

Information Assurance: Final Exam – Key December 11, 2006

Multiple Choice – 2 points each

1. *Mechanisms used to access resources should not be shared.* This is a definition for which Salzer and Schroeder's Design Principle.
 - a. Principle of Least Privilege
 - b. Principle of Safety
 - c. Principle of Economy of Mechanism
 - d. *Principle of Least Common Mechanism*

2. The Trusted Platform Module (TPM) can create a sealed bound message. What does this involve?
 - a. *Encrypt the message with a non-migrateable, public key associated with the target TPM and include PCR values that must be met before the target TPM will decrypt the message.*
 - b. Encrypt the message with a non-migrateable, private key associated with the source TPM and include PCR values that must be met before the target TPM will decrypt the message.
 - c. Encrypt the message with a symmetric key shared with the target and source TPM and include PCR values that must be met before the target TPM will decrypt the message.
 - d. Encrypt the message with a non-migrateable, public key associated with the target TPM.

3. Which of the following is the best definition of slack space?
 - a. The area of MySpace where the slackers hang out.
 - b. *Unused area on the last block of disk assigned to a file.*
 - c. Blank pages within a word document.
 - d. Associated streams on the NT File System.

4. The Encapsulating Security Payload (ESP) protocol in IPSec allows:
 - a. Encryption but not integrity checks.
 - b. Integrity checks but not encryption.
 - c. *Encryption and integrity checks.*
 - d. Compression and encryption.

5. The legal foundation of our privacy protection is:
 - a. 9th amendment
 - b. Communications Assurance for Law Enforcement Act (CALEA)
 - c. *4th amendment*
 - d. PATRIOT Act

Net ID:

6. Which of the following is the best definition of risk?
 - a. The identification of a weakness in the system.
 - b. Likelihood that an entity will attack the system.
 - c. A board game from Hasbro.
 - d. *Probability that a threat will exploit a vulnerability.*

7. A good encryption algorithm results in cipher text that appears random. Changes to the key are not easily correlated to the cipher text. This property is called:
 - a. *Avalanche effect*
 - b. Feistel Network
 - c. Pigeonhole principle
 - d. Differential Cryptanalysis

8. *Made an error in writing this question. Meant to ask about Biba's low-water mark policy. In this case the answer is c. Everyone got 2 free points on this one.* In Biba's Ring Model, which of the following is true?
 - a. On a read, the subject's level is set to that of the object.
 - b. On a write, the object's level is set to that of the subject.
 - c. On a read, the subject's level is set to the level of the object if the object's level is less than the subject.
 - d. A subject is allowed to read an object only if the object has the same or higher integrity than the subject.

9. In which of the following situations is it legal to monitor network traffic?
 - a. Dana hacked into Tara's computer, and Dana is watching Tara's instant message traffic.
 - b. *Dana hacked into Tara's computer, and Tara is watching Dana's IRC traffic from the hacked machine.*
 - c. Tara is at a coffee shop with unencrypted wireless and is sniffing traffic from Dana's machine.
 - d. Dana and Tara are both logging into a common server owned by the University, and Tara has gained access to observe Dana's instant message traffic from that machine.

10. Which of the following is **not** a reasonable protection against online brute force password attack?
 - a. Slowing response after each failed attempt.
 - b. Locking out the account after a fixed number of failed attempts.
 - c. Measure key entry speed to determine whether a human is entering the password, and fail the attempt if the key speed does not what is expected from a human.
 - d. *Adding salt to the password.*

Net ID:

11. Which of the following is best described as a policy instead of a mechanism?
 - a. Fingerprint readers will be installed at the computing labs.
 - b. *Students should be allowed access to the University's computing resources.*
 - c. Wireless access points will be installed across the campus.
 - d. Students will be assigned pronounceable, generated passwords once every six months.

12. Which of the following is true of the HRU Access Control Matrix model?
 - a. You can prove the safety properties of policies expressed in the model.
 - b. It is an efficient implementation model.
 - c. *You can embed many access control policies in the model and compare them on a common footing.*

Net ID:

Short answer

13. (6 points total) Gary's new computer has a CPU with a no-execute bit which is exposed through the Data Execution Prevention (DEP) feature in the Windows operating system. Gary wisely enables DEP.
- Identify one malware exploit that is thwarted.

In general the OS will use the DEP bit to turn off execution of the stack segment. This will foil stack smashing attacks.

- Identify one malware exploit that is still possible.

Return to libc is not affected. You cannot turn off the executability of the library code segment.

14. (10 points) Consider the ring memory protection scheme implemented by the Intel architecture. Use *action* => *condition* constraints to derive what must be logged during each data segment access so an auditor would have sufficient information to ensure that the ring policy is correctly enforced. Be sure to show the constraints in addition to the required logged values.

Ring architecture data access rules.

- $CPL \leq DPL$
- $RPL \leq DPL$

Current and requested privilege levels are at least as privileged as the data segment privilege level if not more so.

Access data segment => $CPL \leq DPL \ \&\& \ RPL \leq DPL$

Therefore, on each data segment access, should log CPL, RPL, and DPL, whether the access succeeded. Should also log the segment ID's in case there is a discrepancy that the auditor must track down.

Net ID:

15. (9 points) Anwen is shopping for a high assurance network tunnel device for her company. She is considering the following products which have Common Criteria evaluations. Based on the basic Common Criteria information from each product, how would you counsel Anwen on the different products?
- a. Product A – Evaluated at EAL 4 based on a specialized security target.

Must examine the security target carefully to determine what functionality the product is claiming. Since it is not using a protection profile it is not as easy to compare against other products. The EAL is mid level and is probably satisfactory for most applications.

- b. Product B – Evaluated at EAL 6 against a security target based on the Labeled Security Protection Profile (LSPP).

While this is evaluated at a high assurance level, the functionality of a trusted operating system (generally what uses the LSPP) may not be appropriate for this network security device. Again will need to carefully consider what functionality the product is claiming.

- c. Product C – Evaluated at EAL2 against a security target based on the Configurable Security Guard (CSG) Protection Profile . Anwen notes that highly regarded Product D in this space is evaluated against the same protection profile. Unfortunately for a variety of non-technical reasons, she cannot consider Product D.

The use of a common protection profile helps us compare the functionality of this product with other well respected products in the field. The lower EAL 2 assurance level would have me concerned. While it is probably implementing what we need, it may not be sufficiently tested and reviewed to meet our assurance needs.

Net ID:

16. (6 points) Erna is concerned about competitors using emanations scanning to learn about cutting edge research occurring in her lab. She already runs her lab with strong restrictions on physical access. Advise her on two additional techniques she can use to protect herself from emanation scanners.

She can use electromagnetic shielding to protect individual computers, labs, or even whole buildings.

She can use fonts with lower frequencies.

She can avoid the use of dithers in displays.

She can ensure that monitors are turned off at night, so there is not the possibility of viruses using odd displays to send out information when no one is watching.

She can divide sensitive and less sensitive devices and use physical separation to limit what a sensitive device could leak to a less sensitive device.

17. (6 points) List three types of evidence that can be gathered during development to provide assurance of the trustworthiness of the product.

- *Design and architecture documents ranging from information to semi-formal to formal.*
- *Proofs of correctness based on the architecture model.*
- *Test suite descriptions and test suite results.*
- *Descriptions of code development environment, e.g., use of source control and code reviews.*

Net ID:

18. (10 points) Imagine that Alice, Bob, Carol, and David have just eaten dinner. The waiter informs them that an anonymous party has paid the bill. One of Alice, Bob, Carol, and David did pay the bill but is too modest to admit it. The diners want to know of one of their party paid the bill, or if the shadowy Eve sitting at the bar did, so they engage in the Dining Cryptographer's protocol. The result of the coin flips is shown below.

Name	Coin Flip	Public Answer	Observed Neighbor
Alice	Head	Different	David
Bob	Head	Same	Alice
Carol	Tail	Different	Bob
David	Tail	Different	Carol

a) Given the global view of the coin flips, who paid?

David

b) Select one of the non-payers, and show that that diner cannot guess the identity of the payer with better than uniform probability. Hint: try constructing a table like the one above.

Take Alice's point of view. She knows the value of her flip and Davids. She knows what everyone reported in public.

For the two hidden coin flips, there are four possibilities. One of the combinations will only happen if Alice lies. Alice knows that she didn't lie. That leaves three other possibilities, and each one matches a different co-dinner, so Alice doesn't have any information to bias her guess as to which dinner paid. The three tables includes the original table above where David lied. The other two options are below.

Assume Bob lies

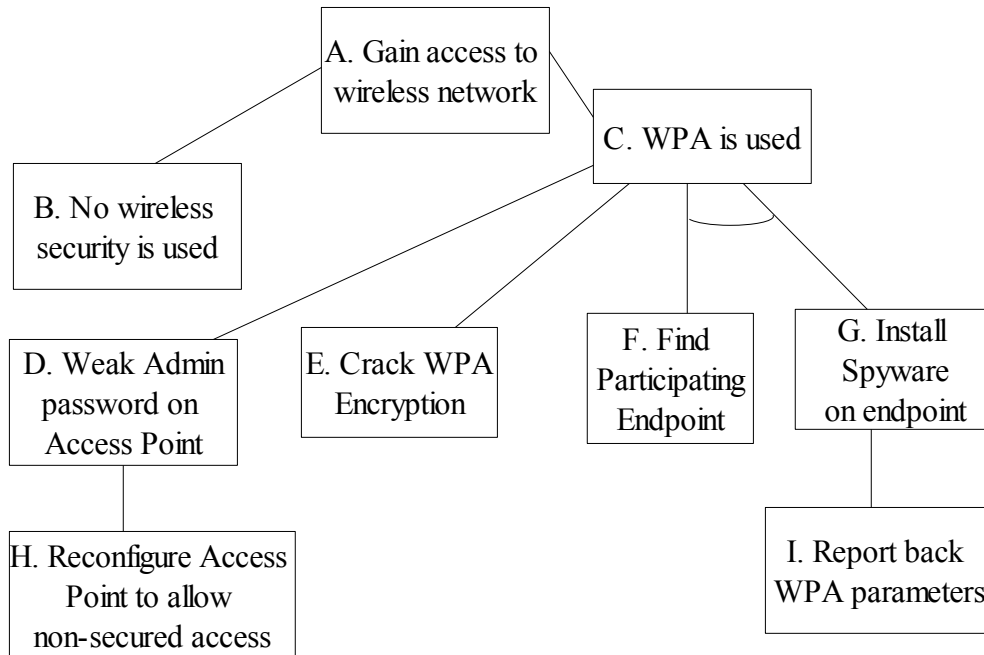
<i>Name</i>	<i>Alice's guess of flip</i>	<i>Public Answer</i>	<i>Observed Neighbor</i>
<i>Alice</i>	<i>Head</i>	<i>Different</i>	<i>David</i>
<i>Bob</i>	<i>Tail</i>	<i>Same</i>	<i>Alice</i>
<i>Carol</i>	<i>Head</i>	<i>Different</i>	<i>Bob</i>
<i>David</i>	<i>Tail</i>	<i>Different</i>	<i>Carol</i>

Net ID:

Assume Carol lies

<i>Name</i>	<i>Alice's guess of flip</i>	<i>Public Answer</i>	<i>Observed Neighbor</i>
<i>Alice</i>	<i>Head</i>	<i>Different</i>	<i>David</i>
<i>Bob</i>	<i>Head</i>	<i>Same</i>	<i>Alice</i>
<i>Carol</i>	<i>Head</i>	<i>Different</i>	<i>Bob</i>
<i>David</i>	<i>Tail</i>	<i>Different</i>	<i>Carol</i>

19. (10 points) Consider the following threat tree.



a. Enumerate the distinct threat paths in the tree.

A->B
A->C->D->H
A->C->E
A->C->F->G->I

b. Identify a set of actions that will mitigate all of the threats identified in the tree.

Mitigate B, by enabling some form of wireless security.
Mitigate D by having a strong administrative password on the access point. Exercise good password practices with your network devices.
Mitigate E, keep up to date on efforts to crack WPA. Unless you are using short keys, the WPA protocols to date have been sound.
Mitigate F, by ensuring that any device participating in your wireless network is clean and is operating with good security procedures.

Net ID:

20. (3 points) What are the security fundamentals identified by CIA?

C – Confidentiality

I – Integrity

A - Availability

21. (8 points) Identify each security scenario as primarily dealing with C, I, or A.

- a. TotallyThomas shopping web site crashes during the holiday season due to customer overload or extra traffic from DominantlyDiesel.

A

- b. Customer knows that he is ordering from TotallyThomas.

I

- c. The TotallyThomas web site provides trustworthy information to its customers.

I

- d. TotallyThomas protects its cutting edge research from competitors.

C

Net ID:

22. (8 points) Compare the following labels using the Bell-LaPadula confidentiality policy and indicate what access is allowed: read-only, write-only, both, or none. The levels are: Supreme \geq High \geq Normal \geq Low.

a. Subject label = Supreme: {A,B} Object Label = Normal: {A}

Read-only

b. Subject Label = Normal: {A,C} Object Label = High: {B,C}

none

c. Subject Label = Normal: {A} Object Label = High: {A,B}

Write-only

d. Subject Label = High: {A} Object Label = High: {A}

Both

23. (10 points) Consider Alice's RSA key pair where $p = 7$ and $q = 11$, $e = 17$ and $d = 53$.

a. What is n ?

$$n = p * q = 77$$

b. What is $\Phi(n)$?

$$\Phi(n) = (p-1)*(q-1) = 60$$

c. What is the rule that e and d satisfy to be a valid RSA key pair?

$$e*d \text{ mod } \Phi(n) = 1$$

$$17*53 \text{ mod } 60 = 1$$

d. What is the equation you would solve to encrypt message, m , to Alice?

$$m^e \text{ mod } 77$$

e. What is the equation Alice would solve to sign message, m ?

$$m^d \text{ mod } 77$$

Net ID:

24. (4 pts) Consider the different modes of AES.

a. List one block-based mode.

- *Cipher Block Chaining*
- *Electronic Code Book*

b. List one stream-based mode.

- *Output Feedback*
- *Cipher Feedback*
- *Counter Mode*

25. (6 points) Consider the Vigènere cipher.

a. Use this cipher to encrypt “Bob is good” using the key “Alice”. Assume $a=0$.

Alice = 0 11 8 2 4

Bob is good = 2 14 2 8 18 6 14 14 3

Encrypted = 2 25 10 12 22 6 25 22 5

b. Is the Vigènere cipher an example of a:

- i. *Substitution cipher*
- ii. *Transposition cipher*,
- iii. *Product cipher*

Net ID:

26. (10 points) Bert receives the following PGP certificate from Ernie:

Bob(l),Count(h),Maria(l)<<Ernie>>

Where Bob(l) means that Bob signed the certificate with low assurance and Count(h) means Count signed with high assurance.

Bert gathers the following certificates:

Elmo(h),Snuffy(h)<<Count>>

Oscar(h),Snuffy(l)<<Bob>>

In addition, Bert has signed the following certificates himself:

Bert(h)<<Maria>>

Bert(h)<<Elmo>

Bert(l)<<Oscar>>

(a) What are the signature chains that Bert can use to convince himself that Ernie's certificate is trustworthy?

1. *Bert signed Maria with high assurance. Maria signed Ernie with low assurance.*
2. *Bert signed Elmo with high assurance. Elmo signed Count with high assurance. Count signed Ernie with high assurance.*
3. *Bert signed Oscar with low assurance. Oscar signed Bob with high assurance. Bob signed Ernie with low assurance.*

(b) Which chain is the best proof? Why?

Chain 2, Bert to Elmo to Count is the best proof. Each signature in the chain is of high assurance not just a casual acquaintance.