Introduction to Information Security

Instructor: C. Pu (Ph.D., Assistant Professor)

Lecture 01

puc@marshall.edu

History of Information Security

- The history of information security begins with the concept of **computer security**

- **computer security**
  - in the early days of computers, this term specified the need to *secure the physical location* of computer technology from outside threats
  - later, this term later came to represent all actions taken to preserve computer systems from losses

History of Information Security

- The need for computer security arose during World War II
  - the first mainframe computers were developed
    - used to aid computations for communication code breaking messages from enemy cryptographic device, like the Enigma

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

- Enigma machine, https://www.youtube.com/watch?v=ASfAPOiq_eQ
- Flaw in Enigma Code, https://www.youtube.com/watch?v=V4V2bpZlqx8

History of Information Security

- Multiple levels of security were implemented to protect these devices and the missions they served
  - new processes as well as tried-and-true methods needed to maintain data confidentiality
    - access to sensitive military locations was controlled by means of
      - badges, keys, the facial recognition of authorized personnel by security guards

- The growing need to maintain national security eventually led to
  - more complex and technologically sophisticated computer security safeguards

History of Information Security

- During these early years, information security was a straightforward process composed pre-dominantly of *physical security* and *simple document classification schemes*
- The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage.
- The first documented security problems occurred in the early 1960s
  - a systems administrator was working on a MOTD (message of the day) file while another administrator was editing the password file
  - a software glitch mixed the two files, and the entire password file was printed on every output file

The 1960s

- During the Cold War, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks

- The Department of Defense's Advanced Research Projects Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the military's exchange of information

- In 1968, Dr. Larry Roberts developed the ARPANET project
  - ARPANET evolved into what we now know as the Internet
  - https://www.internethalloffame.org/inductees/lawrence-roberts

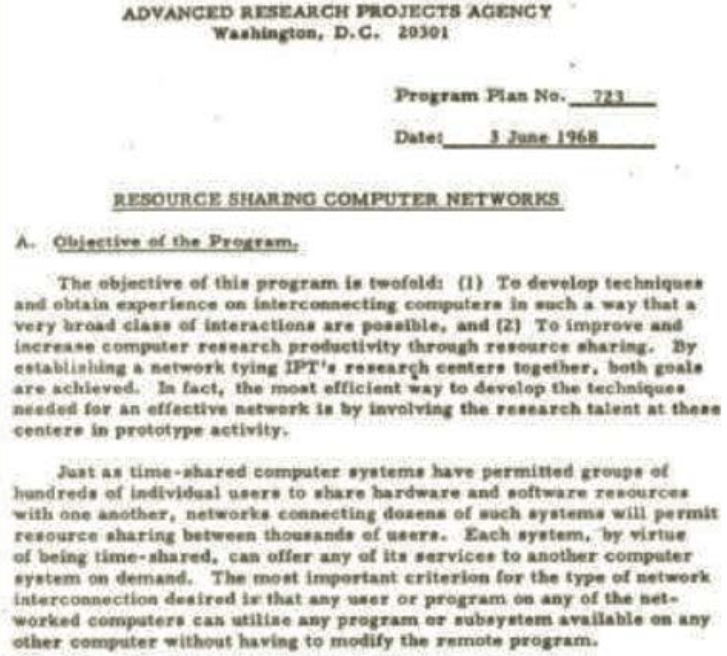
The 1960s: ARPANET Project

ARPANET Program Plan

June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71



ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723

Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

The 1970s and 80s

- ARPANET became more popular and saw wider use, increasing the potential for its *misuse*

- Fundamental problems with ARPANET security
  - no sufficient controls and safeguards to protect data from unauthorized remote users
  - vulnerability of password structure and formats
  - lack of safety procedures for dial-up connections
  - nonexistent user identification and authorizations

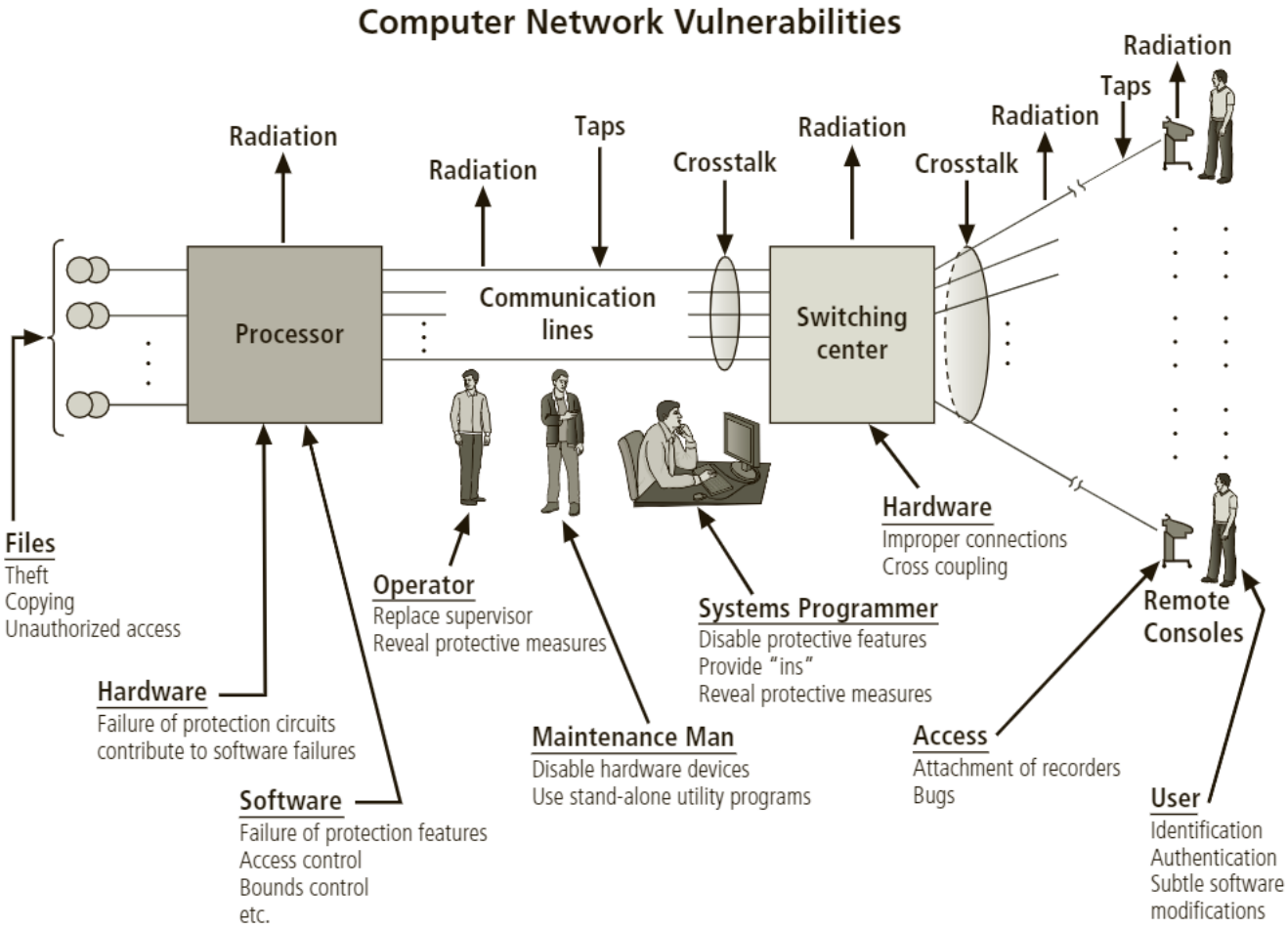
- For example,
  - Phone numbers were widely distributed and openly publicized on the walls of phone booths, giving hackers easy access to ARPANET

The 1970s and 80s

- In June 1967, ARPA formed a task force to study the process of securing classified information systems
- RAND Report R-609
  - the first widely recognized published document to identify the role of management and policy issues in computer security
  - the wide use of networking components in military information systems introduced security risks that could not be mitigated by the routine practices then used to secure these systems
  - this paper signaled a pivotal moment in computer security history
    - the scope of computer security expanded significantly from the safety of physical locations and hardware to include:
      - securing the data
      - limiting random and unauthorized access to that data
      - involving personnel from multiple levels of the organization in information security

The 1970s and 80s

An illustration of computer network vulnerabilities



The 1990s

- At the close of the 20th century, networks of computers became more common, as did the need to connect them to each other
- The Internet brought connectivity to virtually all computers that could reach a phone line or an Internet-connected local area network
- As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats
- In the late 1990s and into the 2000s, many large corporations began publicly integrating security into their organizations
- Antivirus products became extremely popular, and information security began to emerge as an independent discipline

2000 to Present

- Today, the Internet brings millions of *unsecured* computer networks and billions of computer systems into continuous communication with each other
- The security of each computer's stored information is contingent on the security level of every other computer to which it is connected
- The growing threat of cyberattacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure
- Another growing concern is the threat of nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended

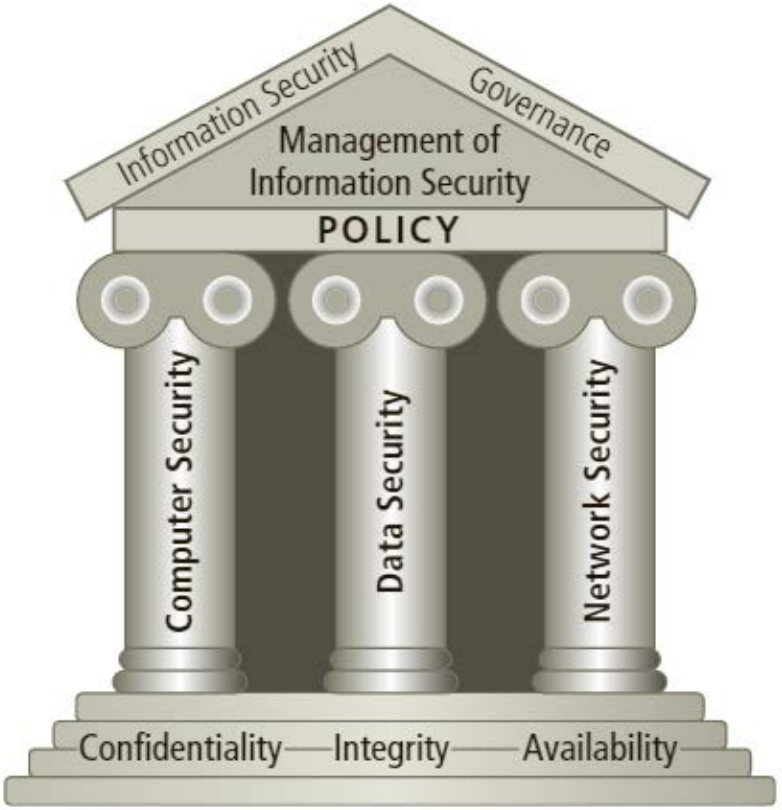
What Is Security?

- ***Security is protection***
  - protection from adversaries—those who would do harm, intentionally or otherwise—is the ultimate objective of security
- Achieving the appropriate level of security for an organization also requires a multifaceted system
- A successful organization should have multiple layers of security in place to protect its operations, physical infrastructure, people, functions, communications, and information

What Is Security?

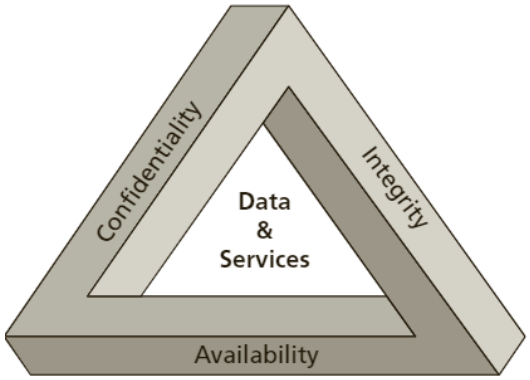
- The Committee on National Security Systems (CNSS) defines ***information security*** as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information

- Information security includes the broad areas of information security management, data security, and network security



What Is Security?

- The CNSS model of information security evolved from a concept developed by the computer security industry called the C.I.A. triad
  - confidentiality
  - integrity
  - availability



- The threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events
  - accidental or intentional damage
  - destruction
  - theft
  - unintended or unauthorized modification
  - other misuse from human or nonhuman threats

Key Information Security Concepts

- Access:
  - A subject or object's ability to use, manipulate, modify, or affect another subject or object
  - Authorized users have legal access to a system, whereas hackers must gain illegal access to a system
  - Access controls regulate this ability

- Asset:
  - The organizational resource that is being protected
  - An asset can be logical, such as a Web site, software information, or data; or an asset can be physical, such as a person, computer system, hardware, or other tangible object
  - Assets, particularly information assets, are the focus of what security efforts are attempting to protect

Key Information Security Concepts

- Attack:
  - An intentional or unintentional act that can damage or otherwise compromise information and the systems that support it
  - Attacks can be active or passive, intentional or unintentional, and direct or indirect

- Control, Safeguard, or Countermeasure:
  - Security mechanisms, policies, or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve security within an organization
  - The various levels and types of controls are discussed more fully in the following lectures

Key Information Security Concepts

- Exploit:
  - A technique used to compromise a system
  - Threat agents may attempt to exploit a system or other information asset by using it illegally for their personal gain
  - Or an exploit can be a documented process to take advantage of a vulnerability or exposure, usually in software, that is either inherent in the software or created by the attacker
  - Exploits make use of existing software tools or custom-made software components

- Exposure:
  - A condition or state of being exposed; in information security, exposure exists when a vulnerability is known to an attacker

Key Information Security Concepts

- Loss:
  - A single instance of an information asset suffering damage or destruction, unintended or unauthorized modification or disclosure, or denial of use
  - When an organization's information is stolen, it has suffered a loss

- Protection Profile or Security Posture:
  - The entire set of controls and safeguards, including policy, education, training and awareness, and technology, that the organization implements to protect the asset.
  - The terms are sometimes used interchangeably with the term security program, although a security program often comprises managerial aspects of security, including planning, personnel, and subordinate programs.

Key Information Security Concepts

- Risk:
  - The probability of an unwanted occurrence, such as an adverse event or loss
  - Organizations must minimize risk to match their risk appetite—the quantity and nature of risk they are willing to accept

- Subjects/Objects of Attack:
  - A computer can be either the subject of an attack—an agent entity used to conduct the attack—or the object of an attack: the target entity
  - A computer can also be both the subject and object of an attack.
    - For example, it can be compromised by an attack (object) and then used to attack other systems (subject)

Key Information Security Concepts

Computer as the subject and object of an attack

Source: Ovchinnkov Vladimir

to steal information across the Internet from…

Source: frank_peters

Hacker using a laptop as the *subject* of an attack…

Source: 4X-image

a remote server that is the *object* of the hacker's attack.

Key Information Security Concepts

- Threat:
  - Any event or circumstance that has the potential to adversely affect operations and assets
  - The term threat source is commonly used interchangeably with the more generic term threat
  - While the two terms are technically distinct, in order to simplify discussion, the text will continue to use the term threat to describe threat sources
- Threat agent:
  - The specific instance or a component of a threat
- Threat event:
  - An occurrence of an event caused by a threat agent
  - This term is commonly used inter-changeably with the term attack
- Threat source:
  - A category of objects, people, or other entities that represents the origin of danger to an asset—in other words, a category of threat agents.

Key Information Security Concepts

- Vulnerability:
  - A potential weakness in an asset or its defensive control system(s)
  - Some examples of vulnerabilities are a flaw in a software package, an unprotected system port, and an unlocked door
  - Some well-known vulnerabilities have been examined, documented, and published; others remain latent (or undiscovered)

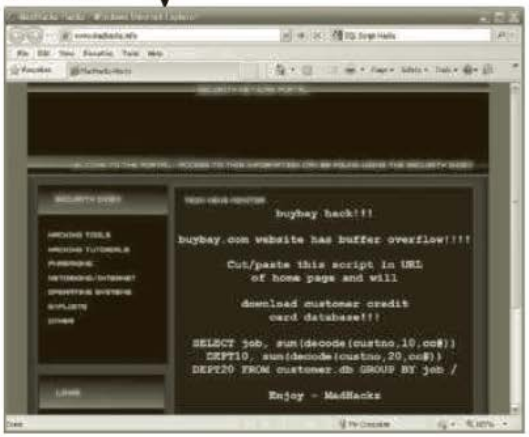
Key Information Security Concepts

Key concepts in information security

Threat: Theft
Threat agent: Ima Hacker

Vulnerability: Buffer overflow in online database Web interface

Exploit: Script from MadHackz Web site



Attack: Ima Hacker downloads an exploit from MadHackz Web site and then accesses buybay's Web site. Ima then applies the script, which runs and compromises buybay's security controls and steals customer data. These actions cause buybay to experience a **loss.**

Asset: buybay's customer database