CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

PART I: CRYPTOGRAPHY

1. INTRODUCTION

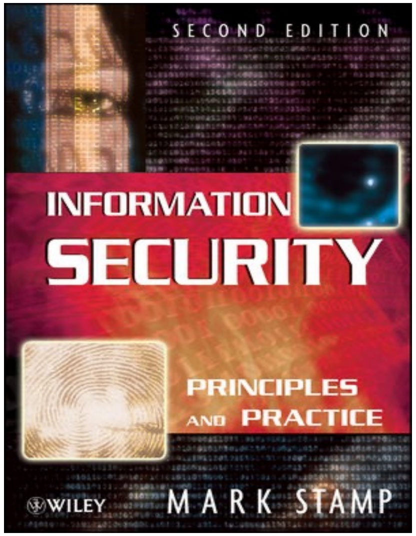
Information Security

Instructor:

Dr. Ibrahim Ali Almerhag

almerhag.wordpress.com

Textbook:



- Information Security: Principles and Practices, Mark Stamp, J. Wiley & sons; 2 edition ,2011.

References:

- Understanding Cryptography: A Textbook for Students and Practitioners., Paar, Pelzl, 1st edition, Springer, 2009.
- Cryptography and Network Security: Principles and Practice, William Stallings, Pearson; 6 edition ,2013.

Course Outline

This module consists of

- an introduction to classical & modern cryptography and network security.
- The concepts of block ciphers and message authentication codes
- public key encryption, digital signatures, and key establishment
- How cryptographic algorithms and protocols work.
- as well as common examples and uses of such schemes.

Introduction

- *Alice and Bob are the* ***good guys***

- *Trudy is the* ***bad "guy"*** →

- *Trudy is our generic "intruder"*

Definitions

- ❑ *Computer Security - generic name for the collection of tools designed to protect data and to hinder hackers*
- ❑ *Network Security - measures to protect data during their transmission*
- ❑ *Internet Security - measures to protect data during their transmission over a collection of interconnected networks*

Basic Terminology

- ***plaintext*** *- original message*
- ***ciphertext*** *- coded message*
- ***cipher*** *- algorithm for transforming plaintext to ciphertext*
- ***encipher (encrypt)*** *- converting plaintext to ciphertext*
- ***decipher (decrypt)*** *- recovering ciphertext from plaintext*

Basic Terminology

- □ ***key*** *- info used in cipher known only to sender/receiver*
- □ ***cryptography*** *- study of encryption principles/methods*
- □ ***cryptanalysis (codebreaking)*** *- study of principles/ methods of deciphering ciphertext without knowing key*
- □ ***cryptology*** *- field of both cryptography and cryptanalysis*

Alice's Online Bank

- Alice opens "Alice's Online Bank" (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice's and Bob's concerns similar? How are they different?
- How does Trudy view the situation?

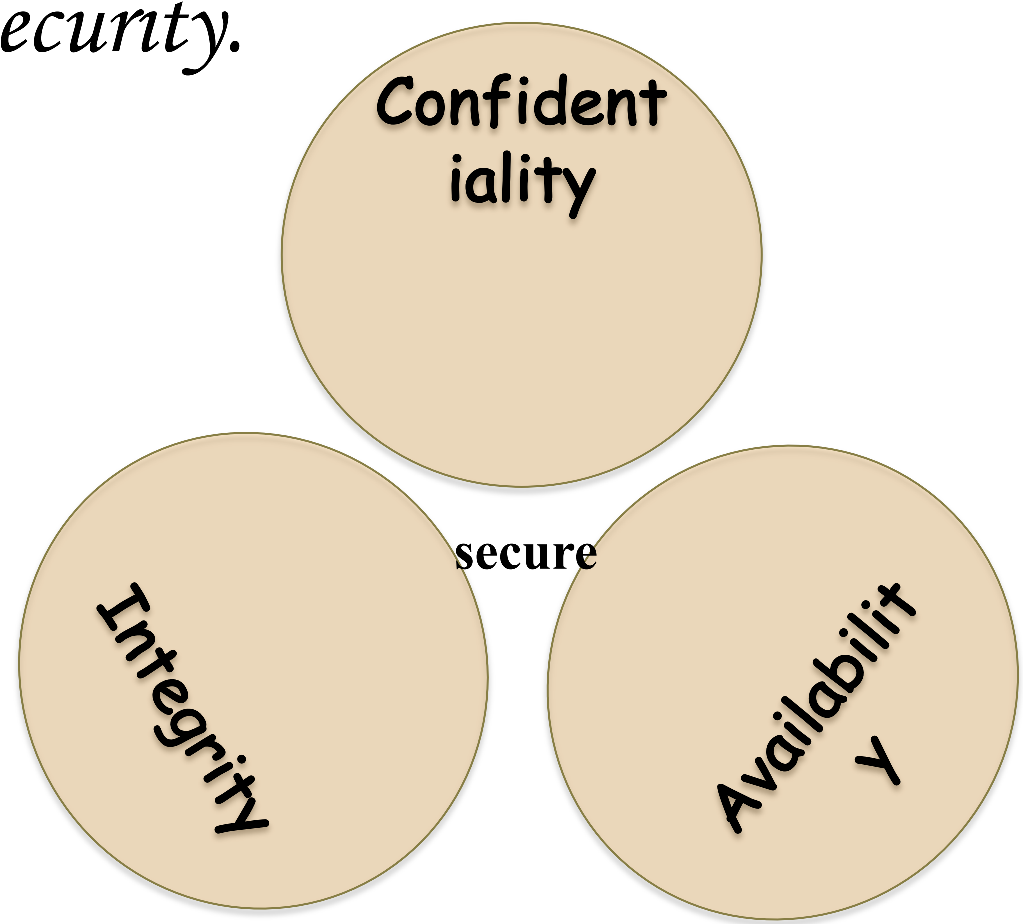
Security Goals

- ❑ There are three fundamental goals of information security.
- ❑ CIA ➔

  Confidentiality,

  Integrity, and

  Availability



Confidentiality

- *AOB must prevent Trudy from learning Bob's account balance*
- ***Confidentiality:** prevent unauthorized reading of information*
  - *Cryptography used for confidentiality*

Integrity

- Trudy must not be able to change Bob's account balance
- Bob must not be able to improperly change his own account balance
- Integrity: detect unauthorized *writing* of information
  - Cryptography used for integrity

Availability

- *AOB's information must be available whenever it's needed*
- *Alice must be able to make transaction*
  - *If not, she'll take her business elsewhere*
- ***Availability:*** *Data is available in a timely manner when needed*
- *Availability is a "new" security concern*
  - *Denial of service (DoS) attacks*

Beyond CIA: Crypto

- ❑ *How does Bob's computer know that "Bob" is really Bob and not Trudy?*
- ❑ *Bob's password must be verified*
  - ➢ *This requires some clever* ***cryptography***
- ❑ *What are security concerns of pwds?*
- ❑ *Are there alternatives to passwords?*

Beyond CIA: Protocols

- When Bob logs into AOB, how does AOB know that “Bob” is really Bob?
- As before, Bob’s password is verified
- Unlike the previous case, **network** security issues arise
- How do we secure network transactions?
  - **Protocols** are critically important
  - Crypto plays critical role in protocols

Beyond CIA: Access Control

- Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, etc.
- Enforcing these restrictions: *authorization*
- **Access control** includes both authentication and authorization

Beyond CIA: Software

- Cryptography, protocols, and access control are implemented in **software**
  - Software is foundation on which security rests
- What are security issues of software?
  - Real world software is complex and buggy
  - Software flaws lead to security flaws
  - How does Trudy attack software?
  - How to reduce flaws in software development?
  - And what about malware?

The People Problem

- People often break security
  - Both intentionally and unintentionally
  - Here, we consider the unintentional
- For example, suppose you want to buy something online
  - To make it concrete, suppose you want to buy *Information Security: Principles and Practice*, 2nd edition from amazon.com

The People Problem

- To buy from amazon.com
  - Your Web browser uses SSL protocol
  - SSL relies on cryptography
  - Access control issues arise
  - All security mechanisms are in software
- Suppose all of this security stuff works perfectly
  - Then you would be safe, right?

The People Problem

- What could go wrong?
- Trudy tries man-in-the-middle attack
  - SSL is secure, so attack doesn’t “work”
  - But, Web browser issues a warning
  - What do you, the user, do?
- If user ignores warning, attack works!
  - None of the security mechanisms failed
  - But user *unintentionally* broke security

Cryptography

- ❑ *"Secret codes"*
- ❑ *This topic covers*
  - o *Classic cryptography*
  - o *Symmetric ciphers*
  - o *Public key cryptography*
  - o *Hash functions++*

Access Control

- ❑ Authentication
  - o Passwords
  - o Biometrics
  - o Other methods of authentication
- ❑ Authorization
  - o Access Control Lists/Capabilities
  - o Firewalls, intrusion detection (IDS)
  - o Multilevel security (MLS), security modeling, covert channel, inference control

Protocols

- “Simple” authentication protocols
  - Focus on basics of security protocols
  - Lots of applied cryptography in protocols
- Real-world security protocols
  - SSH, SSL, IPSec, Kerberos
  - Wireless: WEP, GSM

Software

- ❑ Security-critical flaws in software
  - o Buffer overflow
  - o Race conditions, etc.
- ❑ Malware
  - o viruses and worms
  - o Prevention and detection

Software

- ❑ Software reverse engineering (SRE)
  - o How hackers "dissect" software
- ❑ Software and testing
  - o Open source, closed source, other topics
- ❑ Operating systems
  - o Basic OS security issues
  - o "Trusted OS" requirements

Think Like Trudy

- In the past, no respectable sources talked about "hacking" in detail
  - After all, such info might help Trudy
- Recently, this has changed
  - Lots of books on network hacking, evil software, how to hack software, etc.
  - Classes teach virus writing, SRE, etc.

Think Like Trudy

- Good guys must think like bad guys!
- A police detective…
  - …must study and understand criminals
- In information security
  - We want to understand Trudy's methods
  - Might think about Trudy's motives
  - We'll often pretend to be Trudy