Chapter 1: Introduction

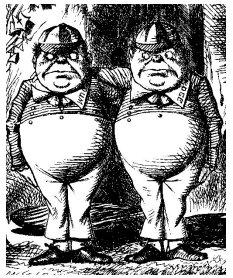
"Information security is a set of practices designed to keep personal data secure from unauthorized access and alteration during storing or transmitting from one place to another.."

—Infoguard Cyber security

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's and Bob's concerns similar? How are they different?
- How does Trudy view the situation?

CIA

- CIA == Confidentiality, Integrity, and Availability
- AOB must prevent Trudy from learning Bob's account balance
- **Confidentiality:** prevent unauthorized *reading* of information
  - Cryptography used for confidentiality

CIA

- 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

CIA

- 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 a relatively new security issue
  - Denial of service (DoS) attacks

Beyond CIA: Crypto (authentication)

- 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 a major role in security protocols

Beyond CIA: (authorization)

- 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, and so on…
- Enforcing such restrictions: *authorization*
- **Access control** includes both authentication and authorization

Beyond CIA: Software

- Cryptography, protocols, and access control are all 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?

Your Textbook

- The text consists of four major parts
  - Cryptography
  - Access control
  - Protocols
  - Software
- We'll focus on mechanics

Cryptography

- "Secret codes"
- The book covers
  - Classic cryptography
  - Symmetric ciphers
  - Public key cryptography
  - Hash functions
  - Advanced cryptanalysis

Access Control

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

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
  - Buffer overflow
  - Race conditions, etc.
- Malware
  - Examples of viruses and worms
  - Prevention and detection
  - Future of malware?

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
  - We might think about Trudy's motives
  - We'll often pretend to be Trudy