CSC 4601: Computer and Network Security

Credit Hours: 3 hours

Prerequisites:
CSC 3102

Prerequisites by Topics:
Fundamentals of algorithm design techniques; strategies to compare relative efficiency of algorithms.

Catalog Course Description:
Information security’s role, threats, elements of cryptography; protocols, architectures, and technologies for secure systems and services.

Course Outcomes:
Provide students with a high-level understanding of how information security functions in an organization. Topics will be both business and technology-centric.
- To master information security governance, and related legal and regulatory issues,
- To master understanding external and internal threats to an organization,
- To be familiarity with information security awareness and a clear understanding of its importance,
- To be familiar with how threats to an organization are discovered, analyzed, and dealt with,
- To master fundamentals of secret and public cryptography,
- To master protocols for security services,
- To be familiar with network security threats and countermeasures,
- To be familiar with network security designs using available secure solutions (such as PGP, SSL, IPSec, etc),
- To be familiar with advanced security issues and technologies (such as DDoS attack detection and containment, and anonymous communications),
- To be exposed to original research in network security,
- To be exposed to the importance of integrating people, processes and technology.

Texts and Other Course Materials

Major Topics

- Primer – information security and network basics
- Information Security and its role in an organization
- Threats Internal – Employees, Contractors, Third parties
- External – Criminals, Corporate Espionage, Hackers, Cyber Warfare, Cyber Terrorism
- Vulnerability Assessment
- Intrusion Detection
- Classic ciphers, modern ciphers and stream ciphers
- One-way functions
- Secret key (symmetric): DES, IDEA, AES,
- Confidentiality Using Symmetric Encryption,
- Public key (asymmetric): RSA
- Key distribution and management: PKI
- Hashes and Message Digests, Non-repudiation and digital signatures: MD5
- Authentication and its protocols: Kerberos
- Real Real-time Communication Security
- Securing Applications: Web security: digital cash, secure network transaction and SSL
- Securing Network Systems: IP security and VPN: IPSec, Firewall
- DDoS attack and its defense: types of DDOS attacks, intrusion detection, trace-back and attack containment, Anonymous communication, Wireless security

Assignments/Projects/Laboratory Projects/Homework

- Individual written homework assignments (4-6). Each homework consist of various problems, including those from the exercises of the text book. Sample problems:
  - Finding security weakness on algorithms and protocols
  - Quantifying the strength of security algorithms and protocols
  - Design elements of security protocols
- Laboratories on Public Key Security (2). Sample labs:
  - Experimenting with RSA, Encryption – Decryption
  - Key Management, Key Recovery, Key Escrow

Curriculum Category Content (estimated in semester hours)
### Relationship to Criterion 3 Outcomes

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

Math and Fundamentals -- 3hr core/2hr advanced:

Differential Cryptanalysis, Linear Cryptanalysis, Birthday Problem, Random Numbers, Pseudorandom Number Generator, Modular Arithmetic, Prime Numbers, Prime Factorization, Fermat’s Theorem, Totient Function, Modular Exponentiation, Factorization Problem, Elliptic Curve Cryptography.

Data Structures:

Algorithms and Software-- 30hr core/13hr advanced:

Modern Block Ciphers, Confusion and Diffusion, DES, Modes of Operations, ECB, CBC, CFB, OFB, CTR, 3DES, IDEA, AES, Hashes, MD2, MD5, SHA, Key Distribution, RSA, Diffie-Hellman Key Exchange Key, DSS, Key Management, Distribution of Public Keys, Authentication Protocols, Kerberos, Public Key Infrastructure – PKI, X. 509 authentication and certificates, IPsec – AH - ESP – Key management, Web Security - SSL, TLS, SET.

Computer Organization and Architecture:

Concepts of Programming Languages:

Social and Ethical Issues:

Oral Communication (presentations)

Written Communication:
Graduate students are required to prepare a project on various topics of security. The written presentation is around 10-15 page.

Students are required to submit 4-6 written home works and two labs involving discussions of security issues.

Course Coordinator: Dr. Arjan Durresi
Last Modified: May 9, 2007