

EECE 655 – Internet Security

Catalog description:

The course covers topics in Internet security. The course discusses security threats, vulnerabilities of protocols and the different types of attacks. Preventive and defensive mechanisms are covered; such as: e-mail security, web security, IP security, network management security, wireless security, intrusion detection techniques, firewalls, VPNs and tracing the source of attacks. The course briefly introduces the basics of cryptography and its application to network security. Student projects will be composed of implementation, simulation and research components.

Credit hours: 3 credits

Required or elective: Elective for ECE and CCE students

Prerequisites: By course: EECE 450, By topic: Internet protocols (IP, TCP, UDP, ARP, DNS, DHCP), internet routing, basic knowledge of socket programming.

Textbook(s) and/or required materials:

Material will be placed on reserve and posted on Moodle.

References:

- William Stallings, Network Security Essentials: Applications and Standards, Prentice-Hall, Third edition, 2007.
- Herbert Thompson and Scott Chase, The Software Vulnerability Guide, Charles River Media, 2005.
- Keith Jones, Richard Bejtlich, Curtis Rose, Real Digital Forensics: Computer Security and Incident Response, Addison Wesley, 2006.

Computer usage: Programming language of student's choice. Local and wide area network.

Course Objectives

| <i>The objectives of this course are to:</i> | <i>Correlates to program objectives</i> |
|---|---|
| Provide advanced knowledge of Internet security threats, vulnerabilities of protocols and the different types of attacks | 1 and 4 |
| Provide advanced knowledge of protocols, devices and tools used in securing networked applications and systems | 1 |
| Provide knowledge of algorithms used in securing networking applications including encryption, hash functions, digital signatures and key management. | 1 |
| Provide advanced knowledge of current research topics and issues in Internet security | 1 |
| Provide experience in conducting and presenting a literature review on a research topic | 1 and 3 |
| Provide hands-on experience in analyzing and securing networked systems | 1, 2 and 3 |

Course Topics

| <i>No.</i> | <i>Subjects covered</i> | <i>75 min. lectures</i> |
|------------|---|-------------------------|
| 1 | Introduction: Internet security threats, economic impact and terminology | 1 |
| 2 | Vulnerabilities of Internet protocols: ARP, IP, TCP, DNS and routing | 2 |
| 3 | Attacks: ARP cache poisoning, Packet sniffing, IP Spoofing, IP fragmentation attacks, ICMP attacks, TCP session hijacking, SYN flooding attack, Denial of service attacks, IP Routing attacks, DNS attacks, Port scanning, Cookie poisoning, Signature identification, Buffer overflow and SQL injection. | 6 |
| 4 | Finding and fixing some of the vulnerabilities | 2 |
| 5 | Cryptography and its Applications: Authentication, Digital signatures and Key management. | 3 |
| 6 | Security Protocols: PGP, S/MIME, SSL, IPsec, and SNMP | 6 |
| 7 | Security Prevention and Detection: Firewalls, VPNs and intrusion detection systems | 4 |

| | | |
|---|---|---|
| 8 | Attack source tracing and digital forensics | 2 |
|---|---|---|

Course Learning Outcomes

| At the end of the course, students should be able to: | Correlates to program outcomes* | | |
|--|---------------------------------|---------|---|
| | H | M | L |
| Assess Internet security threats | a, o | | |
| Estimate and assess the economic impact of network attacks | a, h | f | o |
| Describe the vulnerabilities in internetworking protocols | o | | |
| Describe the different Internet attacks | o | | |
| Find and identify potential vulnerabilities in internets | a, k, o | b | |
| Describe how to resolve identified vulnerabilities | a, k, o | | |
| Describe cryptography and its use in Internet security | a | k, o, n | |
| Describe the different security protocols used in email, web and other Internet applications | n | o | |
| Describe tools used for the prevention and detection of Internet attacks | k | o | |
| Trace the source of some types of Internet attacks | a | b | o |
| Conduct, document and present a literature review on a topic related to Internet security | e, i, j | g | |
| Analyze and secure an internetworked system | a, b, g, k | o | c |

* H: High correlation, M: Medium correlation, L: Low correlation

Class/laboratory schedule: Two 75-minute lectures per week. Use of computer lab is needed for working on the projects.

Evaluation methods

| | |
|-------------------------------|-----|
| 1. Participation/Office Hours | 1% |
| 2. Assignments | 25% |
| 3. Quizzes | 10% |
| 4. Project | 30% |
| 5. Final Exam | 34% |

Professional component

| | |
|---------------------------------|------|
| Engineering topics: | 100% |
| General education: | 0% |
| Mathematics and basic sciences: | 0% |

Person(s) who prepared this description and date of preparation

Imad H. Elhaji and Ayman Kayssi, March 2007.

Date of last revision

N/A