CSE447: CRYPTOGRAPHY AND CRYPTANALYSIS
FALL 2024

PREPARED BY:

DR. MUHAMMAD IQBAL HOSSAIN

ASSOCIATE PROFESSOR

DEPARTMENT OF CSE, BRAC UNIVERSITY

BRAC
UNIVERSITY
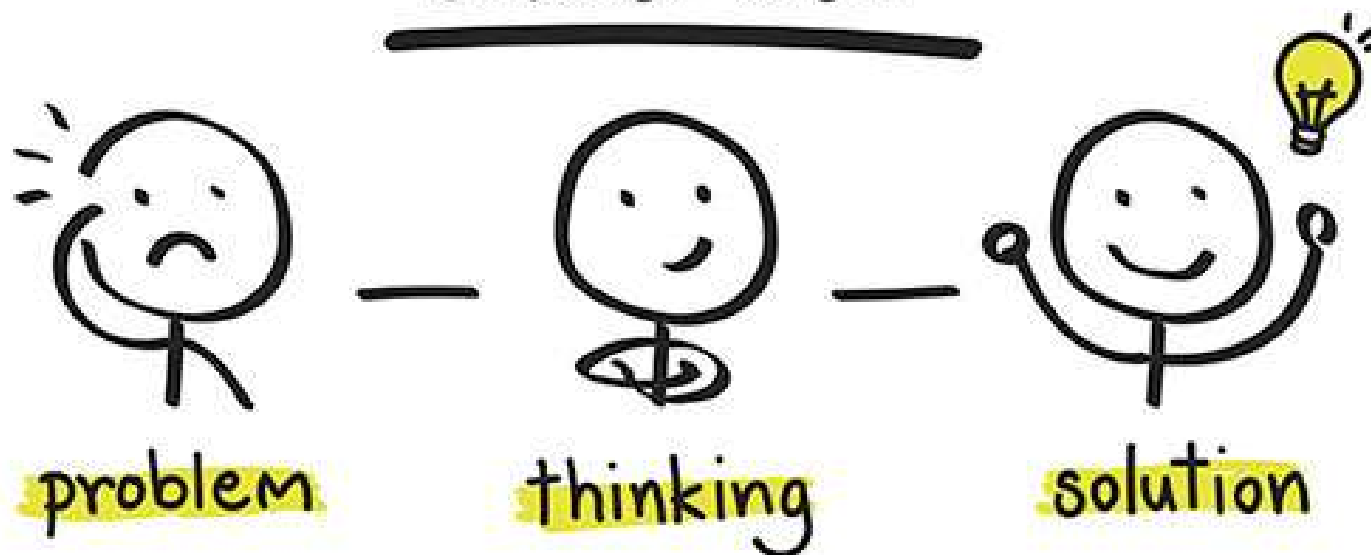
Inspiring Excellence

How to get A in this course???

CHAPTER 1 INTRODUCTION

- THE CAST OF CHARACTERS

- ALICE'S ONLINE BANK

- ABOUT THE TEXT BOOK

THE CAST OF CHARACTERS

○ Alice and Bob are the good guys

- Trudy is the bad guy

- Trudy is our generic "intruder"

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 and Bob concerns similar? How are they different?
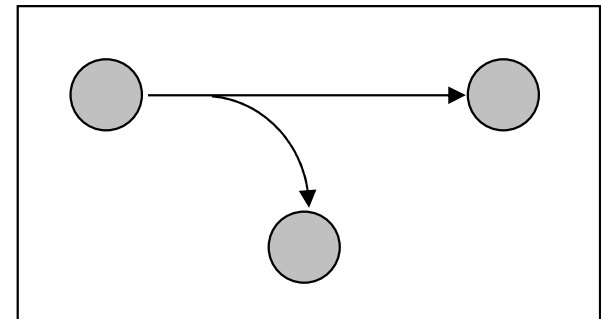
○ How does Trudy view the situation?

CIA

- CIA: Confidentiality, Integrity, and Availability

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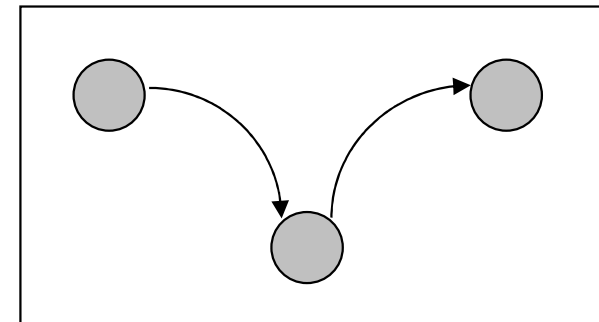 - Confidentiality: prevent unauthorized reading of information
 - Cryptography used for confidentiality

CIA

O Integrity

  O Trudy must not be able to change Bob's account
    balance

  O Bob must not be able to improperly change his
    own account balance

  O Integrity: prevent unauthorized writing of
    information

    O Cryptography used
       for integrity

CIA

○ Availability

  ○ AOB's information must be available when needed

  ○ Alice must be able to make transaction

    ○ If not, Bob'll take his business elsewhere

  ○ Availability: Data is available in a timely manner when needed

  ○ Availability is a "new" security concern

    ○ In response
to denial of service (DoS)
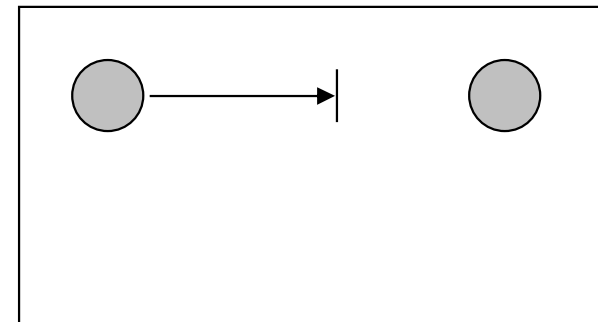
BEYOND CIA

○ CIA are only beginning of the Inf Sec.

○ Case 1: when Bob logs on his computer

   ○ 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

○ Case2: when Bob logs into AOB

   ○ how does AOB know that "Bob" is really Bob?

○ As before, Bob's password is verified

○ Unlike standalone computer case, network security issues arise

○ What are network security concerns?

○ Protocols are critically important

   ○ Crypto also important in protocols

BEYOND CIA

- 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 is known as authorization

- Access control includes both authentication and authorization

BEYOND CIA

○ Cryptography, protocols, and access control are implemented in software

○ What are security issues of software?

  ○ Most 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?

BEYOND CIA

○ Some software is intentionally evil
  ○ Malware: computer viruses, worms, etc.

○ How do the malwares work?

○ What can Alice and Bob do to protect themselves from malware?

○ What can Trudy do to make malware more "effective" ?

BEYOND CIA

○ Operating systems enforce security

    ○ For example, authorization

○ OS: large and complex software

    ○ Win XP has 40,000,000 lines of code!

    ○ Subject to bugs and flaws like any other software

    ○ Many security issues specific to OSs

    ○ Can you trust an OS?

TEXT BOOK

- The text consists of four major parts

  - Cryptography

  - Access control

  - Protocols

  - Software

- Note: Our focus is on technical issues

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 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 these security stuff works perfectly

  ○ What could possibly go wrong?

THE PEOPLE PROBLEM

○ What could go wrong?

○ Trudy can try man-in-the-middle attack

  ○ SSL is secure, so attack doesn't "work"

  ○ 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"

○ The book covers

   ○ Classic cryptography

   ○ Symmetric ciphers

   ○ Public key cryptography

   ○ Hash functions

   ○ Advanced cryptanalysis

ACCESS CONTROL

○ Authentication

    ○ Passwords

    ○ Biometrics and other

○ Authorization

    ○ Access Control Lists and Capabilities

    ○ Multilevel security (MLS), security modeling, covert channel, inference control

    ○ Firewalls and Intrusion Detection Systems

PROTOCOLS

○ Simple" authentication protocols
  ○ Focus on basics of security protocols
  ○ Cryptography used a lot in protocols
○ Real-world security protocols
  ○ SSH, SSL, IPSec, Kerberos

  ○ Wireless: WEP, GSM (Global System for Mobile communications)

SOFTWARE

- Software security-critical flaws
  - Buffer overflow
  - Other common flaws
    - Incomplete Mediation
    - Race Conditions
- Malware
  - Specific viruses and worms
  - Prevention and detection
  - The future of malware

SOFTWARE

- Software reverse engineering (SRE)
  - How hackers "dissect" software
- Digital rights management (DRM)
  - Shows difficulty of security in software
  - Also raises OS security issues
- Software and testing
  - Open source, closed source, other topics

SOFTWARE

- Operating systems
  - Basic OS security issues
  - "Trusted" OS requirements
  - NGSCB("n-scub): Microsoft's trusted OS for PC
    - Next Generation Secure Computing Base
- Software is a big security topic
  - Lots of material to cover
  - Lots of security problems to consider
  - But not nearly enough time available…

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 motives
  - We must know Trudy's methods
  - We'll often pretend to be Trudy

THINK LIKE TRUDY

○ Is all of this security information a good idea?

○ "It's about time somebody wrote a book to teach the good guys what the bad guys already know." ― Bruce Schneier

THINK LIKE TRUDY

○ We must try to think like Trudy

○ We must study Trudy's methods

○ We can admire Trudy's cleverness

○ Often, we can't help but laugh at Alice and Bob's stupidity

○ But, we **cannot act** like Trudy

　○ Except in this class…

IN THIS COURSE…

- Always think like the bad guy

- Always look for weaknesses

- Strive to find a weak link

- It's OK to break the rules

- Think like Trudy!

- But don't do anything illegal…