CS 5700: Computer Security and Information Assurance (CSIA)

Prof. Leszek Lilien, Department of Computer Science, Western Michigan University

Midterm Exam Topics

Notes:

- Answers to all questions are available on the lecture slides given to you.
- The word "**Given**" (in boldface) means that this information will be provided to you as a part of the question. For example, "**Given** the list of requirements for crypto protocols, discuss them." means that I will provide you with the list of requirements (no need to memorize them).
- The word "**SKIP**" (in boldface) and gray background means that this information will not be tested by the exam (e.g., "3E. The Clipper Story" will be omitted). Of course, all information marked as "**SKIP**" in the lecture slides will be omitted as well. Finally, information covered *only* in the long slide versions (marked as: "Optional LONG" on the slide web page) is not required.
- The topics in boldface are (a bit) more likely to be used in the midterm than others.

Section 1. Introduction

1. Introduction to Security

1.1. Examples-Security in Practice— Give a few examples of cyberterrorism / threats to personal privacy.

1.2. What is "Security"?— Give at least five *types* of security threats.

1.3. Pillars of Security: **C-I-A— Define confidentiality / integrity / availability. Explain why C-I-A need be balanced**, illustrate with an example. Which of the C-I-A components is binary (all-or-none) in nature?

1.4. Vulnerabilities, Threats, and Controls— **Define vulnerability / threat / controls. Define attack. Illustrate each def with an example.** List 4 kinds of threats to assets. List 4 levels of vulnerabilities and threats. Give examples of vulnerabilities and threats: for hardware / for software / for data / for other assets. How to prevent identity theft?

1.5. Attackers— Attackers' MOM. **Types of attackers.**

1.6. How to React to an Exploit?— Discuss the problem "To Report or Not To Report" showing arguments on both sides. What is computer forensics?

1.7. Methods of Defense— **List five basic approaches to defense of computing systems. 5 types of controls.** Which controls of the 5 is considered primary / secondary? How encryption protects C-I-A? Give a few examples of h/w controls. What are benefits of policy/procedure controls? Give a few examples of physical controls.

Discuss how each of the following affects effectiveness of controls: awareness of problem, likelihood of use, overlapping controls, periodic reviews.

1.8. Principles of Computer Security— **Define in your own words Principle of Easiest Penetration / Principle of Adequate Protection / Principle of Effectiveness / Principle of Weakest Link.**

Section 2. Security in Networks – Part 1

7.1. Network Concepts

a. [**SKIP**: Introduction]

b. The network

Why network boundary, ownership, and control are difficult or impossible to specify?

c. Media

List 3 or more communication media (one of them is cable).

d. Protocols—(ISO OSI, TCP/IP, UDP, network addressing schemes for LAN and WAN)

List 7 layers of the ISO OSI Reference Model.

Indicate which layer is responsible for: physical communications, reliable data delivery, routing, session control, standardized data appearance, user level messages.

Show example scenario of message sending which uses ISO OSI model.

Indicate which of the two is conceptual model and which is implementation: ISO OSI and TCP/IP.

List 4 layers of TCP/IP.

Indicate which layer is responsible for: physical communications, reliable data delivery, routing, session control, standardized data appearance, user level messages?

What is a *port*?

Describe the UDP protocol. **How UDP differs from TCP?**

Give examples of 2 or more application protocols using TCP/IP, and 1 or more application protocols using UDP.

What are addressing schemes used for LANs and WANs?

How IP address for, e.g., cs.wmich.edu is found by the Internet?

How hosts disseminate address info?

e. Types of networks

Describe characteristics of: LAN, WAN, Internetworks.

f. Topologies

List 2 or more types of network topologies.

g. Distributed systems

What is a distributed system?

What are 2 major types of distributed systems?

h. APIs

What is API? What are benefits of having standard APIs?

i. Advantages of computing networks

Give 3 or more advantages provided by networks.

7.2. Threats in Networks

a. [**SKIP**: Introduction]

b. Network vulnerabilities

Name at least 4 network characteristics that increase security risks.

c. Who attacks networks?

What are motives of attackers?

Is it acceptable to penetrate a system to demonstrate to its owners security weaknesses? Why or why not?

d. Threat precursors

What is a threat precursor?

List 4 or more techniques used as threat precursors.

Explain each of the following techniques and/or show examples of using it:

1) Port scan
2) Social engineering

3) Reconnaissance
4) OS and application fingerprinting
5) Using bulletin boards and chats
6) Getting available documentation

For each of the above techniques, explain what information it can provide to an attacker.

e. Threats in transit: eavesdropping and wiretapping

List two basic categories of threats to data in transit.

Explain differences between passive and active wiretapping.

Show how wiretapping can be used for at least 3 different communication media.

Why it is easy to break wireless installations?

Why the WEP protocol is easy to break?

f. [**SKIP**: Protocol flaws]

g. Types of attacks

Define each of the 9 type of attacks listed as g-1 – g-9 below.

g-1. Impersonation

Explain each of the following types of impersonation attacks:

1) IA by guessing
2) IA by eavesdropping/wiretaping
3) IA by circumventing authentication
4) IA by using lack of authentication
5) IA by exploiting well-known authentication
6) IA by exploiting trusted authentication

Explain why lack of authentication can be a design or administrative decision, not a flaw.

g-2. Spoofing

List at least 2 different types of spoofing.

Define/explain/give example of: masquerading, session hijacking, MITM.

Give full scenario of correct communication and communication showing MITM attack. Be sure to show exactly encryption/decryption formulas (such as C = E(x, y), etc.)

g-3. Message confidentiality threats

List at least 3 different types of message confidentiality threats.

Define/explain/give example of: eavesdropping, impersonation, msg misdelivery, msg exposure, traffic flow analysis.

g-4. Message integrity threats

What are two types of message integrity threats?

Explain what is msg fabrication. Give 3 or more types of msg fabrication.

Explain what is noise, how it can affect msg integrity, and what are countermeasures.

g-5. Web site attacks

List 3 or more types of common web site attacks.

Define/explain/give example of attacking web sites by using: buffer overflows, dot-dot attacks, exploiting application code errors, server-side include attacks.

What controls are available to oppose dot-dot attacks?

g-6. Denial of service (DoS)

Define/explain/give example of a DoS attack.

List types and subtypes of DoS attacks.

(2b) **What DoS attacks can be used to saturate devices?**

(2b-i) Connection flooding:

Define/explain/give example of connection flooding.

What is ICMP and how can it be used for DoS attacks?

(2b-i1) Show example of echo-chargen attack.

(2b-i2) Show example of ping of death attack.

Show example of a smurf attack

(2b-ii) SYN flood

Define/explain of. SYN flood attacks.

Show scenario of SYN flood attack.

Why attacker spoofs sender's address in SYN packets sent to destination D? Why attacker might make *each* spoofed sender's address in SYN packets different

(2c) **What are subtypes of DoS attacks based on redirecting traffic?**

(2c-i) Redirecting traffic by advertising a *false* best path

Define/explain/give example of. an attack by advertising a *false* best path.

What is a packet-dropping attack? black hole attack? How do they differ?

(2c-ii) Redirecting traffic by DNS attacks:

Define/explain attacks redirecting traffic via DNS attacks.

g-7. Distributed denial of service (DDoS).

Give a scenario showing DDoS attack. Make sure to show main stages of DDoS

What is a zombie?

g-8. Threats to active or mobile code

What is active/mobile code?

Why server benefits by downloading active code to a client? Give a specific example.

List 4 types of active code.

Define/explain/give example of each of the following types of active/mobile code: cookies, scripts, active code, automatic execution by type

1) Cookies

List and define two types of cookies.

What info can be captured, stored, and sent to servers by cookies?

What are legitimate and illegitimate roles for cookies?

2) Scripts

How an attacker can use scripts for attacks on servers?

What is CGI? Show scenarios of using HTTP without and with CGI.

Show example of escape-character attack.

How a server can protect itself against script-based attacks?

3) Active code

What are two main types of active code?

(3a) Java code:

List 2 or more security features of Java.

What is a hostile applet? Why can it do harm?

How to prevent harm that could be done by Java applets?

(3b) ActiveX:

What are risks of downloading Active X controls (code)?

How risks of downloading ActiveX controls can be reduced? Why this solution is not complete?

4) Automatic execution by type

What are two types of automatic execution by type?

Different types of files pose security risks when executed (automatically or manually). List the following files in the order from the lowest to the highest security risk: executable files, files with active content, text files *without macros*.

Should opening of files of unknown origin or content be avoided? Why or why not?

g-9. Scripted and complex attacks

1) Scripted attacks
What are scripted attacks?
Who are script kiddies?

2) Complex attacks
What are complex attacks?
Give example of a complex attack with at least 3 phases, using 3 different kinds of tools.

h. [**SKIP**: Summary of network vulnerabilities]

===================== **Good luck on your Midterm Exam!** =====================