CS 356 - System Security
Mid-Semester Review

Spring 2016
Mid-Term Exam

- Thursday, 2:00 – 3:15
- you may bring one 8-1/2 x 11 sheet of paper with any notes you would like
- no cellphones
- Calculator allowed; prefer symbolic answers to show your thinking

- This is to assess your understanding of the material covered. There will be concepts, terminology and problems to be solved

- Since you need to study, there will be no homework assigned this week
Suggestions all in 75 minutes...

- Pass 1: Skim Test Quickly – then do easy parts first to build confidence
  - Some questions will take just a few seconds
  - Some questions will take many minutes
- Pass 2: Beginning to End: do what you can, skip hard stuff for now
- Pass 3: Go back and do the stuff you skipped
- Pass 4: Double-check answers; did you circle true or false?

- ANSWERS SHOULD BE BRIEF; Even T/F requires a brief explanation or no credit given
Essential Terminology

• Integrity
  – Guard against improper information modification or destruction

• Confidentiality:
  – Preserve authorized restrictions on information access and disclosure

• Availability
  – Ensure time and reliable access to and use of information

• Authenticity
  – Verifying that users are who they and that the transmission was valid

• Accountability
  – Actions of an entity can be traced uniquely to that entity
Chapter 1 Summary

- Computer security concepts
  - Definition
  - Challenges
  - Model
- Threats, attacks, and assets
  - Threats and attacks
  - Threats and assets
- Security functional requirements
- Fundamental security design principles
- Attack surfaces and attack trees
  - Attack surfaces
  - Attack trees
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation
Chapter 2 Summary

• Confidentiality with symmetric encryption
  § Symmetric encryption
  § Symmetric block encryption algorithms
  § Stream ciphers

• Message authentication and hash functions
  § Authentication using symmetric encryption
  § Message authentication without message encryption
  § Secure hash functions
  § Other applications of hash functions

• Random and pseudorandom numbers
  § The use of random numbers
  § Random versus pseudorandom

• Public-key encryption
  § Structure
  § Applications for public-key cryptosystems
  § Requirements for public-key cryptography
  § Asymmetric encryption algorithms

• Digital signatures and key management
  § Digital signature
  § Public-key certificates
  § Symmetric key exchange using public-key encryption
  § Digital envelopes
Chapter 3 Summary

• Electronic user authentication principles
  – A model for electronic user authentication
  – Means of authentication
  – Risk assessment for user authentication

• Password-based authentication
  – The vulnerability of passwords
  – The use of hashed passwords
  – Password cracking of user-chosen passwords
  – Password file access control
  – Password selection strategies

• Token-based authentication
  – Memory cards
  – Smart cards
  – Electronic identity cards

• Biometric authentication
  – Physical characteristics used in biometric applications
  – Operation of a biometric authentication system
  – Biometric accuracy

• Remote user authentication
  – Password protocol
  – Token protocol
  – Static biometric protocol
  – Dynamic biometric protocol

• Security issues for user authentication
Chapter 4 Summary

• Access control principles
  – Access control context
  – Access control policies

• Subjects, objects, and access rights

• Discretionary access control
  – Access control model
  – Protection domains

• UNIX file access control
  – Traditional UNIX file access control
  – Access control lists in UNIX

• Role-based access control
  – RBAC reference models

• Attribute-based access control
  – Attributes
  – ABAC logical architecture
  – ABAC policies

• Identity, credential, and access management
  – Identity management
  – Credential management
  – Access management
  – Identity federation

• Trust frameworks
  – Traditional identity exchange approach
  – Open identity trust framework

• Bank RBAC system
Chapter 5 Summary

• The need for database security
• Database management systems
• Relational databases
  – Elements of a relational database system
  – Structured Query Language
• SQL injection attacks
  – A typical SQLi attack
  – The injection technique
  – SQLi attack avenues and types
  – SQLi countermeasures
• Inference

• Database access control
  – SQL-based access definition
  – Cascading authorizations
  – Role-based access control
• Database encryption
Chapter 6 Summary

• Types of malicious software (malware)
• Advanced persistent threat
• Propagation
  – Infected content
    • viruses
  – Vulnerability exploit
    • worms
  – Social engineering
    • spam
    • e-mail
    • Trojans

• Payload
  – System corruption
  – Attack agent
    • Zombie
    • Bots
  – Information theft
    • Keyloggers
    • Phishing
    • Spyware
  – Stealthing

• Countermeasures