Homework 6

CS161 Computer Security, Spring 2008

This homework will not be collected.

Use this to help prepare for the final exam.

1. **Hardware Support for Dual-Mode Operation**

   Early Intel processors (e.g., the 8086) did not provide hardware support for dual-mode operation (i.e., support for a separate user mode and kernel mode). As a result, most of the systems implemented on these processors did not support multi-user operation. List and explain one potential problem associated with supporting multi-user operation without hardware support for dual-mode operation. Be concise: one or two sentences should suffice.

2. **Gesundheit**

   Kachoo!, Inc. has just released a new web service that allows people to sign their web pages. The service does this by appending, hidden inside a special HTML tag at the bottom of an otherwise normal web page, the author's name, the date, and a signature (which contains the author's name and date signed by the author's RSA private key). The web page itself is unencrypted, but the signature can be validated by downloading http://www.kachoo.com/pubkeys.html (which contains a list of all registered Kachoo! users and each user's public key) to retrieve the author's public key. Explain why this gives a completely false sense of security, by outlining two different ways that you could make it appear that Linus Torvalds has posted a web page saying "Open source is for losers; I've decided to go work for SCO". The definition of "different" is that each attack has a unique fix. For each of the attacks you list, give a countermeasure that the author/viewer could take to protect themselves against that attack.

   (a) Attack 1:

(b) Countermeasure 1:

(c) Attack 2:

(d) Countermeasure 2:

3. **One is the Loneliest Number**

   In this class, we have seen several different mechanisms for isolating untrusted programs, including virtual memory, system call interposition, and virtual machines.

   (a) Name one threat that system call interposition protects against but virtual memory does not.

   (b) The military runs a multi-user computer that all government employees can log into; programs that require access to top-secret data are run inside a virtual machine. Richard Stallman is given an account on this computer so that he can install emacs. Colonel Greene runs a copy of Stallman's emacs program inside a virtual machine and uses it to edit the top-secret list of UFOs stored in Area 51's warehouses. (Only Greene has an account on the guest OS running inside the virtual machine.) If Richard Stallman were malicious, could he arrange to learn the contents of this list? If yes, explain how; if no, say why not.

4. **Secure PIN Entry** We want to allow a user to enter a secure PIN (numeric password) into a terminal. We assume that an adversary can monitor any input (such as a keyboard or keypad) but that the channel of the display to the user (such as a screen) is secure: the adversary cannot monitor it. Give a secure way for the user to enter his or her PIN (the adversary should gain no information about the PIN).

5. **Firewalls and Reference Monitors** Explain how the requirements of a reference monitor apply specifically to a firewall. Address the feasibility of determining whether a real firewall meets these requirements.

6. **Intrusion Detection Systems** Explain succinctly the difference between rule-based intrusion detection and statistical anomaly detection. Give one advantage each has over the other.

7. **Buffer Overflow** Why is having a non-executable stack and heap insufficient to protect against buffer overflow code execution attacks?

8. **Rootkits** Joe wants to protect himself against rootkits, so he runs a virtual Windows XP system on top of Mac OS X. Is Joe vulnerable to Windows XP rootkits? Why or why not?

9. **SQL Injection Attacks** SQL's prepared statements add the "?" syntax to the language:

   select * from foo where bar=?

   "?" can then be replaced with a string using a seperate function "setString()". This is more secure than building up queries by concatenating strings, because "setArgument()" understands enough of the SQL language to ensure that its arguments are properly interpreted at the database server. For example, if the "bar" column contains strings, then "setArgument" ensures that its parameter is a string, and the server interprets it as raw string data, instead of as part of a SQL expression.

   setArgument can be applied in various different points in the query syntax. Which of the following can safely interpret untrusted user input? For each case, explain what setArgument would have to verify, or explain why passing such data in from the user is unsafe:

   a) setArgument takes an integer: "select * from foo where num=?"

   b) setArgument takes a set of values: "select * from foo where num in ?"

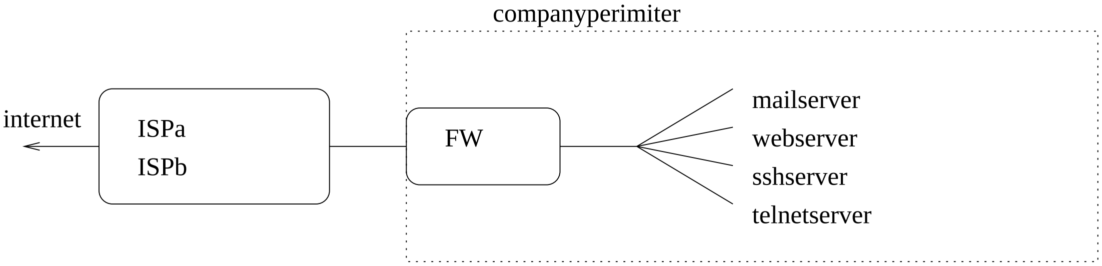
   c) setArgument takes a nested SQL query: "select * from foo where num in ?"

10. **Cross Site Scripting and SQL Injection**

    In class, we saw an example of a cross site scripting attack involving javascript. That example enabled the attacker to authenticate as the victim user, to the victim server. This is a two step attack, requiring the attacker to first obtain the user's cookies, and then authenticate to the server. Describe how the attacker could develop a more elaborate cross site scripting attack, involving SQL injection along with javascript injection, to eliminate the need for the step where the attacker authenticates as the user. Feel free to make any reasonable assumptions necessary about the victim server, in order to make your attack possible.

11. **Firewalls**

    The following diagram shows the architecture for your company's network and connection to the internet.



IP addresses:

ISP router	2.2.2.1
Mail server	1.2.3.5
Web server	1.2.3.4
SSH server	1.2.3.3
Telnet server	1.2.3.2

Example rules:

```
allow * *:*/in -> *:*/out
drop * *:* -> *:*
```

Your company is installing a packet filter firewall. Here is the proposed security policy for the firewall:

[I] By default, block all inbound connections.

[II] Allow all inbound TCP connections to SMTP on mail server.

[III] Allow all inbound TCP connections to HTTP and HTTPS on web server.

[IV] Allow all inbound TCP connections to SSH on SSH server.

[V] Allow all outbound connections.

[VI] Telnet access should not be allowed (because it sends passwords in cleartext).

(a) (12 points) Using the syntax from lecture (examples above), write the firewall ruleset for your company's firewall. For each rule, give a brief description of its purpose.

(b) (8 points) Hackers target your company's network with repeated requests for large images on your company's webserver. The hackers machines are on the `20.1.21.x` subnet. How could you change your firewall ruleset to block these attacks?

(c) (8 points) Employees start downloading lots of movie trailers from the new Pear SlowTime website at `4.3.2.1:80`. How could you change your firewall rules to stop employees from accessing the website?