SE-4920 Detailed Lesson Outcomes

Dr. E. Durant <durant@msoe.edu> – Updated March 4, 2007

1. Lesson 1: Introduction
    a. State the key objectives of the course
    b. State the key assignments and their weights
2. Lesson 2: Security Principles
    a. Discuss the 12 generally accepted principles of information security
    b. Discuss the 8 generally accepted principles underlying security mechanisms
3. Lesson 3: Engineering Introduction: Briefly describe the following concepts as they relate to computer security…
    a. How data crosses a network
    b. Active vs. passive attacks
    c. Benefits of cryptography at various layers
    d. Authorization systems
    e. Tempest and zone of control
    f. Key escrow
    g. Discretionary and mandatory access controls
    h. Covert channels
    i. Orange book
    j. Overview of legal climate
4. Lesson 4: Legal Issues and HIPAA
    a. Identify the types and targets of computer crime
    b. Summarize the major types of attacks performed by cyber criminals
    c. Understand the context of the computer in the legal system
    d. Appreciate the complexities of intellectual property law
    e. Discuss the issues surrounding computer security and privacy rights
    f. Articulate the challenges of computer forensics
    g. Discuss the major provisions of HIPAA
5. Lesson 5: Developing Secure Software
    a. Discuss the connection between defects and security
    b. Identify several types of defects
    c. Discuss the cost/schedule ramifications of defect reduction
    d. State several benefits of managing defects throughout the SDLC
    e. Identify key aspects of the TSP and TSP-Secure processes
6. Lesson 6: Introduction to cryptography
    a. Define common cryptography terms
    b. Discuss the effect of processing power on the effectiveness of cryptography
    c. Explain the meaning of and relationship between the 3 basic classes of cryptographic attacks: ciphertext only, known plaintext, chosen plaintext
    d. Discuss the similarities and differences among the 3 basic types of cryptographic functions: (0-, 1-, and 2-key): hash, secret key, public key
7. Lesson 7: Secret key cryptography
    a. Discuss block and key length issues related to secret key cryptography
    b. Define several terms related to secret key cryptography

   c. Describe and evaluate DES, focusing on both design and implementation issues
   d. Explain some uses of one-time pads with RC4 as a representative example

8. Lesson 8: Modes of operation
   a. Explain various methods for applying secret key (block) encryption to a message stream
   b. Using secret key techniques to generate MACs (message authentication codes)
9. Lesson 9: Hashes and message digests
   a. Discuss the uses of hashes for fingerprinting and signing
   b. Discuss the key properties of a cryptographic hash function contrasted with a general hash function
   c. Explain why hashes need to be roughly twice as long as secret keys
   d. Explain how a hash can be used for an MAC
10. Lessons 10-11: Public key algorithms
   a. Perform modular arithmetic (addition, multiplication, exponentiation)
   b. Apply basic theory of modular arithmetic (Totient function, Euler’s theorem, …)
   c. Execute and apply the RSA algorithm for encryption and digital signatures
   d. Execute and apply the Diffie-Hellman algorithm for establishing a shared secret
11. Lesson 12: Authentication
   a. Explain the difference between authorization and authentication
   b. Critique authentication methods using password and/or address-based methods
   c. Discuss eavesdropping and server database reading and how various authentication methods deal with them
   d. Explain the general use of trusted intermediaries for both secret and private key based systems
   e. Discuss issues specific to authenticating people, including the three main approaches to doing so
12. Lesson 13: Kerberos V4
   a. Describe the services provided by Kerberos V4
   b. Diagram the generation and use of tickets and ticket-granting tickets for authentication and establishment of a shared secret
13. Lesson 14: Real-time communication security
   a. Define “real-time communication security”
   b. Discuss problems unique to real-time communication security and some solutions
   c. Define “perfect forward secrecy,” explain why it is desirable, and show one way that it can be attained
14. Lesson 15: Encryption: PGP
   a. Give an overview of the history and current application of PGP
15. Lesson 16: Firewalls, SSH, VPNs
   a. Discuss the reasons for using a firewall, various topologies, and firewall limitations
   b. Diagram and explain the use of VPNs and how they are used in conjunction with firewalls
   c. Explain the key security features provided by SSH
16. Lesson 17: Stack overruns in C
   a. Explain how a stack overrun attack is executed and what knowledge it requires

17. Lesson 18: Web issues, OWASP (Open Web Application Security Project) and SQL injection
    a. Describe the basic structure of URLs, HTTP requests, and HTTP digest authentication as they relate to security
    b. Explain the use of HTTP cookies
    c. Define cross-site scripting
    d. Explain an SQL injection attack and various methods of remediation
    e. Be familiar with OWASP and the OWASP Top 10 list
18. Lessons 19+: Student presentations