Mid-Term Exam

• Thursday, 9:30 - 10:45
• you may bring one 8-1/2 x 11 sheet of paper with any notes you would like
• no cellphones, calculators

• 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
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 2: Cryptographic Tools

- introduced cryptographic algorithms
- symmetric encryption algorithms for confidentiality
- message authentication & hash functions
- public-key encryption
- digital signatures and key management
- random numbers
Chapter 3: User Authentication

The four means of authenticating user identity are based on:

<table>
<thead>
<tr>
<th>Something the Individual Knows</th>
<th>Something the Individual Possesses (Token)</th>
<th>Something the Individual Is (Static Biometrics)</th>
<th>Something the Individual Does (Dynamic Biometrics)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password, PIN, answers to prearranged questions</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smartcard, electronic keycard, physical key</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint, retina, face</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Voice pattern, handwriting, typing rhythm</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Chapter 3: User Authentication

- **four means of authenticating a user’s identity**
  - something the individual knows
  - something the individual possesses
  - something the individual is
  - something the individual does

- **vulnerability of passwords**
  - offline dictionary attack
  - specific account attack
  - popular password attack
  - password guessing against single user
  - workstation hijacking
  - exploiting user mistakes
  - exploiting multiple password use
  - electronic monitoring

- **hashed password and salt value**
- **password file access control**

password selection strategies
  - user education
  - computer generated passwords
  - reactive password checking
  - proactive password checking

Bloom filter
  - token based authentication
  - memory cards
  - smart cards

biometric authentication
  - remote user authentication
  - password protocol
  - token protocol
  - static biometric protocol
  - dynamic biometric protocol
DNS & DNSSEC

- DNS is essential internet service
- Very little security
- Cache Poisoning
  - Kaminsky attack

- DNSSEC - security extensions for DNS
- adds authentication to existing DNS protocol via new record types employing crypto RRSIG, DNSKEY, NSEC
- DNS Signing
- DNS Validating
- Trust Anchor (root of trust)
- Chain of Trust: DS record
Chapter 4: Access Control

- introduced access control principles
  - subjects, objects, access rights
- discretionary access controls
  - access matrix, access control lists (ACLs), capability tickets
  - UNIX traditional and ACL mechanisms
- role-based access control
- case study
Chapter 5

• Data Base Security not discussed, not on exam
Chapter 6: Malicious Software

- types of malicious software (malware)
- terminology for malicious software
- viruses – infected content
  - infection mechanism, trigger, payload
  - dormant, propagation, triggering, and execution phases
  - boot sector infector, file infector, macro virus, and multipartite virus
  - encrypted, stealth, polymorphic, and metamorphic viruses
- worms – vulnerability exploit
  - replicates via remote systems
  - e-mail, file sharing, remote execution, remote file access, remote login capability
  - scanning/fingerprinting
- spam e-mail/trojans – social engineering
- payload – system corruption
  - data destruction, real world damage
  - ransomware, logic bomb

- payload – attack agent
  - bots
  - remote control facility

- payload – information theft
  - credential theft, keyloggers, spyware
  - phishing, identity theft

- payload – stealthing
  - backdoor/trapdoor
  - rootkit
  - kernel mode rootkits
  - virtual machine/external rootkits

- countermeasures
  - prevention
  - detection, identification, removal
  - host based scanners/behavior blocking software
  - digital immune system
IP Hijacking

• If this is on the exam, the ONLY area I will consider as valid for questions are in the first 5 slides:

• definition of IP hijacking

• Consequences of IP hijacking: blackhole, eavesdrop, impersonation, spam, etc.
Chapter 7: Denial of Service

- introduced denial of service (DoS) attacks
- classic flooding and SYN spoofing attacks
- ICMP, UDP, TCP SYN floods
- distributed denial of service (DDoS) attacks
- reflection and amplification attacks
- defenses against DoS attacks
- responding to DoS attacks