CS 5950: Computer Security and Information Assurance
Spring 2007

Prof. Leszek Lilien
Department of Computer Science
Western Michigan University

Final Exam Topics

Notes:

- The final exam covers only material that was *not* covered by the midterm exam.
- Answers to all questions are available on the lecture slides (at: http://www.cs.wmich.edu/~llilien/teaching/2007spring/cs5950/slides+announcements.htm).
- 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 questions in boldface are (a bit) more likely to be asked than others.

Leftover material from: **Lecture Section 3 (Ch.2, Part 1): Introduction to Cryptology – Part 1**

Note: This material, not covered in the midterm exam, starts with Section "3B.2. Transposition Ciphers"

(From Subsection 3B. Basic Types of Ciphers)

3B.2. Transposition ciphers— **Give an example of columnar transposition cipher, indicate key value. Describe attacking transposition ciphers, using an example.**

3B.3. Product (combination) ciphers— Define product ciphers. Is it guaranteed to be stronger than any of its components?

3C. Making Good Ciphers

3C.1. Criteria for "Good Ciphers"

Given Shannon's criteria for "good ciphers," discuss these criteria. Define confusion and diffusion. Discuss confusion and diffusion as criteria for good ciphers.

3C.2. Stream and block ciphers

a. Stream ciphers— Define stream cipher. **Describe polyalphabetic cipher using Vigenere Tableaux as a stream cipher.**

b. Problems with stream ciphers— Illustrate with example problem with stream ciphers.

c. Block ciphers— Define block cipher. What are benefits of block ciphers?

d. Pros / cons for stream and block ciphers— **Compare pros and cons for stream and block ciphers based on delay, error propagation, diffusion, and susceptibility to malicious insertion.**

3C.3. Cryptanalysis

Define each one of 5 possible cryptanalyst attack approaches: ciphertext-only attack, known plaintext attack, probable plaintext attac, chosen plaintext attack, chosen ciphertext attack.

3C.4. Symmetric cryptosystems and asymmetric (public key) cryptosystems

Compare symmetric and asymmetric cryptography (in terms of: nr of keys, key secrecy, E/D secrecy, distribution of key or E/D, analogy to a safe or safe with a deposit slot).

3D. The DES Algorithm

3D.1. Background and History of DES— **Motivation for DES.**

3D.2. Overview of DES— **Given** figures showing basic encryption structure and key encryption structure, describe DES. Key length vs. effective key length. Problems with DES.

3D.3. Double and Triple DES— Describe double DES (show formal notation). **Problem with double DES. Describe triple DES (show formal notation). What is the benefit of using triple DES.**

3D.4. Security of DES— Is DES insecure?

[**SKIP**—3E. The Clipper Story-----]

3F. The AES Algorithm

3F.1. The AES Contest— **Given** list of NIST criteria for new encryption algorithm, discuss each criterion.

3F.2. Overview of Rijndael— **Describe AES; specify key lengths and basic operations.**

3F.3. Strength of AES— **What are strengths of AES?**

3F.4. Comparison of DES and AES— Compare DES and AES w.r.t. block size, key length, design rationale, selection process, and source.

Lecture Section 4 (Ch.2, Part 2): Introduction to Cryptology – Part 2

4G. Public Key Encryption (PKE)

4G.1. Motivation for PKE— Problems with symmetric key encryption. Inventors of the first asymmetric cryptosystem. **Describe the principles of asymmetric cryptosystems.** Nr of keys for n users? (compare with symmetric encryption)

4G.2. Characteristics of PKE— **List PKE requirements. Compare speed of symmetric and asymmetric encryption—what are the consequences?**

4G.3. RSA (Rivest-Shamir-Adelman) Encryption**— Give formulas for RSA encryption and decryption.**

4H. The Uses of Encryption

4H.1. Cryptographic Hash Functions

strong hash fcn; collisions and attacks on message integrity; file checksum; keyed crypto checksums (using DES, AES) vs. keyless crypto checksums (remember names MD5/MD4, SHA/SHS)

4H.2. Key Exchange

motivation; **deriving symmetric key via PKE** – remember the "good" solution and problems with bad solutions;

4H.3. Digital Signatures (DSs)

motivation; roles for signatures; required and desirable properties for DSs; **scenario of sending and receiving a digitally signed msg (msg encrypted or not);**

4H.4. Certificates

a. Introduction

basic means of building trust; basic means of verifying trust; what is the role of trusted third party (TTP) in interactions?

b. Trust Through a Common Respected Individual

give examples of Common Respected Individual in an organization; problems with using a Common Respected Individual; solutions to the problems with using a Common Respected Individual

c. Certificates for Identity Authentication

certificate structure; scenario of creating certificates within a company; **problems with certificates in multilevel certification hierarchy, and solution to the problem; requirements for a certification scheme**

d. Trust Without a Single Hierarchy

how trust established if there is no "natural" trust hierarchy (or trust authority) to rely on?

Lecture Section 5 (Ch.7, Part 2): Security in Networks – Part 2

Note: Section numbers (and slide numbers if any) are from the SHORT version of this section.

Note: Textbook chapter Sections 7.1 and 7.1 are covered by Lecture Section 2 (Lecture Subsections 2.1 and 2.2, respectively).
Textbook chapter Sections 7.3 and 7.4 are covered by Lecture Section 5 (Lecture Subsections 5.1 and 5.2, respectively).

5.1. Network Security Controls

[**SKIP**: a. Introduction-----]

b. Security threat analysis

Name the 3 steps of security threat analysis.

c. Impact of network architecture/design & implementation on security.

Name 2 or more means by which network architecture can improve security. Explain how they can improve it.

Explain and give examples how each of the following can improve network security:

segmentation, redundancy, avoiding, single points of failure.

Explain and give examples for cold, warm, and hot spares.

d. Encryption

(d-i) Link encryption vs. end-to-end {e2e} encryption

Explain what is link encryption and e2e encryption. Draw appropriate figures.

In which cases link encryption is sufficient? When e2e encryption is needed?

Compare link encryption and e2e encryption. Which is visible to a user or her application? Which is more efficient? Why?

(d-ii) Virtual private network {VPN}

Explain what is VPN.

Provide a scenario showing how it works.

(d-iii) PKI and certificates

Name 3 elements of PKI.

Name at least 4 (of 5 discussed) PKI services.

Explain the roles played by Certificate Authority (CA) and Registration Authority (RA). Give examples of analogous services in social systems (outside Cyberspace).

(d-iv) SSH protocol

Explain the role of the SSH protocol. What attacks does it protect against?

What service were replaced by the SSH protocol?

(d-v) SSL protocol (a.k.a. TLS protocol)

Explain the role of the SSL protocol. What attacks does it protect against?

Give a full SSL use scenario (as discussed in class).

(d-vi) IPsec protocol suite

What is IPsec? What threats does it control? At which TCP/IP protocol layer does it run?

What are the main differences between IPv6 and IPv4?

What is: Security Association (SA)? Security Parameter Index (SPI)? Authentication header (AH)? Encapsulated security payload (ESP)?

Give an IPsec use scenario.

What is ISAKMP (Internet Security Association Key Management Protocol) and what are its roles?

(d-vii) Signed code

What is a partial solution to the malicious active code problem? How is it done?

[**SKIP** HERE-COVERED BELOW: (d-viii) Encrypted e-mail-----]

[**SKIP**: e. Message content integrity controls-----]

f. Strong authentication

[**SKIP** HERE: (f-i) One-time passwords-----]

[**SKIP** HERE: (f-ii) Challenge-response systems-----]

[**SKIP** HERE: (f-iii) Digital distributed authentication-----]

(f-iv) Kerberos

What is the role of Kerberos? What is its basic idea?

What are tickets in Kerberos?

List two user's steps needed to use Kerberos.

Provide a full scenario of using Kerberos, showing interchange of information among user (U), Kerberos Server (KS), Ticket-Granting Server (T-GS), and the service requested by the user. Make sure that you show contents of messages, using the E(msg, key) notation where relevant.

What is the security advantage of Kerberos? (Hint: it has to do with password use by Kerberos.)

Name at least 3 strengths of Kerberos (6 were named).

Name at least 4 weaknesses of Kerberos (7 were named).

g. Access controls

Name two major mechanisms for access controls.

(g-1) ACLs on routers

What is the role of network routers?

How to use ACLs on routers?

How ACLs should *not* be used on routers ("problems") and why?

(g-2) Firewalls

What is the role of firewalls? Compare security roles of firewalls and routers.

h. Intrusion Detection Systems: alarms and alerts

Show example of a 3-layer network protection using IDS as Layer 3. Give examples (name) mechanisms used in Layers 1 and 2.

What is an IDS?

i. Honeypots

What is a honeypot? Name at least 2 (of 3 shown) ways of using it. How can it help design better security controls?

j. Traffic flow security

Name 2 solutions available for preventing attackers from inferring occurrence/location of some event/structure from intensity of encrypted network traffic.

Give an example scenario showing use of onion-routing. Point out why sender S and destination D remain unknown to intermediate nodes.

[**SKIP**: k. Review of network security controls-----]

5.2. Network Security Tools

5.2.1. Firewalls

[**SKIP**: a. Introduction-----]

b. What is a firewall?

What is a firewall?

How does firewall achieve its goal (how does it handle packets)?

What are two types of default firewall behaviors?

[**SKIP**: How do they correspond to security policy requirements w.r.t. firewalls?-----]

[**SKIP**: c. Firewall design

Name at least 2 firewall design principles.-----]

d. Types of firewalls

List all 3 types of firewalls as discussed. List their subtypes as well.

[**SKIP**: Guards are the most powerful among all types of firewalls. Would you recommend use of guards for all applications that require firewalls? Why or why not?-----]

[**SKIP**: (d-i) Packet filters

Name two types of packet filters.

What information can be used by packet filters to accept or reject packets? How does it affect their power of filtering?

Can packet filters block only some commands of an application using a given port (such as Telnet using port 23)? Why or why not?

(d-i-1) Simple packet filters

What is *the* difference between simple and stateful packet filters? How does it affect their capabilities?

(d-i-2) Stateful packet filters

Explain why remembering more previous packets can improve filtering done by stateful packet filters.-----]

[**SKIP**: (d-ii) Application proxies (incl. guides)

Why app proxies are more powerful than even stateful packet filters?

Can app proxies block only some commands of an application using a given port (such as Telnet using port 23)? Why or why not?

Give a scenario showing use of an application proxy (with a figure showing a few applications).

(d-ii-1) Guards

What is a guard? Is there a clear boundary between "regular" app proxies and guards? Why or why not?

What are the limitations of the power of guards?-----]

[**SKIP**: (d-iii) Personal firewalls

How personal firewalls differ from other firewalls?

Would you recommend using personal firewalls on company's desktops connected by a LAN that has an application proxy firewall? Why or why not?

Which other security controls should be used together with personal firewalls?-----]

[**SKIP**: e. Comparison of firewall types-----]

f. Example firewall configurations

Explain what is a DMZ. Draw a figure showing a DMZ (indicate DMZ by circling it).

g. What firewalls can—and can't—block

Why firewalls should be simple, with no functionality beyond what is needed for their basic filtering functions? Give examples of functionalities that should *not* be available on firewalls.

5.2.2. Intrusion Detection Systems

a. Introduction

Intrusion detection is often called the second line of defense. In this case, what is the first line of defense?

What is an IDS? Which of the following groups of users do they control: (1) insiders, (2) outsiders?

[**SKIP**: Why IDSs should operate in the stealth mode? How can this be assured?

Draw a figure and indicate in it the only two recommended IDS interfaces. Explain how these interfaces should be used, especially how their uses should be restricted.-----]

What is an anomaly? a misuse? How one is related to the other? Is an intrusion an anomaly, a misuse or both?

Define profiling. How is it used in IDSs?

b. Types of IDSs

What are the types of IDSs w.r.t. to operation?

[**SKIP**: (b-i) Signature-based IDSs

Define a signature-based IDS.

Can signature-based IDSs detect new attacks? Why or why not?

List 2 or more problems with signature-based IDSs.-----]

[**SKIP**: (b-ii) Anomaly-based IDSs
Define anomaly-based IDSs.
Can anomaly-based IDSs detect new attacks? Why or why not?

(b-ii-1) Misuse-based IDSs
Define a misuse-based IDS. How does it differ from signature-based IDSs and other anomaly-based IDSs?-----]
[**SKIP**: (b-iii) Other IDSs
What is a hybrid IDS?-----]

c. Goals for IDSs
List 2 or more categories of IDS responses.

[**SKIP**: d. IDS strengths and limitations
Name at least 2 strength and at least 2 limitations of IDSs (in general).----]

5.2.3. Secure E-Mail

a. Introduction
Which of the C-I-A security properties are missing from typical e-mail usage?

[**SKIP**: b. Security for e-mail
Name at least 4 different threats to e-mail and the corresponding controls.
Name at least 3 requirements for secure e-mail. Are all of them desirable for every message?-----]

c. Design of PEM (Privacy-enhanced Electronic Mail)
One of design goals for PEM (secure e-mail) was allowing PEM msgs travel as ordinary mail msgs. Why was it important?
Give a scenario showing use of PEM. Use the E(msg, key) notation where appropriate. Draw a figure showing three components of PEM messages. Indicate which components include elements of the original user's message.
[**SKIP**: Can PEM be used for anonymous e-mail? Why or why not?-----]
Name at least one of two major problems with PEM.

e. Example secure e-mail systems
(e-i) PGP
[**SKIP**: What is PGP?-----]
What is keyring in PGP, and how is it used?
[**SKIP**: (e-ii) S/MIME
What is the principal difference between PGP and S/MIME?-----]

Lecture Section 6 (Ch.3): Program Security

Note: Section numbers (and slide numbers if any) are from the SHORT version of this section.

What is the role of "program security"?

6.1. Secure Programs— Defining and Testing

a. Introduction
what is pgm security for user, for programmer, and for manager? **give a single scenario in which error, fault, and failure can be illustrated**;
list 3 basic approaches to having secure programs;

[**SKIP**: b. Judging S/w Security by Fixing Faults
explain principle of the penetrate and patch approach to judging pgm security; what are shortcomings of the penetrate and patch approach?

c. Judging S/w Security by Testing Pgm Behavior
explain principle of Testing Pgm Behavior approach to judging pgm security;
why detecting a failure is not suffuicient?
should we be concerned with inadvertent faults and failures? why?
what are the shortcomings of the Testing Pgm Behavior approach?

d. Judging S/w Security by Pgm Security Analysis
explain principle of judging s/w security by Pgm Security Analysis-----]

e. Types of Pgm Flaws
what are 2 major types of flaws? what are 2 types of intentional flaws? Give at least 3 examples of inadvertent pgm flaws

6.2. Nonmalicious Program Errors

a. Buffer overflows
what is buffer overflow flaw? why is it dangerous?
write a detailed scenario of a buffer overflow affecting a call stack area (emphasize/explain how attacker achieves her goals)
what is web server (overflow) attack?

b. Incomplete mediation
what is incomplete mediation?
write a detailed scenario showing incomplete mediation (emphasize/explain how attacker achieves her goals)
[**SKIP**: what are possible solutions for a server?-----]

c. Time-to-check to time-to-use errors (TOCTTOU)
what is TOCTTOU?
give example of TOCTTOU in computing (emphasize/explain how attacker achieves her goals)

d. Combinations of nonmalicious program flaws
why nonmalicious flaws are security threats?

6.3. Malicious Code
define what is "malicious code"

6.3.1. General purpose malicious code

a. Introduction
are all viruses harmful? can viruses be transferred from trusted sources?

b. Kinds of Malicious Code (malware):
Define each of the following kinds of malware: Trojan horse, Virus, Worm, Logic bomb (incl. time bombs), Rabbit, Trapdoor / backdoor. Be able to indicate which are independent programs and which are sections (parts) of programs. Which are self-replicating?
Give an example of malware that is a combination of two(or more) of the basic kinds.

c. How Viruses Work
explain how viruses work. remember 2 phases of virus activities (infect and spread)
[**SKIP**: explain how document viruses work.-----]
[**SKIP**: remember 4 kinds of viruses w.r.t. the way of attaching to infected pgms-----]
what are characteristics of a perfect virus?

where viruses can hide and which of these hiding places are best for viruses and why?

d. Virus Signatures

what is Virus Signature? What patterns define Virus Signatures?
what are polymorphic viruses? Why are they more difficult to detect?
examples of polymorphic virus mutations

e. Preventing Virus Infections

list t least 5 of the 7 recommended ways of Preventing Virus Infections

f. Seven Truths About Viruses

be able to confirm or deny each of the seven truths or their negations (e.g., you should be able to qualify as "false" the following statement: "Viruses can infect only some OSs")

[**SKIP**:

g. Case Studies

what was the impact of Internet worm (1988)?
what kind of attack and on what target was performed by Code Red (2001)?
what are web bugs? how they work? How can they be neutralized (located/blocked/deleted)?-----]

h. virus removal and system recovery after infection

describe virus removal and system recovery after infection
when infected file can't be recovered?

6.3.2. Targeted malicious code

a. Trapdoors

what is a trapdoor? who and why can insert it into code? give examples of benevolent trapdoors

b. Salami attack

what is salami attack: define and give example. what types of computations are easy targets for salami attacks?

c. Covert channels (CCs)

i. **What is a covert channel – define and give examples. How programmers create CCs?**
give examples how leaked data can be hidden to create CCs?
ii. List types of Covert Channels
[**SKIP**: iii. Describe in a sufficient detail an example of a storage Covert Channel-----]
[**SKIP**: describe how CC can be created by using: file locks / disk storage quota / existence of a file-----]
[**SKIP**: why storage CCs require synchronization?-----]
[**SKIP**: iv. How timing CCs convey information? Describe in a sufficient detail an example of a Timing Covert Channel.-----]
[**SKIP**: v. Name two techniques for identifying potential Covert Channels. What is the basic idea behind the Shared Resource Matrix method? Use an example to describe the Shared Resource Matrix method. What is the basic idea behind the Information Flow Method? Use an example (e.g, a 3-statement program with different kinds of statements) to describe the Information Flow Method.-----]
vi. Can covert channels be prevented in open systems? Why?

6.4. Controls for Security

a. Introduction

List three types of security controls.

b. Developmental controls for security

Why security controls should be used in software development? Give example of a fundamental principle of s/w engineering that contributes to security (we listed 3).

How modularity / encapsulation / info hiding improves security?

[**SKIP**: Be able to discuss each of the following techniques for building solid software:

1) Peer reviews

How reviews / walkthroughs / inspections differ from each other? How can they improve security?

2) Hazard analysis

Remember two major components: hazard lists and what-if scenarios. How can it improve security?

3) Testing

Define Module/component/unit testing, integration testing, function testing, performance testing, acceptance testing, installation testing, regression testing.

Types of testing w.r.t. code availability.

How can testing improve security?-----]

4) Good design

i. Modularity / encapsulation / info hiding (covered above)

ii. **Fault tolerance – What are principles of fault-tolerant approach? Explain majority voting / recovery block. How can it improve security?**

[**SKIP**: iii. Consistent failure handling policies— Name three ways of handling failures

iv. Design rationale and history— How can it improve security?

v. Design patterns— How can it improve security?-----]

[**SKIP**: 5) Risk prediction & management— Why is it important for security?

6) Static analysis— Define it. What program elements are checked by static analysis? How can it improve security?

7) Configuration management (CM)— Define CM. Define corrective changes, adaptive changes, perfective changes, preventive changes.

What is a baseline and how is it used for CM? What are deltas, and how are they used for CM? What is conditional compilation and how is it used for CM?

What is the purpose of configuration auditing?

What is the purpose of status accounting?

What is Configuration Control Board (CCB)?

What are security benefits of configuration management?

8) Additional developmental controls

How learning from pgm development an maintenance mistakes can improve pgm security?

How (formal) proofs of program correctness can improve security? What are their practical limitations?-----]

c. OS controls for security

What is “trusted software”? How can it be used for an OS?

What are 3 mentioned ways of of increasing system security if untrusted pgms are present? Explain notions of mutual suspicion / confinement / access log, and tell how mutual suspicion / confinement / access log improve s security.

d. Administrative controls for security

List at least 2 administrative controls for security (we mentioned 3). Explain how standards / security audits / separation of duties in pgm development contribute to better security.

Lecture Section 7 (Ch.9): Legal, Privacy, and Ethical Issues in Computer Security

Note: Since the slides were covered ion lecture and posted just days before exam, only a few topics (that is, slides) will be required for the Final Exam, as listed below.

7.1. Basic Legal Issues

a. Protecting Programs and Data

What is the role of a copyright?

Which of the following are protected under *copyrights*: ideas, expression of ideas, tangible objects, ways to make tangible objects, or trade secrets?

What properties must creative work of mind possess to become intellectual property (IP), protectable under copyrights?

What is the role of a patent?

Which of the following are protected under *patents*: ideas, their expression, tangible objects, ways to make tangible objects, or trade secrets?

What are trade secrets? How trade secrets can protect IP (intellectual property)?

Which of the following are protected as *trade secrets*: ideas, their expression, tangible objects, ways to make tangible objects, or secrets providing competitive edge?

Is reverse engineering of a trade secret, a copyrighted material, or a patented object/process a legal activity?

[SKIP:

Which forms of IP (intellectual property) protection are best suited for *hardware*?

Which forms of IP protection are best suited for *firmware (microcode)*?

Which forms of IP protection are best suited for *object code*?

Which forms of IP protection are best suited for *source code*?

-----]

b. Information and the Law

[SKIP:

Name at least 3 characteristics of information as an object of value.

Are copyrights, patents, and trade secrets sufficient to cover all protection needs? Why or why not?

What controls can be used if copyrights, patents, and trade secrets are not sufficient to cover protection needs?------]

List all law categories/subcategories named in class.

What penalties are remedies under criminal law? under civil law?

c. Ownership Rights of Employees and Employers

Can employer claim ownership of *products* developed by you? How to increases chances that courts will recognize your ownership?
Can employer claim ownership of *patents* developed by you? How to increases chances that courts will recognize your ownership?
Can employer claim ownership of *copyrights* developed by you? How to increases chances that courts will recognize your ownership?
Can employer claim ownership of *trade secrets* developed by you? How to increases chances that courts will recognize your ownership?

You could be employed under work-for-hire agreement or an employment contract, or you could license products developed by you. How each of these forms of work affect ownership of products, patents, or trade secrets developed by you?

d. Software Failures

[SKIP: ------
How vendor and user interests can conflict in the context of reporting software flaws? **----------]**
Describe responsible vulnerability reporting. Indicate clearly obligations of vendors and coordinators.

[**SKIP**: 7.2. Computer Crime
Why a separate category is needed for computer crime? **----------]**

7.3. Privacy

List 3 or more privacy threats posed by computing systems.
How can you inadvertently sell out your own privacy? Give an example.
[SKIP:
Name at least 3 privacy controls.
What is the area of applicability for the HIPAA laws?
What is the area of applicability for the Gramm-Leach-Bliley Act?
----------]

7.4. Ethics

a. Introduction to Ethics

[SKIP: What is the difference between law and ethics?-----]
Why law alone can't control human behavior?
[**SKIP**: b. Case Studies of Ethics-----]

c. Codes of Professional Ethics

GIVEN a code of professional ethics (one of the three from Fig. 9-1, 9-2, or 9-3 in the textbook)**, select one of its imperative principles** ("I agree," "I will," or "thou shall not") **and give an example of its abuse.**

========== **Good luck for your Final Exam!** ==========