

**University of Illinois at Urbana-Champaign
Department of Computer Science**

Midterm 2 – Answers and Comments
CS461/ECE422 – Computer Security I
Fall 2008

Wednesday, November, 2008

Multiple choice (2 points each)

1. Which element of Bell-LaPadula's confidentiality model addresses the no read up constraint?
 - a) Basic Security Theorem
 - b) *Simple security condition*
 - c) *-property
 - d) †-property

2. What is needed by law enforcement to access stored electronic data such as e-mail?
 - a) Wire tap warrant
 - b) *Search warrant*
 - c) Consent of service provider
 - d) Probable cause

3. Which of the following classes/levels specifies the highest level of assurance?
 - a) Common Criteria EAL4
 - b) *Common Criteria EAL6*
 - c) TCSEC class C2
 - d) TCSEC class B1

4. In which integrity model is the integrity level of the subject changed upon reading a lower integrity object?
 - a) Biba ring model
 - b) Biba strict model
 - c) *Biba low water mark model*
 - d) Clark-Wilson model

5. Object reuse is a functionality requirement identified by TCSEC and Common Criteria. Which of the following is the best definition for object reuse?
 - a) *Zero out objects before the object is reused by another entity.*
 - b) Reuse the same object across multiple program invocation.
 - c) Ensure that access control rules are checked on each object access.
 - d) Reuse the same object between processes for secure communication.

6. Which best defines the DNS Baliwick constraint?
 - a) The DNS implementation should not accept results from the additional information section of the DNS response.
 - b) The DNS implementation should only accept one element in the additional information section of the DNS response.
 - c) The DNS implementation should randomize the source port on each request.
 - d) *The DNS implementation should only accept results from the additional information section of the DNS response if the additional information is from the same domain as the original request.*

7. Which best defines the allowed relationship of the Clark-Wilson requirements?
 - a) *The definition of which users can invoke which transaction procedures on what constrained data items.*
 - b) The definition of which transaction procedures can operate on which constrained data items.
 - c) The definition of which users can invoke which transaction procedures.
 - d) The definition of which users can invoke which transaction procedures on what unconstrained data items.

8. Which style of intrusion detection system will be most likely to identify a zero-day exploit?
 - a) Signature-based or mis-use detection
 - b) Inline intrusion detection or intrusion protection system
 - c) *Anomaly or statistical detection*
 - d) Packet filtering

9. Canary values can be used to protect from exploits of which common programming error?
 - a) Time of use to time of check error.
 - b) Improper input cleansing.
 - c) Logical error.
 - d) *Buffer overflow.*

10. Which software development process is best suited to generating assurance information?
 - a) Extreme programming model
 - b) Elbonian programming model
 - c) Prototyping
 - d) *Waterfall model*

Short Answer

11. Many techniques can be used to improve assurance during the life cycle of a product. For each technique listed below, describe how it can be used to improve product assurance and identify what part of the product life cycle it is more relevant for. (3 pts each, 6 points total)

a) Source control

This one ended up not being graded. Everyone just got three points for this part. I was intending this to mean a source control tool like subversion or clear case. A large number of folks didn't catch that meaning. Finally, I realized that the text and slides used the term configuration management. Since I was using an equivalent term that wasn't used in class, I didn't feel it was fair to grade you on it.

The answer I was looking for was that source control (configuration management systems) provide a measure of assurance during the development or manufacturing phase. The source control system provides a means of determining who changed source code when. Often times source can only be checked in after a code review making it difficult for people to check in obviously buggy or malicious code.

A source control system can also help during the maintenance phase. By saving the versions of the files used to build each system, any particular version can be rebuilt.

b) Installation and getting started manuals

Theses manuals provide assurance during the deployment or fielded product phase.

With the installation manual the user can learn how to appropriately configuration and install the product increasing its operational assurance.

12. Consider the following subjects, objects and labels.

Subject	Subject Label	Object	Object Label
Alice	High: {c1,c2}	Apple	Med: {c2}
Bob	Med: {c1,c2}	Banana	Low: {c1,c2}
Carol	Low: {c1}	Cookie	High: {c1}
Dave	High: {c1}	Donut	Med: {c1}

- a) (3 pts) Interpret the labels as security labels in the BLP model. What accesses should the subjects have on the specified objects: read, append (pure-write)?

Subject	Object	Access
Alice	Cookie	<i>read</i>
Bob	Cookie	<i>none</i>
Dave	Donut	<i>read</i>

- b) (3 pts) Interpret the labels as integrity labels in the strict Biba model. What accesses should the subjects have on the specified objects: read, append (pure-write)?

Subject	Object	Access
Bob	Donut	<i>append</i>
Carol	Banana	<i>read</i>
Dave	Banana	<i>none</i>

- c) (3 pts) Now assume that BLP system supports security clearances. How would this change the accesses from part a)?

Subject	Clearance	Object	Access
Alice	High: {c1,c2}-High: {}	Cookie	<i>Read, append</i>
Bob	Med: {c1,c2}-Med: {}	Cookie	<i>append</i>
Dave	Low: {c1}-Low: {}	Donut	<i>append</i>

- d) (2 pts) Does the system in part c implement strong, weak, or no tranquility? Why?

Since the subject label can change within the clearance range, this system does not have strong tranquility.

If moving within the clearance range keeps the system within the security policy constraints, this system implements weak tranquility.

Since we haven't specified the security policy constraints, you could argue there is no tranquility.

13. This question considers worms.

- a) (2 pts) In the classic worm, address scanning can be used to identify potential victims. In an IPv4 environment, how many potential victim addresses can be searched?

32 bits of address space so 2^{32} addresses are possibility (within a constant to address non host addresses such as multi cast and of course the address of the attacking host).

- b) (2 pts) In flash worms, the victim identification phase and actual propagation phases are separate. What is one benefit of the separation for the attack?

In a separate identification phase, the scans can operate much more slowly and be likely likely to be noticed by intrusion detection systems.

With a list of already identified real potential victims, the attack phase can go much faster. So fast, that the attack can complete across the entire Internet before anyone can really react to it.

- c) (3 pts) Assume a service on a computer is exploited. How can an integrity level help limit the impact of the exploit?

If the exploited service is running at a low integrity level, the exploit will not be able to write higher integrity data (assuming a Biba integrity model). Thus critical system is probably safe.

- d) (3 pts) How can fine-grained privileges help limit the impact of an exploited service?

Privileges are ways a process can operate outside the normal security model. Root in Unix is an extreme version of privilege where the root user does not follow any of the security model constraints. If the privileges are divided into finer divisions a process can run with only the privileges it needs (ideally no privileges). If the service is running with only a few exceptions to the security policy, the exploit will only run with those security policy exceptions rather than running with no security constraints as it would in the root model.

A lot of folks confused privileges with access control. Privileges can turn off access control checks, but they are not the same thing.

14. Suppose a database for a department store contains an 'employee' table listing all employees' names, e-mail addresses, SSNs, salaries, hiring dates, and departments. The employee table rows for three employees is shown below

Name	Email	SSN	Salary	Hired	Department
Alice	alice@mart.com	xxx-xx-xxxx	\$10	1/1/2005	Appliance
Bob	bob@mart.com	yyy-yy-yyyy	\$15	7/11/1997	Shoes
Carol	carol@mart.com	zzz-zz-zzzz	\$20	11/11/2001	Hardware

- a) (3 pts) Suppose you are the database administrator. Your company has a policy that each employee can see the names, e-mails, and hiring dates of all other employees in the same department. Show the SQL statements for these three employees to enforce this policy. (Your SQL does not have to be exact, but it should be clear what you mean.)

```
create view app_view as select ( name, email, hired) from 'Employee'
where 'Department=Appliance';
grant select on app_view to Alice;

create view app_view as select ( name, email, hired) from 'Employee'
where 'Department=Shoes';
grant select on app_view to Bob;

create view app_view as select ( name, email, hired) from 'Employee'
where 'Department=Hardware';
grant select on app_view to Carol;
```

- b) (3 pts) The company policy states that every employee should be able to view all fields about themselves in the 'employee' table. Show the SQL statements you would use to enforce this policy.

```
create view alice_view as select * from 'Employee' where 'Name=Alice';
grant select on alice_view to Alice;

create view bob_view as select * from 'Employee' where 'Name=Bob';
grant select on bob_view to Bob;

create view carol_view as select * from 'Employee' where 'Name=Carol';
grant select on carol_view to Carol;
```

- c) (3 pts) The company policy further states that an employee may choose to share this information with other employees of the company. How would you amend your answer in part b to enable an employee to allow other employees to view his or her non-public information in the 'employee' table?

Add the 'with grant option' at the end of the grant statements in part b.