信息安全基础

课程性质：专业选修课　　学时数：32学时

厚 德 健 行

课　程　介　绍

厚 德 健 行

课程大纲

- 第一部分：加解密
- 第二部分：访问控制
- 第三部分：网络与软件安全

角色列表

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

- Trudy is the **bad "guy"**

- Trudy is our generic "intruder"

Alice的网上银行

- 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/Control Access 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/Control Access used for integrity

- 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: 密码

- 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: 协议

- 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: 访问控制

- 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: 软件

- 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 technical issues
- But, people cause lots of problems…

The People Problem

- People often break security
  - Both intentionally and unintentionally
  - Here, we consider an unintentional case
- For example, suppose you want to buy something online
  - Say, *Information Security: Principles and Practice*, 3rd edition from amazon.com

Cryptography

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

- 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?

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

- 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…

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

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 …
  - … and even then, there are limits

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!

关注我，下节内容更精彩：
第一章：加解密