Information Assurance Specialization
College of Technology, University of Houston

Course Description

Course:	Cryptography and Information Systems Security
Course Number:	ITEC 6323
Credit Hours:	3 hours
Department:	Information and Logistics Technology

Catalog Description
ITEC6323
Cryptography and Information Systems Security
3 credit hours
Practical issues in cryptography, including examples of current historical cryptography systems; major types of cryptosystems and cryptanalytic techniques and how they operate; hands-on experience with current cryptographic technology.

Course Overview
This class examines applied cryptographic security services. It also examines enterprise related system threats and countermeasures. Specific cryptographic services include confidentiality, integrity, authentication and non repudiation. Specific mechanisms include encryption, hashes, message authentication codes, digital signatures and digital certificates Specific applications include: Public Key Infrastructure (PKI), secure protocols and virtual private networks (VPNs). Network counter-measures including 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, as well as Public Key Infrastructure Issues. "Hands-on" system and network vulnerability scanning are also included as are lab activities relating to IPSec and SSL based Virtual Private Networks (VPNs).

Learning Objectives
At the end of this course, students will be able to:

1. Identify and explain major cryptographic services and mechanisms.
2. Define relevant cryptographic terms including random number, private key, public key, algorithm, trusted third party and cryptanalysis.
3. Name, explain and utilize major algorithms including MD5, SHA1, DES, AES and RSA.
4. Compare and contrast symmetric and asymmetric cryptography and explain cryptographic services relevant to each.

5. Define key management and 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.

Subject Matter Modules*

Module#	Topic
Mod 1	Applied Cryptography Overview
Mod 1A	Toolkit Preparation
Mod 2	Symmetric Key Cryptography
Mod 2A	"Hands-On" Symmetric Cryptography Techniques
Mod 3	Symmetric Algorithms, DES Operation, and Vulnerabilities
Mod 3A	Symmetric Key and File Exchange, Symmetric Description
Mod 4	Asymmetric Cryptography, Public Key Infrastructure
Mod 4A	Authentication and Non-repudiation with Asymmetric Cryptography
Mod 5	Security Testing
Mod 5A	Applied Cryptography
Mod 6	Network Security
Mod 6A	Monitoring Security
Mod 7	Secure Networking, Virtual Private Networks
Mod 7A	Advanced Protocol Analysis SSL & IPSec
Mod 8	Network and Computer Attacks, E-mail
Mod 8A	Group work IAM Case Study
Mod 9	Intrusion Detection
Mod 9A	Network Security Monitoring (NSM) with Snort
Mod 10	Project Preparation and Preliminary Poster Presentation
Mod 11	Final
Mod 11A	Project Presentation

* Note that each subject matter module consists of 4 contact hours. Note also that each module includes a lecture component as well as an active learning component. In the active learning component the students work either on 'Hands-On" laboratory assignments or on group projects.

Detailed Course Outline

1. Applied Cryptography Overview
    1.1. Cryptographic Concepts
    1.2. Cryptographic Services
    1.3. Confidentiality
    1.4. Integrity
    1.5. Authentication
    1.6. Non-repudiation
    1.7. Processes
    1.8. Encryption
    1.9. Hash Functions
    1.10. Message Authentication
    1.11. Digital Signatures

1A. Toolkit Preparation
    1.1A Burn Security Toolkit from image
    1.2A Knoppix Live CD
    1.3A Network Security Monitor (NSM) Live CD
    1.4A OpenSSL cryptography toolkit interactive demonstration

2. Symmetric Key Cryptography
    2.1. Symmetric Cryptography History
    2.2. Substitution Ciphers
    2.3. Transposition Ciphers
    2.4. Diffusion and Confusion
    2.5. Classical cryptanalysis
    2.6. Frequency Analysis
    2.7. Brute Force
    2.8. Modern cryptanalysis
    2.9. Cryptanalysis Attacks
    2.10. Ciphertext-only
    2.11. Known-plain text
    2.12. Chosen-plain text (chosen-cipher text)
    2.13. Adaptive chosen-plain text

2A. "Hands-On" Symmetric Cryptography Techniques
    2A.1 OpenSSL Cryptographic Toolkit
    2A.2 Generate Pseudo Random Number
    2A.3 Generate DES Keys
    2A.4 Encrypt and Decrypt with DES
    2A.5 Demonstrate Integrity with MD5Sum and SHA-1 hashes

3. Symmetric Algorithms, DES Operation and Vulnerabilities
    3.1. Symmetric Algorithms including AES, TwoFish and IDEA
    3.2. DES Operation

3.3. DES Vulnerabilities
3.4. AES
3.5. Secret Key Assurances
3.6. Key Exchange Problem

3A. Symmetric Key and File Exchange, Symmetric Description
3A.1 Distribute an Encrypted Document with Apache
3A.2 Distribute a DES Key with NetCat
3A.3 Capture the DES Key packets with Wireshark
3A.4 Demonstrate Integrity with MD5 and SHA-1

4. Asymmetric Cryptography, Public Key Infrastructure
4.1. Public Key Cryptosystems
4.2. Hash Functions
4.3. Digital Signatures
4.4. Public Key Infrastructure
4.5. Purpose and Functions
4.6. Components
4.7. PGP and the Web of Trust
4.8. Electronic Key Management Systems (EKMS)
4.9. Key Management Infrastructure (KMI)
4.10. Automated Generation, Distribution, Storage, Accounting

4A. Authentication and Non-repudiation with Asymmetric Cryptography
4A.1 Create Asymmetric (RSA) Key Pairs
4A.2 Distribute Public Key with Apache
4A.3 Encrypt and Exchange a Text File
4A.4 Decrypt the Text File
4A.5 Demonstrate File Integrity with MD5 and SHA-1 Hashes

5. Security Testing
5.1. Configuration Management
5.2. Security Testing Techniques
5.3. Network Scanning
5.4. Virus Detectors
5.5. Vulnerability Scanning
5.6. Password Auditing
5.7. Auditing and Logging
5.8. File Integrity Checkers
5.9. Wireless LAN Testing

5A. Applied Cryptography
5A.1 Message Authentication Codes
5A.2 Hashed Message Authentication Codes
5A.3 Digital Signatures
5A.4 NetCat and CryptCat

6. Network Security
    6.1. Systems interconnection
    6.2. Authentication and Authorization
    6.3. Kerberos
    6.4. How Kerberos Works
    6.5. CORBA
    6.6. Object Request Broker
    6.7. Access Control for Networks
    6.8. Firewalls
    6.9. Screening Router
    6.10. Filtering Rules
    6.11. Proxy Gateway
    6.12. Dynamic Firewall Techniques

6A Monitoring Security
    6A.1 Keystroke Monitoring
    6A.2 Password Management
    6A.3 Strong Passwords
    6A.4 Password Policies, Monitoring and Auditing
    6A.5 Firewalls
    6A.6 IPTables and Rules

7. Secure Networking, Virtual Private Networks
    7.1. Account Management and User authentication
    7.2. Access control policies
    7.3. Access control mechanisms
    7.4. The HRU Model
    7.5. The Take-Grant Model
    7.6. Discretionary Vs. Mandatory Access
    7.7. The Bell-LaPadula Model
    7.8. Virtual Private Networks
    7.9. SSL
    7.10. IPSec

7A. Advanced Protocol Analysis SSL & IPSec
    7A.1 Use Wireshark to sniff SSL & IPSec sessions.
    7A.2 Compare and Contrast SSL and IPSec

8. Network and Computer Attacks
    8.1. Basic Tools and Techniques
    8.2. Covert channels
    8.3. Traffic analysis
    8.4. Access control attacks
    8.5. State attacks
    8.6. Timing attacks

8.7. TEMPEST vulnerabilities
8.8. IP based attacks, Teardrop and IP Spoofing
8.9. ICMP based attacks, Ping of Death and Smurf
8.10. UDP based attacks, Fraggle and Trinoo
8.11. Denial of Service (DoS) Attacks
8.12. TCP based Attacks, Syn Floods
8.13. DoS Attacks, Land and Tribal Flood Network (TFN)
8.14. E-mail System Security
8.15. E-mail system and retention policies
8.16. E-mail system monitoring

8A Group work IAM Case Study
8A.1 Information Criticality, Asset Analysis
8A.2 Enterprise Boundary
8A.3 Application and System Vulnerabilities Analysis
8A.4 Threat Evaluation Process
8A.5 Controls (Countermeasures) Evaluation Plan
8A.6 Report

9. Intrusion Detection, E-mail Security and WWW Threats
9.1. Maintenance Programs And Privileged Programs
9.2. System Threats
9.3. Screening Routers
9.4. Proxy Gateways
9.5. Firewalls
9.6. System, Network, and Internet Logs
9.7. E-mail Security and WWW Threats
9.8. E-mail Retention Policies
9.9. Email system Security
9.10. Email Monitoring

9A. Network Security Monitoring (NSM) with Snort
9A.1 NSM with Snort and Sguil
9A.2 Sguil architecture
9A.3 Snort Overview
9A.4 NTOP

10. Project Preparation and Preliminary Poster Presentation

11 Final

11A Project Presentation

Text Books

Title Fundamentals of Secure Computer Systems, ISBN 1-887902-66-X

Author Tjaden
Publisher Franklin, Beedle & Associates
Year 2004

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

That
Title Guideline for Implementing Cryptography In the Federal Government
Author Barker, Barker, and Lee
Publisher NIST SP-800-21
Year 2005

Title Guide to IPsec VPNs
Author Frankel, Kent, Lewkowski, Orebaugh, Ritchey, Sharma
Publisher NIST SP-800-77
Year 2005

Title Introduction to Public Key Technology and the Federal PKI Infrastructure
Author Kuhn, Hu, Polk, Chang
Publisher NIST SP-800-32
Year 2001