CSE 5/7339
Computer System Security

Mark D. Hoffman
mhoffman@smu.edu
Office Hours: By Appointment

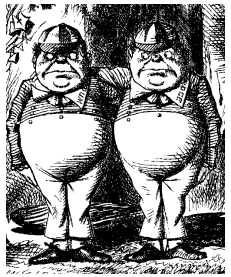
Chapter 1: Introduction

"Begin at the beginning," the King said, very gravely,
"and go on till you come to the end: then stop."
— Lewis Carroll, *Alice in Wonderland*

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

机密的

- CIA == Confid~~entiality~~, 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
- Bob must be able to make transactions
  - 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?

恶意软件

Your Textbook

- 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 *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?

Your connection is not private

Attackers might be trying to steal your information from **192.168.1.1** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically report details of possible security incidents to Google. Privacy policy

Hide advanced

Back to safety

This server could not prove that it is **192.168.1.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.1.1 (unsafe)

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"
- 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/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?

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: Microsoft's trusted OS for the PC
- 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

- 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

Think Like Trudy

- Is all of this security information a good idea?
- Bruce Schneier (referring to *Security Engineering*, by Ross Anderson):
  - "It's about time somebody wrote a book to teach the good guys what the bad guys already know."

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's and/or Bob's stupidity
- But, we **cannot** act like Trudy
  - Except in this class…

In This Course…

- Think like the bad guy
- Always look for weaknesses
  - Find the *weak link* before Trudy does
- It's OK to break the rules
  - What rules?
- Think like Trudy
- But don't do anything illegal!