Introduction

Modifications by Prof. Dong Xuan
and Adam C. Champion

Learning Objectives

Upon completion of this material, you should be able to:

- Understand the definition of information security
- Understand the key terms and critical concepts of information security
- Comprehend the history of computer security and how it evolved into information security

Administrative Matters

- Syllabus
- Class website: http://cse.osu.edu/~champion/4471/
- Group project
- Textbook (4th ed. preferable)
- Readings
  - Chaps. 1–2 in the book

What is an Information System?

- Information System (IS) is an entire set of ***software, hardware, data, people, procedures,*** and ***networks*** necessary to use information as a resource in the organization

Critical Characteristics of Information

- The value of information comes from the characteristics it possesses:
  - **Confidentiality:** self-explanatory
  - **Integrity:** (Bitwise) identical to the original
  - **Availability:** of info, services, etc.
  - **Authenticity**: "it is what it claims to be"
  - **Accuracy:** free from mistakes and errors
  - **Utility:** self-explanatory
  - **Possession:** different from confidentiality
- Others: user authentication, auditability, non-repudiation

What is Security?

- Definitions:
  - Book: "The quality or state of being secure—to be free from danger"
  - James Anderson, Inovant: "Well-informed sense that information risks and controls are in balance"
  - Rita Summers, *IBM Systems Journal*, 1984: "Includes concepts, techniques and measures that are used to protect computing systems and the information they maintain against deliberate or accidental threats"
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - ***Information security***

What is Information Security?

- The protection of information and its critical elements, including systems that use, store, and transmit that information
- Necessary tools: ***policy, awareness, training, education, technology***

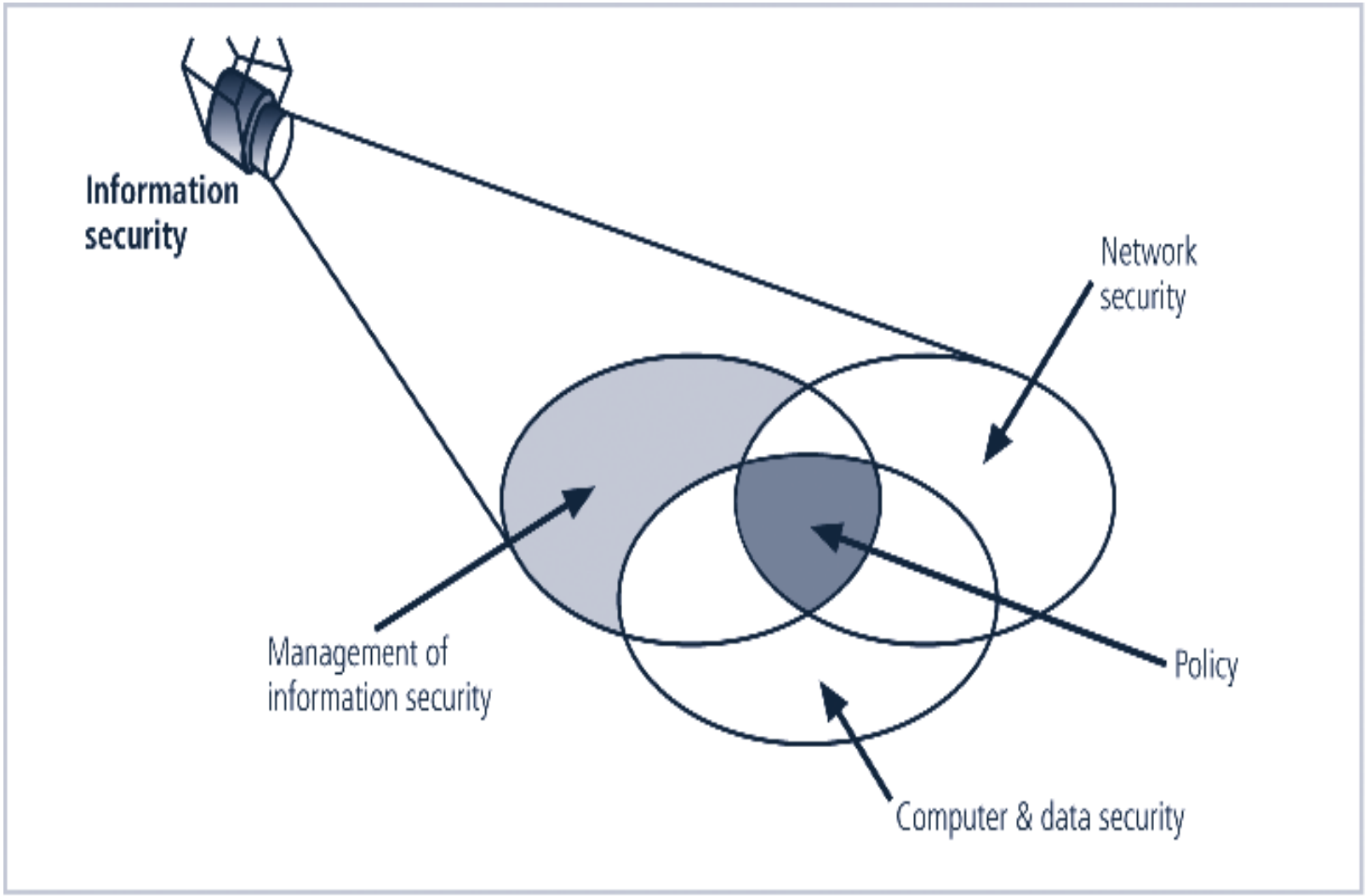

FIGURE 1-3 Components of Information Security

Securing Components in an Information System

- Computer (software and hardware) is the key component in an information system
- Computer can be subject of an attack and/or the object of an attack
  - When the subject of an attack, computer is used as an active tool to conduct attack
  - When the object of an attack, computer is the entity being attacked

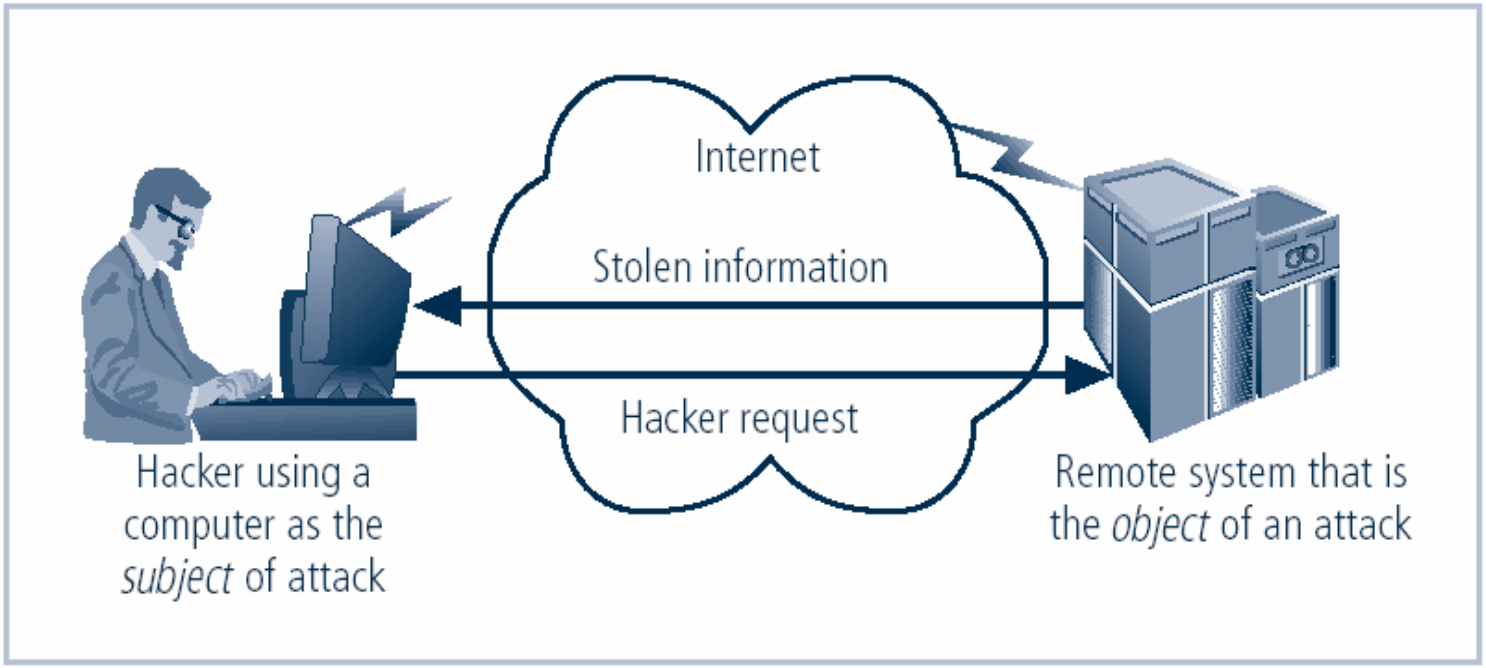

FIGURE 1-6 Computer as the Subject and Object of an Attack

Balancing Information Security and Access

- Impossible to obtain perfect security—it is a process, not an absolute
- Security should be considered balance between protection and availability
- To achieve balance, level of security must allow reasonable access, yet protect against threats

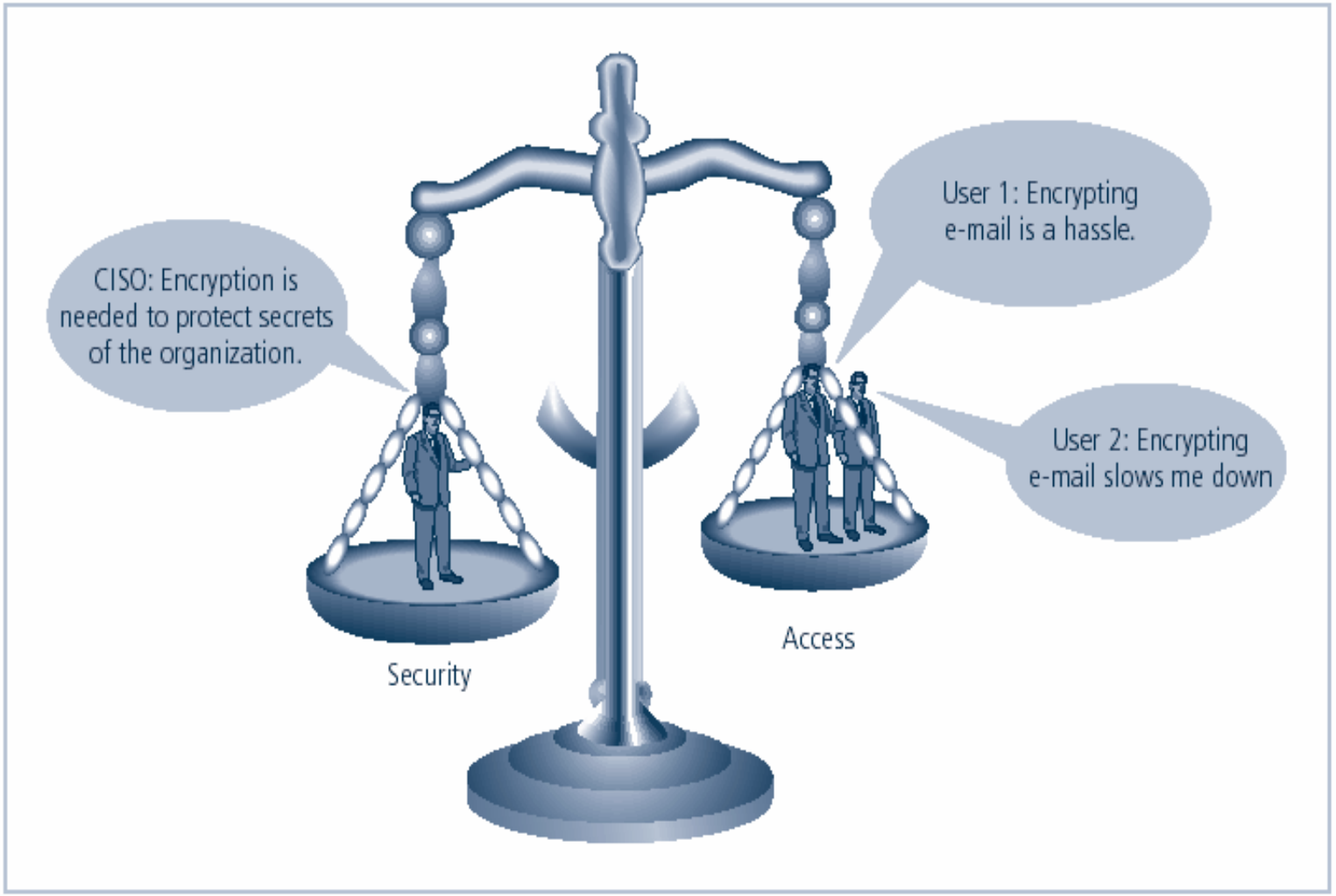

FIGURE 1-7 Balancing Information Security and Access

History of Information Security

- Began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers

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."

Courtesy of National Security Agency

FIGURE 1-1 The Enigma[2]

The 1960s

- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications
- Larry Roberts developed ARPANET from its inception

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.

Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan[4]

The 1970s and 80s

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to ARPANET
  - Non-existent user identification and authorization to system
- Late 1970s: microprocessor expanded computing capabilities and security threats

R-609

- Information security began with Rand Report R-609 (paper that started the study of computer security)
- Scope of computer security grew from physical security to include:
  - Safety of data
  - Limiting unauthorized access to data
  - Involvement of personnel from multiple levels of an organization

The 1990s

- Networks of computers became more common; so too did the need to interconnect networks
- Internet became first manifestation of a global network of networks
- In early Internet deployments, security was treated as a low priority

The Present

- The Internet brings millions of computer networks into communication with each other—many of them unsecured
- Ability to secure a computer's data influenced by the security of every computer to which it is connected
- The same problems apply for emerging networked computer systems, *e.g.*, smartphones

Summary

- Information security is a "well-informed sense of assurance that the information risks and controls are in balance."
- Security should be considered a balance between protection and availability.
- Computer security began immediately after first mainframes were developed