NetID:

University of Illinois at Urbana-Champaign
Department of Computer Science

Midterm 2 – Comments and Answers
CS461/ECE422 – Computer Security I
Fall 2010

Multiple choice (3 points each)

1. An attacker takes advantage of an error in chess game server. He is able to execute code of his choice in the chess server process. The resulting shell process that he initiates is running as root. Beyond the error in the chess server, which Design Principle of Salzer and Schroeder did the game developer or the manager of the target system violate that enabled a root shell to be launched?
   a) Principle of Economy of Mechanism
   b) Principle of Separation of Privilege
   c) Principle of Least Privilege
   d) Principle of Psychological Acceptability

2. What is the difference between Biba's Low Water Mark Policy and Biba's Ring Policy?
   a) The Low Water Mark Policy resets the subject's integrity level to the minimum of the subject's original integrity level and the integrity level of the object read.
   b) In the Ring Policy the subject can only read objects at its integrity level or higher.
   c) In the Low Water Mark Policy, the subject can write objects at any integrity level.
   d) The Ring Policy resets the object's integrity level to the minimum of the object's original integrity level and the integrity level of the reading subject.

3. Which of the following is the most appropriate definition for Trusted Computing Base (TCB)?
   a) Assurance that images created from trustworthy code are accurately delivered to the customers.
   b) An abstract machine that mediates all accesses to objects by subjects.
   c) A non-spoofable means to interact with the operating system.
   d) All protection mechanisms including hardware, firmware, and software responsible for enforcing the security policy.

4. In the modern DNS cache poisoning attack, which entity does the attacker directly try to manipulate?
   a) The DNS client
   b) The recursive DNS server
   c) The authoritative DNS server
   d) The root DNS server

The DNS clients are the ultimate targets for trickery, but they are tricked by directly sending fake messages to the recursive DNS server.

5. Alice creates a database table, friend_data with the columns: name, phone, and notes. Which of the following statements can she execute to give Bob read access to the name and phone columns but not give him the ability to give anyone else the ability to read the name and phone columns.
   a) `grant select (name, phone) on friend_data to Bob;`
   b) `grant select on friend_data to Bob;`
   c) `grant update (name, phone) on friend_data to Bob with grant option;`
   d) `grant select (name, phone) on friend_data to Bob with grant option;`

6. The following definition best defines which type of malicious code? "Hooks or augments file system calls with additional logic that causes specified files and directories to effectively disappear."
   a) Trojan program
   b) Rabbit
   c) Netbot
   d) Rootkit

7. What is a key feature of stacks and heaps that enables a well chosen buffer overflow to result in the execution of code of the attacker's choosing?
   a) User data and system control data combined in a single memory segment.
   b) Bad programming languages that enable the possibility of overwriting the end of allocated memory.
   c) Processor architectures that allow execution of machine code from data segments.
   d) Over reliance on a single operating system (mono-culture of windows).

8. In which environment would Firesheep **not** be effective in hijacking web sessions.
   a) Switched ethernet network
   b) Open wireless network
   c) Running on a device acting as a border router for the site
   d) Running with access to a span or monitor port on a switch.

Short Answer

9. 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 clearance levels are ordered as T > U > V and the categories are m, o, p

Subject	Subject Label	Object	Object Label
Alice	T:{m, o, p}	Xray	U:{m, o}
Bob	V:{p}	Yoyo	T:{p}
Carol	U:{m, p}	Zebra	U:{m, p}

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), where append is a "pure" write that assumes no ability to also read the data. (9 points)

	Xray	***Yoyo***	***Zebra***
Alice	*r*	*r*	*r*
Bob		*a*	*a*
Carol			*ra*

b) Write the Access Control Lists (ACLs) that would capture the protection state you identified in part a. (3 points)

acl(Xray) = (Alice, {r})
acl(Yoyo) = (Alice, {r}), (Bob, {a})
acl(Zebra) = (Alice, {r}), (Bob, {a}), (Carol, {ra})

c) 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 most common answer is that in a MAC model an unprivileged user cannot change how the security policy is enforced.

10. Below is a list of network security operations and a list of network security mechanisms. Match the most appropriate enforcing mechanism for each security operation. One mechanism should be selected for each operation. (6 points)

Operations	**Mechanisms**
C → 1. Perform egress filtering.	A. Virtual Private Network
D → 2. Log or drop traffic that matches the characteristics of a worm payload identified at a security conference last week.	B. Application Proxy Firewall
B → 3. HTTP 1.0 requests are old and feared to be harbingers of old attacks. Drop such requests or update them to follow the HTTP 1.1 standard	C. Packet Filter Firewall
	D. Network Intrusion Detection System

11. Consider the requirements identified in the Common Criteria and before that in the TCSEC (orange book). (12 points)

There are a large number of possibilities here. Below are two examples for each question part.

a) Identify and briefly describe two security functional requirements that appear in Common Criteria security targets and/or TCSEC classes.

Trusted Path – An unspoofable mechanism to talk with the TCB of the system, e.g. Ctl-Alt-Del in Windows.

Mandatory Access Control – Implement access control model such that unprivileged users cannot change the implementation of the access control rules.

b) Identify and briefly describe two security assurance requirements that appear in Common Criteria EALs and/or TCSEC classes.

Structural Testing - The system should be tested. The knowledge of how the system is designed should be used in designing the tests to ensure that relevant portions of the design are adequately tested.

Source Control/Code Management – The TCB code base should be stored in a repository when changes are reviewed before entry, and a history of the changes is kept.

12. This question addresses IP routing. As an attacker, assume you could inject a new route into the routing table of the router that sits between an organization and the rest of the Internet. (12 points)

a) How could you use this ability to implement a man-in-the-middle (MITM) attack?

The attacker could insert a route for the target destination that has a next-hop machine that the attacker controls. As traffic is sent to the target destination, it is routed to the attacker controlled machine. The attacker could send that traffic onto the next portion of the route that would take the packet to the target destination.

If the attacker needed the return traffic, he could insert another route in the path from the target destination to the original source. Some of you suggested changing the address to be that of the attacker's router. Technically that would work for most protocols, but I think that would make it more obvious to the target that the packet has been messed with. In the routing-only case, the packet is unchanged when it reaches the destination. But if you change the address, the packet is changed and it is pointing directly back to the attacker's machine.

Also inserting a route isn't as easy as finding a poorly configured router. The next hop device must be withing ARP-ing distance (in the same network) as one of the interfaces in the target router. So the attacker must still have control of a device "close" to one of the routers along the routing path from source to destination.

b) Does the MITM attack target confidentiality, integrity, or availability? Select one of these security elements and describe how MITM targets it.

MITM can attack all three.

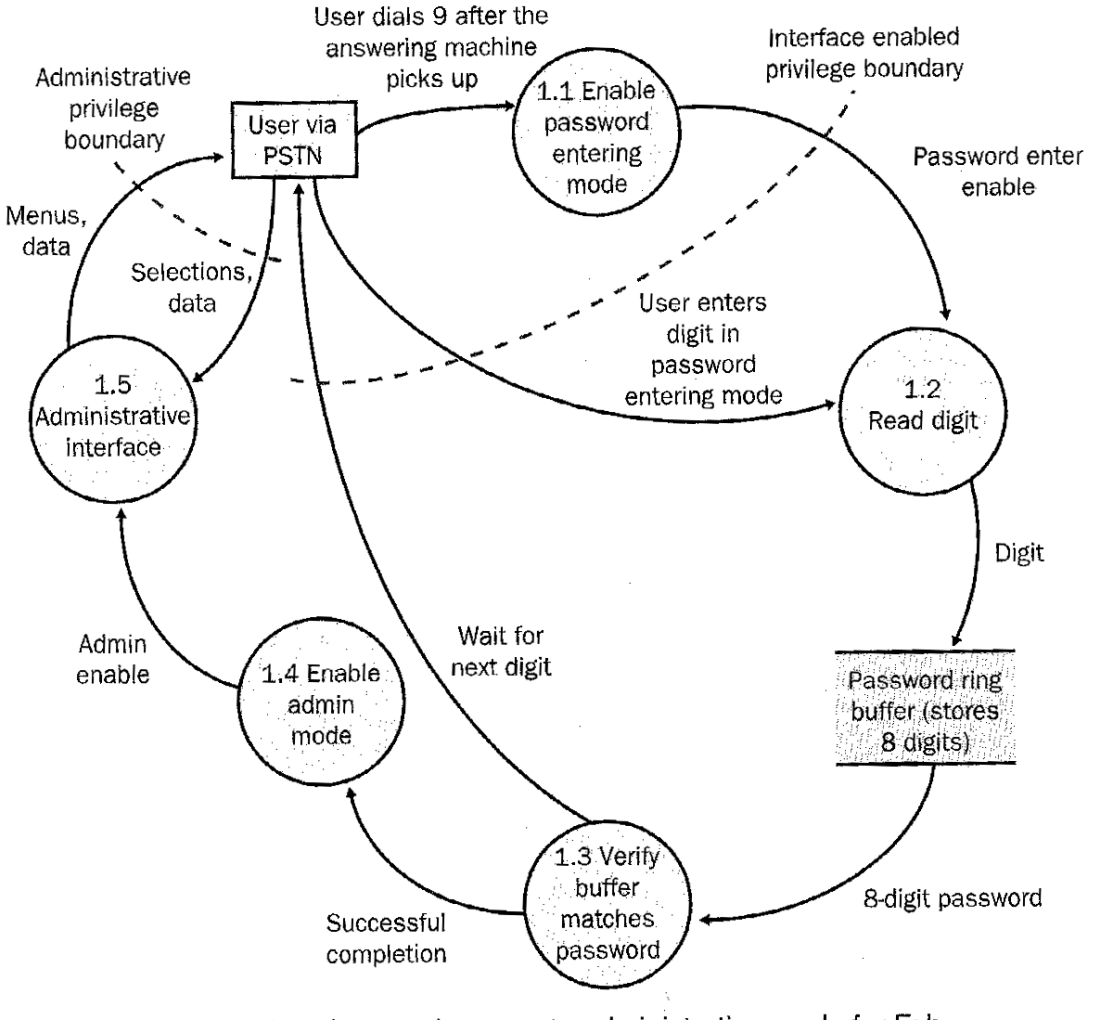
- *Confidentiality – Attacker can see traffic that was not intended for him.*
- *Availability - Attacker can chose to not forward traffic onto original destination.*
- *Integrity – Attack can change the packet that pass through his malicious router.*

c) As an end user, how could you protect yourself from the effects of MITM attacks?

Encrypting the traffic is the most common answer. Even if the encrypted traffic passes through the attacker's router, he won't see the information and he won't be able to change the data without being detected.
Trace route (double checking the paths used by packets) would also work.

A number of folks suggested fixes that only a system administrator not an end user could perform, like run network analysis tools, change the configuration of the routers, etc.

13. You have joined the Fabrikam Phone 1.0 project that is using the Threat Modeling techniques discussed in class to improve the security results of the project. This project is development phone menuing software that user's interact with primarily via the publicly switch telephone network (PSTN). The data flow diagram for the remote administrative interface design shown below. The questions follow on the next pages. (16 points)



Most people seemed to have done well on this question. It was fairly open-ended. As long as you showed good understanding of the threat modeling concepts in your example, you got full points.

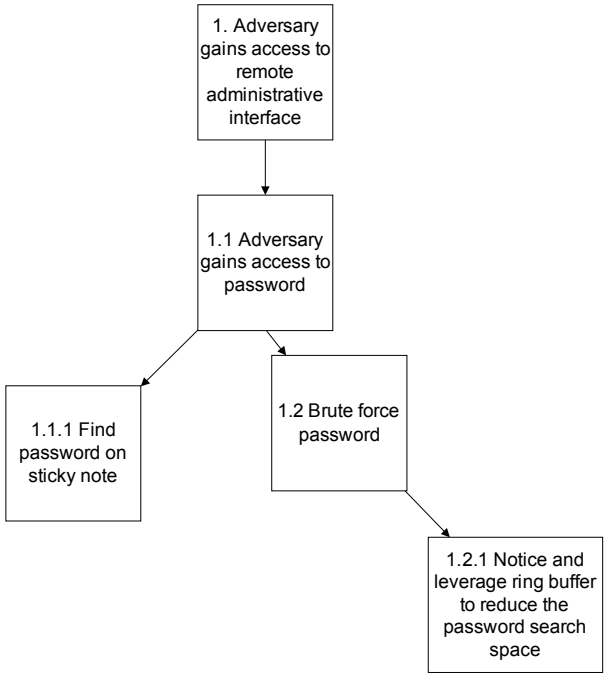
a) The team has identified a number of threats, but they have not classified them according to STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of privilege). Consider the following threat, identify which aspects of STRIDE apply to this threat, and describe why they apply.

Threat ID = 1
Name = An adversary gains access to the remote administration interface, resulting in access to the phone configuration.
Description = Phone 1.0 has remote administration interface that allows an authorized user to configure it via the Public Switched Telephone Network (PSTN). The interface is disabled by default but can be enabled using the local key pad
Entry Points = (6) remote administration, (3) telephone line, (2) keypad
Assets = (5) phone configuration

You could probably make good cases for most of the STRIDE elements

- *Information Disclosure – By accessing the remote administration interface, the adversary sees information about the phone system he is not authorized to see.*
- *Elevation of Privilege – By accessing the remote administration interface, the adversary is able to perform privileged operations to change how the phone system operates.*

b) Write an attack tree for this threat. The tree should have at least two branches and roughly 5 nodes.



(More parts on the next page)

c) Enumerate one of the attack paths through this tree.

One path in this case would be 1 → 1.2 → 1.2.1

d) Does the DFD show any mitigation for the attack paths you listed in part c? If so, identify how it is mitigated. If not, identify something that could be added to the design to at least partially mitigate the attack (and describe how it mitigates the attack). If you feel the attack is impossible to even partially mitigate, explain why.

In this case, the ring buffer can indeed be leveraged to reduce the password search. Once the ring buffer is filled, we only need to add one more digit to make a new password that will be checked. The decision to use a ring buffer to store the password should be reconsidered (node 1.2.1). We could in addition add some logic to stop the conversation after a certain number of failed password attempts (node 1.2).