and soundness of the organization.*
  - *Part of that responsibility includes ensuring the continuing operation of the organization. Accordingly, organizations that rely on computers for their continuing operation must develop policies and procedures that address organizational security requirements. Such policies and procedures are necessary not only to protect company assets but also to protect the organization from liability. For-profit organizations must also protect shareholders' investments and maximize return. In addition, many organizations are subject to governmental regulation, which often stipulates requirements for the safety and security of an organization. For example, most financial institutions are subject to federal regulation. Failure to comply with federal guidelines can result in the seizure of a financial institution by federal regulators. In some cases, corporate officers who have not properly performed their regulatory and fiduciary responsibilities are personally liable for any losses incurred by the financial institution that employs them.*

6. Why Is Computer and Network Security Important?

- Computer and network security is important for the following reasons.

d) To keep your job:

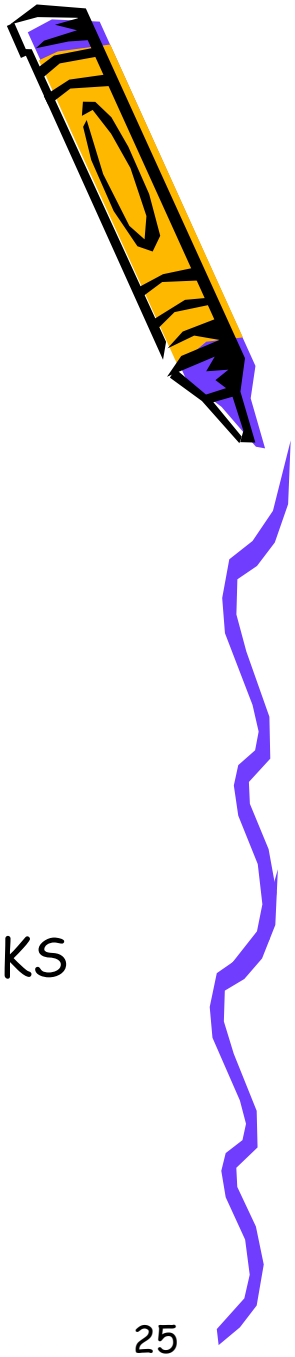
- *Finally, to secure one's position within an organization and to ensure future career prospects, it is important to put into place measures that protect organizational assets. Security should be part of every network or systems administrator's job. Failure to perform adequately can result in termination. Termination should not be the automatic result of a security failure, but if, after a thorough postmortem, it is determined that the failure was the result of inadequate policies and procedures or failure to comply with existing procedures, then management needs to step in and make some changes.*

- ***Recap:***

– *One thing to keep in mind is that network security costs money:*
  - *It costs money to hire, train, and retain personnel;*
  - *to buy hardware and software to secure an organization's networks; and to pay for the increased overhead and degraded network and system performance that results from firewalls, filters, and intrusion detection systems (IDSs).*

– *As a result, network security is not cheap. However, it is probably cheaper than the costs associated with having an organization's network compromised.*

The END



Q&A

THANKS