NetID:

University of Illinois at Urbana-Champaign
Department of Computer Science

Midterm 2 – Answers and Comments
CS461/ECE422 – Computer Security I
Fall 2009
Wednesday, November 18, 2009
Time Limit: 50 minutes

Multiple choice (3 points each)

1. What is the legal basis for expectation of privacy in the United States?
   a) Gramm-Leach Bliley Act
   b) Electronic Communication Privacy Act
   c) 1st Amendment
   d) 4th Amendment

2. Which of the following is the most valid reason (from the perspective of using trustworthy systems) for a US government agency to reject a product evaluated against the Common Criteria?
   a) The product's security target includes some functionality targets that are not needed by the government agency
   b) The product's security target was based on a protection profile.
   c) The product was not evaluated at a sufficiently high EAL for the needs of the government agency.
   d) The evaluation was performed in another country that is a member of the common criteria.

3. Which network control would be most effective for ensuring that malformed TCP packets do not reach your organization's desktop machines?
   a) Stateful inspection firewall
   b) Network intrusion detection system (NIDS)
   c) Segmentation
   d) Network sniffing

4. In what case is it not legal to track an individuals network communication?
   a) Service provider monitoring communication to ensure good operation of their system.
   b) Law enforcement with appropriate court order recording communication from the target identified in the court order.
   c) An individual running a packet sniffer at a coffee shop.
   d) An individual who has had her system attacked and is tracking the communication of the attacker.

5. Which Biba integrity model is the dual of the Bell-LaPadula Model?
   a) Low-Water-Mark policy
   b) Ring Policy
   c) Strict Integrity Policy
   d) All three of them

6. What best defines an "information transfer path"?
   a) When data in an object can be transferred into another object along an information flow path by a succession of reads and writes.
   b) When a subject reads data from one object and writes it to another object.
   c) When a subject with high clearance can read objects from all clearances
   d) When auditors and managers can access both the system state and the logs.

7. Attacks such as SQL Injection and Cross-Site Scripting attacks are due to which common programming error?
   a) Insufficient bounds checks
   b) Time of check to time of use error
   c) Insufficient identification and authorization
   d) Incomplete user input checks

8. Syn flood is an attack against what level of the network stack?
   a) Data link (Layer 2)
   b) Network (Layer 3)
   c) Transport (Layer 4)
   d) Application (Layer 7)

Short Answer

9. Match the following malware types to the characteristics: (~~*18*~~ *20* points)

Messed up and didn't realize that the first two lines were supposed to be a malware and definition. In fact the "good" definition for "virus" had been removed. Everyone got two points for the Virus definition.

Virus	Allows unauthorized access to functionality
Polymorphic Virus	An exploit that has no patch available
Macro Virus	Code that allows unauthorized quick access at a later time.
Trojan Horse	Contains unexpected covert effect
Logic Bomb	Hooks standard OS calls to hide data
Time Bomb	Instructions interpreted rather than executed
Trapdoor	Produces varying but operationally equivalent copies of itself
Worm	Propagates copies of itself through a network
Rootkit	Triggers action when condition occurs
Zero Day Exploit	Triggers action when the specified time occurs

10. Examine the following SQL statements. Match them with the most appropriate description. There will be an extra SQL statement. (8 points)

Note: that the grading matrix said 10 points for this question, but 8 points on the question was correct.

SQL Statements:

```
a)      grant select, update on employee_table('name', 'email',
   'phone') to Alice with grant option;
b)      create view Info as select * from employee_table where name =
   'Alice';
   grant select, update on Info to Alice with grant option;
c)      revoke select on employee_table('name', 'email', 'phone') from
   Alice;
d)      create view Info as select * from employee_table where name =
   'Alice';
   grant select, update on Info to Alice;
e)      grant select on employee_table('name', 'email', 'phone') to
   Alice;
```

Descriptions:

I. *(d)* Give Alice the ability to read and write all of her employee data
II. *(e)* Give Alice the ability to see the public information of everyone in the company
III. *(b)* Give Alice the ability to read and write all of her employee data and enable others to read and write her employee data.
IV. *(c)* Remove Alice's ability to see the public information for the company

11. In class we discussed how the DHCP protocol is used to dynamically assign IP addresses to machines. (9 points)

a) Describe how an attacker can use the DHCP protocol to attack the registering machine.

In addition to the IP address, the clients often ask for the DNS and default gateway addresses.

An attacker can try to respond to DHCP requests faster than the legitimate DHCP server on the network and return either the DNS or default gateway address of their choosing. If they provide for the default gateway the address of a machine they control, all client communication to the outside world will be routed through that machine putting the attacker in the man-in-the-middle position.

Many people proposed sending bogus address in respond to a DHCP request, but were unclear on the actual attack, or specified MITM but didn't provide details of how responding to the DHCP request would get them in the middle.

Some people proposed Denial of Service (DoS) attacks. If they provided good arguments, this got full or most credit.

b) What is one limitation on the attacking machine?

The attacker must be in broadcast range of the client.

The client must ask for the default gateway or DNS address.

c) What is one way a client can protect itself from a DHCP attack?

The client can select a static IP address and avoid DHCP entirely.

The client can statically select his default gateway and DNS addresses.

The client can encrypt all traffic, so even if it is intercepted it will not be visible to the MITM.

12. In a Mandatory Access Control (MAC) system based on the Bell-LaPadula model, the subjects and objects in the system have the following security labels. The levels are ordered as High > Medium > Low

Subject	Subject Label	Object	Object Label
Alice	Low:{}	Xray	High:{Proj1}
Bob	High:{Proj1}	Yoyo	Medium:{}
Carol	Medium:{Proj1, Proj2}	Zebra	Low:{Proj1, Proj2}

a) Write an Access Control Matrix that shows the protection state of the system with these security labels considering the rights read(r) and append (a). (9 points)

	Xray	*Yoyo*	*Zebra*
Alice	*A*	*A*	*A*
Bob	*R,A*	*R*	
Carol		*R*	*R*

Some people added Alice, Bob, and Carol as columns. We didn't grade for those extra columns.

b) What is one security benefit of using a MAC model such as Bell-LaPadula instead of a Discretionary Access Control (DAC) model? (3 points)

The normal user cannot accidentally or maliciously bypass the security model of the system.

13. Assurance techniques can be used at different parts of a product life cycle. What specific assurance techniques would you use to address assurance concerns at the following points in the product life cycle? Describe how your proposed technique would address the issue. (9 points)

a) Resulting design does not meet the security requirements.

During the design phase do mapping of requirements to design elements.

If certain requirements do not map to any design elements, it will be clear before you reach implementation that particular security requirements are not adequately addressed.

b) Employee inserts untrustworthy code such as a back door during the development process.

Use a configuration management or source control system. The manager can review code changes that are checked in each day.

Employ code reviews before code is accepted into the official code base.

In both cases, another employee will be reviewing code changes at some point as they are made part of the official code base.

c) Untrustworthy code is inserted into the software image between the time the company publishes the program and the client takes delivery.

Provide a crypto hash of the system image on your companies web site that can be verified by your customer's. If the image has been corrupted it can be checked by the customers before installation.

Build your distribution media (e.g. DVDs) on site in a physically secure environment. If you control the physical site from development to physical production you reduce the possibilities for an untrusted entity to corrupt your software distribution.

14. Consider the following scenario.

Bank.com has set up an ebanking system. Customers connect to the banking server. The customer authenticates using either a password or a certificate and private key generated by an application from bank.com. Once the customer is authenticated against the banking server, he can view and update his account information. The client's access rights are checked on every transaction. Bank.com hired a cryptographer to design a new encryption scheme that can be used to ensure the confidentiality and integrity of data communicated between the client and the server. It is keeping the information about the new algorithm secret to limit the information available to the attacker.

a) Which of the eight design principles of Salzer and Schroeder does this scenario violate? (2 points)

Principle of Open Design. The cryptographic algorithm is not open for general review.

b) How does this violation affect the security of the system? (3 points)

The complex cryptographic algorithm has probably not had sufficient review, and may have some fairly simplistic weaknesses.

An attacker may discover the algorithm and discover and exploit an algorithmic weakness without telling the banking company.

c) How would you change the design to make it follow the design principle? (3 points)

I would either use a well reviewed cryptographic algorithm like AES, or I would put my new cryptographic algorithm up for review. I would probably use AES (or some similarly widely reviewed algorithm) in the short term, because it takes a while for a complex cryptographic algorithm to be sufficiently reviewed by the community.