CS 5950/6030: Network Security — Fall 2005

M A S T E R

Please note that answers are more detailed than required for full credit.
This is in order to give you a credit for any partial answers (e.g., if you include one subcase for, say, the case of limitations of testing, you get a credit for the full case).

Midterm Exam
-- Version 2 –

First Name _____ Last Name: _____

Row_____ Seat _____

>>> Please do NOT open this exam booklet until <<<
>>> the instructor gives a clear signal to start. <<<

Question Nr	Max. Score	Your Score	Comments
1	5		
2	10		
3	15+10		
4	10		
5	20		
6	10		
7	10		
8	10		
9	10		
TOTAL	**100+10**		

Notes:

- Sign the front page now. After the signal to start, sign *all* pages.
- You can use both sides of exam booklet if needed.
- You may have 1 sheet of notes, front and back. **>>> If you plan to use an extra sheet, you must sign it now! <<<** Turn in the sheet of notes with your exam.
- If you are unsure of a question, write down your assumptions regarding the question. Remember, I cannot guess what you are thinking, let me know your thought process for at least partial credit.
- Write clearly. Illegible answers will not be graded.
- You will have 45 minutes to complete the exam.

Good luck!

First Name:_____ LAST Name:_____

1. [5 pts] Define in your own words Principle of Easiest Penetration.

An intruder must be expected to use any available means of penetration, attacking weak link. The penetration may not necessarily be by the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.

2. [10 pts] Compare DES and AES encryption using the criteria listed in the table below. Enter D (for DES) or A (for AES) into the second column to indicate which encryption type is better under a given criterion. Enter a brief explanation into the 3rd row.

Criterion	**D or A better?**	Why?
block size	A	**Allows larger block sizes for faster coding.**
key length	A	**Allows longer keys.**
selection process	A	**Secret selection process but accepted public comments.**
source code availability	**A**	**Publicly available code.**

3. [15 pts+extra]
   [15 pts] Give an example scenario of sending and receiving a digitally signed msg. It can be a solution which does *not* provide message encryption.
   [EXTRA: 10 pts] For an extra credit, show both a scenario without message encryption and with message encryption.

Any of the two solutions above are sufficient for 15 pts. Both must b presented for 25 pts.

S = sender
R = receiver

Unencrypted message signed

- Original message: P (plaintext)
- Signing: $Sg = Sg(S, P) = D(P, K_{PRIV\text{-}S})$
- Sent message: [P, Sg]

- Received msg = sent message: [P, Sg]
- R verifies signature Sg with S's public key $K_{PUB\text{-}S}$:
  if $E(Sg, K_{PUB\text{-}S}) = P$, then signature is valid
  bec. $E(Sg, K_{PUB\text{-}S}) = E(D(P, K_{PRIV\text{-}S}), K_{PUB\text{-}S}) = P$

First Name:_____ LAST Name:_____

Encrypted message signed

- Original message: P (plaintext)
- Encryption: C = E(P, K_{PUB-R})
- Signing: Sg = Sg(S, C) = D(C, K_{PRIV-S})
- Sent message: [C, Sg]

- Received msg = sent message: [C, Sg]
- R verifies signature Sg with S's public key K_{PUB-S} :
  if E(Sg, K_{PUB-S}) = C, then signature is valid
  bec. E(Sg, K_{PUB-S}) = E(D(C, K_{PRIV-S}), K_{PUB-S}) = C
- R decodes C with R's private key K_{PRIV-R}: P = D(C, K_{PRIV-R})

First Name:_____ LAST Name:_____

4. [10 pts]
   a. [5 pts] Explain the testing program behavior approach to judging program security.
   b. [5 pts] What are the shortcomings of the testing program behavior approach?

For a)

Compares program behavior (displayed during testing) vs. its requirements.
If behavior is consistent with requirements => security is judged as good.

For b)

Problems include:

--Limitations of the "power" testing

Can't test exhaustively
Testing checks what the pgm should do
Can't test what the pgm should *not* do
i.e., can't make sure that pgm does *only* what it should do – nothing more

--Program complexity is malicious attacker's best friend.

Too complex to model / to test
Exponential # of pgm states / data combinations
a faulty line hiding in 10 million lines of code

--Evolving technology

New s/w technologies appear
Security techniques catching up with s/w technologies

5. [20 pts]
   a. [15 pts] Write a detailed scenario showing incomplete mediation.
   b. [5pts] Explain how attacker can achieve her goals.

For a)

URL to be generated by *client's browser* to access server, e.g.:
http://www.things.com/order/final&custID=101& total=205
Instead, *user* edits URL directly, changing price and total cost as follows:
http://www.things.com/order/final&custID=101&total=25

For b)

By using the above scenario, user can use forged URL to access server.
In the above example, the server takes $25instead of $205 as the total cost.

First Name:_____ LAST Name:_____

6. [10 pts] Describe in a sufficient detail an example of a timing covert channel.

Example:

- Multiprogramming system „slices" processor time for programs running on the processor.
- 2 processes only: Trojan (Program w/ Trojan) and Spy Program.
- Trojan receives all odd time slices for its use (can abstain).
- Spy Program receives all even time slices for its use (can abstain).
- Trojan signals Xk=1 by using its time slice;
  signals Xk=0 by abstaining from using its slice

7. [10 pts]
   a. [5 pts] Explain the recovery block technique for fault tolerance.
   b. [5 pts] How can it improve security?

   For a)
   A program module (e.g., sorting module) includes at least two versions of code.
   First primary code is executed first (e.g., quick sort). If its result passes acceptance test checking that elements are sorted), the result is accepted.
   Otherwise the secondary code (e.g., bubble sort) is executed.

   For b)
   Even if an attacker penetrates quick sort code, the acceptance test discovers its failure and calls the bubble sort code. If bubble sort code is not penetrated, the module as a whole will give a correct result.

8. [10 pts] Explain using access control matrices (ACMs) for object access control using an example ACM.

Subjects and objects as shown in the matrix (table).

	Object 1	Object 2	Object 3	Object 4	Object 5
Subject A	OWR	R	OWR	WR	-
Subject B	R	OWR	-	OWR	OWR
Subject C	R	R	-	WR	-
Subject D	R	-	-	WR	-
Subject E	-	R	-	WR	R

:t 5.

First Name:_____ LAST Name:_____

9. [10 pts]
   a. [5 pts] Explain the per-object and per-user protection approach for file protection.
   b. [5 pts] What are its advantages and disadvantages?

For a)
File owner specifies access rights for *each file* he owns for *each user*.
(It can be implemented with access control list or access control matrix.)

For b)
Advantages:
--Fine granularity of file access
--Allows to create groups of users with similar ARs

Problem:
--Complex to create and maintain groups
(File owner's overhead to specify access rights for *each file* for *each user*.)