CS 5950: Computer Security and Information Assurance — Spring 2007

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

Midterm Exam

First Name _____

Last Name (in BLOCK LETTERS): _____

Row_____ Seat _____ Email: _____

Do *not* open this exam booklet until the instructor gives a clear signal to start.

Question Nr	Max. Score	Your Score	Comments
1	10		
2	10		
3	5		
4	5		
5	5		
6	15		
7	15		
8	5		
9	5		
10	10		
11	15		
TOTAL	**100**		

Notes:

- Sign this page and enter requested information. After the signal to start, to be safe sign *all* pages.
- This is a **closed book/notes/laptop/desktop exam.**
- Read the instructions for each question carefully.
- If you are unsure how to understand a question, write down your assumptions regarding the question.
- To receive a partial credit for an imperfect answer or result, you must show the process of arriving at the final answer or result. (Remember: I cannot guess what you are thinking, let me know your thought process for at least a partial credit.)
- You can use both sides of the exam booklet if needed. You are not allowed to add any extra sheets of paper. If you need more sheets, ask me.
- Write succinctly. A 'long' answer does not mean a 'better' one.
- **Write legibly**. **Illegible answers will earn no points.**
- You have 60 minutes to complete the exam.

Good luck!

First Name:_____ LAST Name:_____

1. [5+5 pts] a) Define vulnerability / threat / controls.
b) Illustrate all three notions with a single system, and point vulnerability / threat / controls in the system.

[Sec.1, Slide XX]

a) Vulnerability - def.: a weakness in a security system
Threat - def.: circumstances that have a *potential* to cause harm
Controls - def.: means and ways to block a threat, which tries to exploit one or more vulnerabilities

b) Example: The City of New Orleans
vulnerabilities: location of the city below water level
threats: hurricanes, earthquakes, terrorist attacks, …
controls: e.g., dams for hurricanes and earthquakes; security forces for terrorist attacks

2. [5+5 pts] a) Define in your own words *Principle of Weakest Link.*
b) Define in your own words *Principle of Adequate Protection*.

[Sec.1, Slides XXX and 59]

Principle of Weakest Link:

Security can be no stronger than its weakest link.

OPTIONAL: Whether it is the power supply that powers the firewall or the operating system under the security application or the human, who plans, implements, and administers controls, a failure of any control can lead to a security failure.

Principle of Adequate Protection:
Computer items must be protected to a degree consistent with their value and only until they lose their value.

3. [5 pts] Explain clearly and succinctly (briefly) what are GSSAPI and CAPI.

[Sec.2, Slide 32]

They are interfaces for security and cryptographic routines or services.

Optional (more detail):

- API = Application Programming Interface
- GSSAPI (Generic Security Services API) = template for many kinds of security services that a routine could provide
- CAPI (Cryptographic API) = Microsoft API for cryptographic services

4. [5 pts] Name at least 4 network characteristics that increase security risks.

[Sec.2, Slides 39-41]

Naming just 4 of the following 7 network characteristics that increase security risks is sufficient:

1) Attacker anonymity

2) Many points of origin and target for attacks
3) Resource and workload sharing
4) Network complexity
5) Unknown or dynamic network perimeter
6) Uknown paths between hosts and users
7) Nonuniform security policies/mechanisms for hosts belonging to multiple networks

5. [5 pts] Name at least 4 techniques used as threat precursors.

[Sec.2, Slides 39-47]
Naming just 4 of the following 7 threat prescursors techniques is sufficient:

1) Port scan
2) Social engineering
3) Reconnaissance
4) OS and application fingerprinting
5) Using bulletin boards and chats
6) Getting available documentation

6. [15 pts] a) [5 pts] Explain what is ICMP.
b) [10 pts] Give a clear and succinct example showing how the echo-chargen DoS attack uses (really: abuses) ICMP.

[Sec.2, Slides 84-85]
a) ICMP – is Internet protocol for system diagnostic
OPTIONAL: ICMP = Internet Control Msg Protocol

b) Echo-chargen attack
OPTIONAL: *chargen* protocol – generates stream of packets; used for testing network

Just one example is sufficient:
- Echo-chargen attack example 1:
(1) attacker uses chargen on server X to send stream of *echo request* packets to Y
(2) Y sends *echo reply* packets back to X; this creates endless „busy loop" beetween X & Y

- Echo-chargen attack example 2:
(1) attacker uses chargen on X to send stream of *echo request* packets *to X*
(2) X sends *echo reply* packets back to itself

7. [15 pts] a) [10 pts] Explain what is a *packet dropping* attack and how it works.
b) [5 pts] What is a *black hole* attack?

[Sec.2, Slide 92]
a) OPTIONAL: This is DoS attack by Redirecting traffic

Normally:

- Routers find best path for passing packets from S to D
- Routers advertise their connections to their neighbors

Example of traffic redirection attack:

- Router R taken over by attacker
- R advertises (falsely) to all neighbors that it has the best (e.g., shortest) path to hosts H1, H2, ..., Hn
- Hosts around R forward to R all packets addressed to H1, H2, ..., Hn
- R drops *some* or *all* these packets

drops *some* => packet-dropping attack

b)

drops *all* => black hole attack

(=> black hole attack is spec. case of pkt-drop. attack)

8. [5 pts] What are risks of downloading Active X controls (code)?

[Sec.2, Slide 107]

Risks of downloading ActiveX controls:

After object of type T is downloaded:

a) If handler (or viewer) for type T is available, it is invoked to present object T ←RISK

- E.g., after file.doc downloaded, MS Word is invoked to open file.doc ← BIG security risk!

b) If no handler for type T exists on C, C asks S for handler for T ←RISK

Then uses handler to present object T ←RISK

- E.g., attacker defines type .bomb

  After file.bomb is downloaded by C, C asks S for handler for type .bomb! ← HUGE security risk!

9. [5 pts] Explain the meaning of the following requirement for a correct keyed cryptosystem:

$$P = D(K_D, E(K_E, P))$$

[Sec.3, Slides 9 and 11]

This means that the keyed cryptosystem allows to get back the original plaintext from the corresponding ciphertext.

OPTIONAL:

In more detail, it means that after: (1) applying the *encryption* with key K_E to the plaintext P; and then (2) applying the *decryption* with key K_D to the ciphertext obtained in Step 1; we obtain the original plaintext.

10. [10 pts] Contrast keyless, symmetric, and asymmetric cryptography w.r.t. their use of keys.

[Sec.3, Slide 12]

1) Keyless cryptosystems – do not use cryptographic keys (e.g., Caesar's cipher - below)

First Name:_____ LAST Name:_____

2) Keyed cryptosystems

2a) Symmetric cryptosystems: $K_E = K_D$

OPTIONAL: This means that encryption and decryption use the same key, or one key is easily derived from other.

2b) Asymmetric cryptosystems: $K_E \neq K_D$

OPTIONAL: A.k.a. a public key system

This means that encryption and decryption use different keys and it computationally infeasible to derive one key from the other.

11. [15 pts] Give a clear example of using 2-key substitution cipher for P = "SPRING BREAK".

[Sec.3, Slide 32]