Applied Cryptography and Information Systems Security

Overview

This class examines applied cryptographic services, mechanisms, and applications as well as their related threats within an enterprise context. Specific cryptographic services include confidentiality, integrity, authentication, and nonrepudiation. Specific mechanisms include encryption, message authentication codes, digital signatures and digital certificates Specific applications include: Public Key Infrastructure (PKI), secure protocols, and virtual private networks (VPNs). Counter-measures including network monitoring and intrusion detection are also examined.

Intrusion detection systems can detect and limit potential system compromises. Since these systems provide a historical record of network and system events, they can also provide assurance that an enterprise's infrastructure has not been compromised.

Laboratory exercises provide an opportunity to apply class concepts. Laboratory activities include: encryption/decryption, file integrity testing, secure key exchange, Public Key Infrastructure, system, network, and vulnerability scanning. Other lab activities relate to secure protocols and Virtual Private Networks (VPNs).

Objectives

Upon successful completion of this course, you will be able to

1. List and define major cryptographic services and mechanisms.
2. Define relevant cryptographic terms including random number, private key, public key, public key infrastructure, trusted third party and cryptanalysis.
3. Name, explain and utilize major algorithms including MD5, SHA1, RC4, DES, AES and RSA.

4. Compare and contrast symmetric and asymmetric cryptography. For each, explain the relevant cryptographic services.
5. Define key management. Explain the “key management problem”.
6. Define and explain Public Key Infrastructure (PKI) principles and components.
7. Explain PKI management and policy.
8. Implement and utilize secure key exchange with certificates.
9. List and explain secure protocols including Secure Socket Layer (SSL) and IPSec.
10. Define and implement a VPN.
11. Define and explain Kerberos.
12. List and define major cryptographic vulnerabilities.
13. Define and explain major attacks on cryptography.
14. Articulate primary computer and network system threats.
15. Plan and execute an enterprise level vulnerability scan.
16. Define and demonstrate basic Intrusion Detection Systems concepts.
17. Explain Network security monitoring.
18. Analyze N-tier application vulnerabilities.

Texts

Required

Tjaden; Fundamentals of Secure Computer Systems; Franklin, Beedle & Associates; 2004, ISBN 1-887902-66-X.

Mell, H.X., Baker, D., Cryptography Decrypted, Pearson Education, 2001, ISBN-10 0201616475.

NIST Manuals

Barker,Barker,and Lee; Guideline for Implementing Cryptography In the Federal Government; NIST SP-800-21; 2005.

Frankel et.al.; Guide to IPsec VPNs; NIST; 2005

Kuhn et.al.; Introduction to Public Key Technology and the Federal PKI Infrastructure; NIST; 2001.

Recommended

Ferguson and Schneier; Practical Cryptography; Wiley; 2003; ISBN 0-471-22357-3.

McNab; Network Security Assessment; O'Reilly; 2004; ISBN 059600611-X.

Note *Recommended texts don't need to be purchased. Required text will be supplemented with instructor notes and outside readings.*

Evaluation

Exams/Quizzes	35%
Class Portfolio	25%
Lab Narrative	15%
Poster	10%
Activities/Journal	15%

Projects, Labs, and Activities

There will be frequent class discussions, as well as group labs and/or other "Hands On" activities. Since these are participatory activities, students not present do not participate. Students not participating cannot earn credit. Participatory activities cannot be made up at a later date. Students that cannot attend class should drop.

Each class period may include informal writing assignments.

Instructor	**Office**
Crowley	T2, Room 331
Phone: 713-743-4096 E-mail: Crowleye@yahoo.com	Hours: Monday, Tuesday, e p.m. to 7 p.m. Saturdays before and/or after class or by appointment Web Site: unokitty.freehostia.com

For information concerning UH student policies see:

http://www.uh.edu/provost/stu/stu_syllabsuppl.html