(CE372) INFORMATION AND CYBERSECURITY

Introduction

Instructor: Dr Eric Affum

Reading: Whitman and Mattord, Chaps. 1, 2

Course Outline

An introduction to security of digital information including:

- Attacks on Computers and Computer Security
- Cryptography: Concepts and Techniques
- Symmetric key Ciphers
- Asymmetric key Ciphers
- Message Authentication Algorithms and Hash Functions
- Authentication Applications
- E-Mail Security
- IP Security
- Web Security
- Intruders, Virus and Firewalls

Learning Objectives

Provide students with a high-level understanding of how information security functions in an organization

- Explain the objectives of information security
- Explain the importance and application of each of confidentiality, integrity, authentication and availability
- Understand various cryptographic algorithms.
- Understand the basic categories of threats to computers and networks
- Describe public-key cryptosystem.
- Describe the enhancements made to IPv4 by IPSec
- Understand Intrusions and intrusion detection
- Discuss the fundamental ideas of public-key cryptography.
- Generate and distribute a PGP key pair and use the PGP package to send an encrypted e-mail message.
- Discuss Web security and Firewalls

Texts

TEXT BOOKS:

- Cryptography and Network Security : William Stallings, Pearson Education,4^{11}i Edition
- Cryptography and Network Security : Atul Kahate, Mc Graw Hill, 2" Edition

REFERENCE BOOKS:

- Cryptography and Network Security: C K Shyamala, N Harini, Dr T R Padmanabhan, Wiley India, lst Edition.
    - Cryptography and Network Security : Forouzan Mukhopadhyay, Mc Graw Hill, 2"d Edition
    - Information Security, Principles and Practice: Mark Stamp, Wiley India.
    - Principles of Computer Sceurity: WM.Arthur Conklin, Greg White, TMH
    - Introduction to Network Security: Neal Krawetz, CENGAGE Learning
    - Network Security and Cryptography: Bernard Menezes, CENGAGE Learning

Course Assessment

Grading System	Factor	Weight	Location	Date	Time
	Exercises	15 %	In class/HW		
	Attendance	10 %	In class		
	Quizzes	15 %	In class	Date to be Announced	2 Hrs
	Final Exam	60 %	(TBA)	Date to be Announced	3 Hrs

80-100% = A, 70-79.9%=B, 60-69.9%=C, 50-59.9%=D, 0-49.9%=Fail

What is an Information System?

- Information System (IS): an entire set of
  - **Software**
  - **Hardware**
  - **Data**
  - **People**
  - **Procedures,** and
  - **Networks**

necessary to use information within an organization

Critical Characteristics of Information

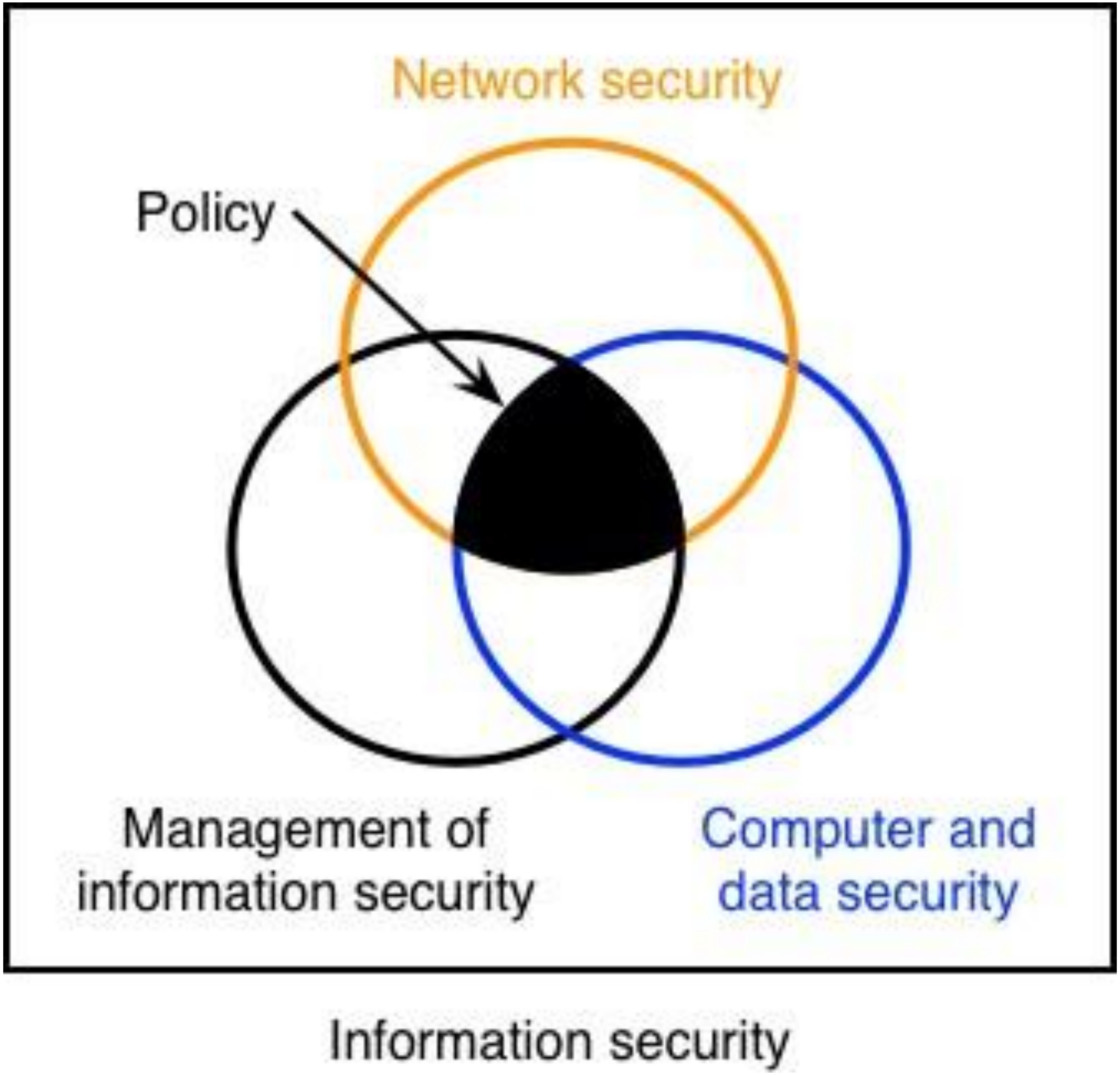
- The value of information comes from its characteristics:
  - **Confidentiality:** self-explanatory
  - **Integrity:** identical to the original/expected state/can be trusted
  - **Availability:** of info, services, etc.
  - **Authenticity**: “it is what it claims to be”
  - **Accuracy:** free from mistakes and errors
  - **Utility:** How data is useful for end purpose/data value
  - **Possession:** state of ownership/control
- Others:
  - User authentication: users are who they claim to be
  - Auditability: there’s a record of who accessed what
  - Non-repudiation: one cannot claim “I didn’t sign this”

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”
- Successful companies should have multiple security “tiers”:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - ***Information security***

What is Information Security?

- Protection of information and its critical elements, including systems that use, store, and transmit that info
- Necessary tools:
  - ***Policy***
  - ***Awareness***
  - ***Training***
  - ***Education***
  - ***Technology***


Network security
Policy
Management of information security
Computer and data security
Information security

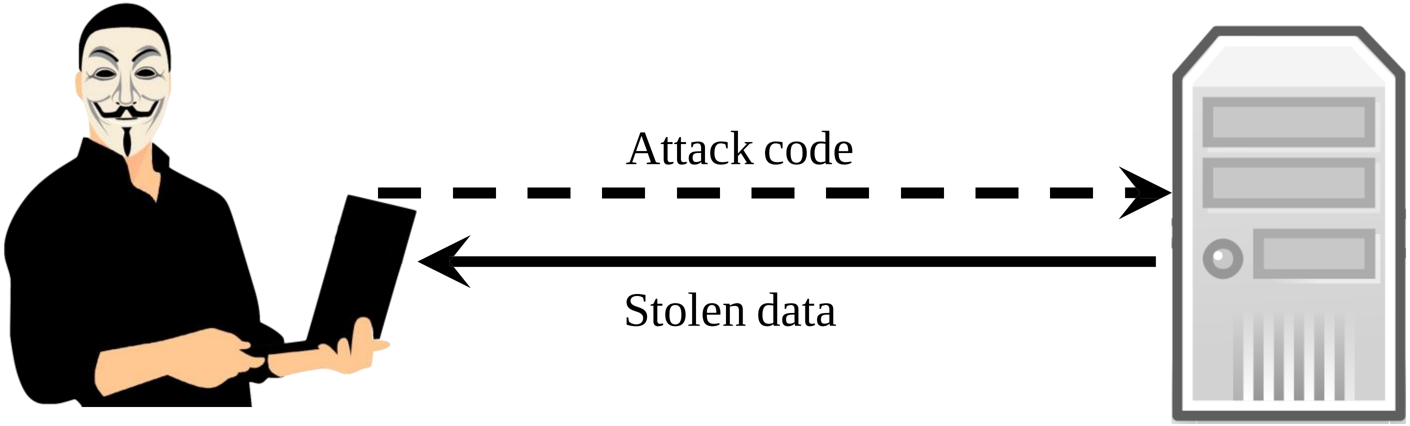
Aspects of Information Security (after Fig. 1.3 in book)

Securing Components in an Information System

- Computers (software and hardware): key components in an IS

- Computers can be subjects and/or objects of an attack:
  - Subject of an attack: attackers use computers actively to launch attacks against targets
  - Object of an attack: computers are what are under attack!

Computers: Subjects/Objects of Attack



Attack code

Stolen data

Hacker using computer to
conduct attack (*subject* of attack)

Server with private info
(*object* of attack)

Computer as Subject/Object of Attack (after Fig. 1.6 in book).
Source: publicdomainpictures.net, Tango icon set

Balancing Information Security and Access

- Impossible to obtain perfect security: it’s 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

Security vs. Access

Security

- CIO: Two-factor authentication is necessary to protect private data
- Auditor: We need to comply with laws/regulations

…

Access

- Student 1: I forgot my authentication device
- Student 2: It's a hassle

…

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

The 1960s

- Advanced Research Procurement Agency (ARPA) began to examine feasibility of redundant networked communications

- Larry Roberts developed ARPANET from its inception

The 1970s and 1980s

- 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, IoT devices)

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