20-ECES-653  NETWORK SECURITY


References:
8. Feldmeier and Karn, UNIX Password Security – Ten Years later, Crypto89

Coordinator: John Franco, Professor, Computer Science

Knowledge and Comprehension Goals:
1. What a secret key cryptosystem is
2. What a public key cryptosystem is
3. What a message digest is
4. What stream and block ciphers are
5. How to implement message integrity, confidentiality and authentication
6. Some of the mathematics behind the crypto algorithms discussed

Application Goals:
The student will be able to:
1. Implement RSA, HMAC, Diffie-Hellman, Fiat-Feige-Shamir algorithms in Java.
2. Use network security principles to protect a complex system.
3. Use certificates to authenticate some party.
4. Use an asymmetric block cipher (Karn) to encrypt.

Prerequisites by Topic:
The usual programming courses that a senior will have taken including 20-CS-229, Software Development in C++ and 15-MATH-253, Calculus 3. The student is expected to know what Object Oriented Programming is and is expected to have significant programming experience in OOP, especially using C++.

Topics:
1. Introduction: Firewalls, Viruses, Hashes, Message Digests, etc
2. Cryptography: Secret Key Algorithms (DES, 3DES, AES, IDEA)
3. Cryptography: Hashes and Message Digests (SHA and variants)
4. Cryptography: Public Key Algorithms: (RSA, ECC, DH, Zero-knowledge)
5. Authentication, Handshake Pitfalls
6. Review and Exam
7. Kerberos
8. IPSec+IKE
9. SSL/TLS
10. PEM, PGP, GPG, etc.

Contributions to CS

Student Outcomes:

(a) an ability to apply knowledge of mathematics, science, and engineering

(i) a recognition of and an ability to engage in life-long learning

(j) a knowledge of contemporary issues

Outcomes × Goals and Primary Assessment Methods:

<table>
<thead>
<tr>
<th>Goal</th>
<th>(a)</th>
<th>(i)</th>
<th>(j)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know-1</td>
<td>HW</td>
<td>Project</td>
<td></td>
</tr>
<tr>
<td>Know-2</td>
<td>HW</td>
<td>Project</td>
<td></td>
</tr>
<tr>
<td>Know-3</td>
<td>HW</td>
<td>Project</td>
<td></td>
</tr>
<tr>
<td>Know-4</td>
<td>HW</td>
<td>Project</td>
<td></td>
</tr>
<tr>
<td>Know-5</td>
<td>HW</td>
<td>Project</td>
<td></td>
</tr>
<tr>
<td>Know-6</td>
<td>HW</td>
<td>Project</td>
<td></td>
</tr>
<tr>
<td>App-1</td>
<td></td>
<td></td>
<td>Project</td>
</tr>
<tr>
<td>App-2</td>
<td></td>
<td></td>
<td>Project</td>
</tr>
<tr>
<td>App-3</td>
<td></td>
<td></td>
<td>Project</td>
</tr>
<tr>
<td>App-4</td>
<td></td>
<td></td>
<td>Project</td>
</tr>
</tbody>
</table>

Computer Usage: Four homeworks and project

Area Coverage:  

<table>
<thead>
<tr>
<th>AREA</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithms</td>
<td>5</td>
</tr>
<tr>
<td>Data Structures</td>
<td>1</td>
</tr>
<tr>
<td>Computer Organization and Architecture</td>
<td>0</td>
</tr>
<tr>
<td>Software Design</td>
<td>6</td>
</tr>
<tr>
<td>Concepts of Programming Languages</td>
<td>0</td>
</tr>
</tbody>
</table>

Laboratory Projects: Final project that counts as a final examination

Prepared by: John Franco., Ph.D.  

Date: June 2009