CS 155: Spring 2004
June 2004

CS 155 Final Exam

This exam is open books and open notes, but you may not use a laptop. You have 2 hours. Make sure you print your name legibly and sign the honor code below. All of the intended answers may be written well within the space provided. You may use the back of the preceding page for scratch work. If you want to use the back side of a page to write part of your answer, be sure to mark your answer clearly.

The following is a statement of the Stanford University Honor Code:

A. The Honor Code is an undertaking of the students, individually and collectively:

(1) that they will not give or receive aid in examinations; that they will not give or receive unpermitted aid in class work, in the preparation of reports, or in any other work that is to be used by the instructor as the basis of grading;

(2) that they will do their share and take an active part in seeing to it that others as well as themselves uphold the spirit and letter of the Honor Code.

B. The faculty on its part manifests its confidence in the honor of its students by refraining from proctoring examinations and from taking unusual and unreasonable precautions to prevent the forms of dishonesty mentioned above. The faculty will also avoid, as far as practicable, academic procedures that create temptations to violate the Honor Code.

C. While the faculty alone has the right and obligation to set academic requirements, the students and faculty will work together to establish optimal conditions for honorable academic work.

I acknowledge and accept the Honor Code.

____
(Signature)

____
(Print your name, legibly!*)*

Prob	# 1	# 2	# 3	# 4	# 5	# 6	# 7	# 8	# 9	Total
Score										
Max	16	12	5	9	12	12	8	14	12	100

1. (*16 points*) . . . . General attacks

Describe the following general kinds of attacks, in a few sentences each.

(a) (*4 points*) Buffer overflow attack

(b) (*4 points*) Shell script race condition attack

(c) (*4 points*) DNS cache poisoning attack

(d) (*4 points*) SYN flooding attack

2. (*12 points*) .... Short Answer

(a) (*4 points*) In comparison with access control lists, what are the advantages and disadvantages of capabilities? List one advantage and one disadvantage.

(b) (*4 points*) Banks use an Electronic Clearing House (ECH) network to process checks. Suppose that Bank A may send a file to Bank B, with each record in the file representing one check deposited in Bank A that is to be withdrawn from Bank B. Assume that each record contains only two account numbers and the amount of money to be transferred. The ECH file format specifies an integrity checksum for each record, but not for the entire file. How can this be exploited by an insider at Bank A who does not have the ability to write valid checksums, but can modify a file?

(c) (*4 points*) The source code for an electronic voting machine contains the following definition.

```
#define DESKEY ((des_key*)"F2654hD4")
```

Explain why this indicates a security problem.

3. (*5 points*) .... SQL Injection

Suppose a web site issues the following SQL query to its database:

```
sql = "SELECT lname, fname, phone FROM usertable
       WHERE lname='" & Request.QueryString("lname") & "';"
```

What will happen as a result of the following http request to this site?

```
http://www.myserver.com/search.asp?lname=smith\%27\%3bupdate
\%20usertable\%20set\%20passwd\%3d\%27hAx0r\%27\%3b--\%00
```

The character equivalents are: %20 is space, %27 is `'`, %3b is ; and %3d is =
Explain why this is probably not what the author of the server script had in mind.

4. (*9 points*) .... NX bit

Intel is currently adding the NX bit feature to the Pentium architecture. Briefly, the NX bit (no-execute bit) is a flag bit added to every memory page indicating whether the contents of the page can be executed. When the NX bit of a memory page is set, control flow cannot jump anywhere in the page.

(a) (*5 points*) Explain why the NX bit is considered a security feature. What type of attack is the bit intended to defend against? Briefly, how would you change the OS to take advantage of this new flag?

(b) (*4 points*) Will the NX bit prevent the type of attack you described in part (a)? If so, explain why. If not, give an example attack that would work even though the NX bit is fully integrated into the processor and Operating System.

.

5. (*12 points*) .... Mutual Suspicion and SetUID

The mutual suspicion problem arises when two users must share information but neither user trusts the other. For example, when a caller requests a service, the caller would like the called process (the “callee”) to only have access to caller resources that are passed explicitly.

Under Unix, a plausible approach to the mutual suspicion problem involves setting up a restricted user ID and running the callee executable program under this restricted ID. Then (hopefully) the callee will only have access to the objects passed to it, not arbitrary files owned by the caller. The setuid bit is intended to facilitate this approach.

(a) (*6 points*) Recall that every UNIX process has a Real User ID (RUID) and an Effective User ID (EUID). (there is also a Saved User ID (SUID) which we ignore here). What is the difference between the RUID and EUID? How is each one used by the OS? Explain what happens to the RUID and EUID when the caller’s process activates an executable file (e.g. by calling `exec`) whose setuid bit is set to the callee’s user ID.

(b) (*6 points*) In some versions of UNIX the `setuid` call enables any process to set its current EUID to its RUID. Does this make the setuid mechanism more useful or less useful for solving the mutual suspicion problem? Why? Recall that the caller and callee do not trust one another and either one could be malicious.

6. (*12 points*) .... Mobile IP

Using *Mobile IP,* a mobile device may maintain an IP connection with another device while moving from one location on the network to another. This is done differently in different versions of IP. To keep things simple, we will refer to the two options as (1) triangle routing, and (2) route optimization. Some terms associated with Mobile IP are:

MH - the "mobile host," the machine that changes location,
HA - the "home agent," a server on the mobile host's home network,
CH - the "corresponding host" that wants to communicate with MH.

In triangle routing, the CH always sends packets to the HA, which forwards to the MH. However, response packets from the MH can be sent directly to the CH. For example, if you take your wireless device from Stanford to Berkeley, your MH can get a local "care-of address" from Berkeley and send this to your HA at Stanford. Then when someone (a CH) sends packets to your Stanford IP address, your HA at Stanford will forward them to your address at Berkeley.

(a) (*4 points*) The protocol used to send the care-of address to the HA is called *registration.* Why is authentication important in registration? Is secrecy necessary?

(b) (*4 points*) Ingress filtering is a common firewall policy that blocks packets whose source address does not match the portion of the network the packets are coming from. Why is ingress filtering an issue for Mobile IP? (*Hint:* what is the source address on a packet from the MH to the CH?)

(c) (*4 points*) In route optimization, the MH executes a *binding update* protocol with the CH. This gives the CH the care-of address of the MH, allowing the two to communicate directly without using the HA. However, route optimization only works if the CH implements Mobile IP, whereas triangle routing is transparent to the CH. In the binding update protocol, the MH and CH generate new numbers called "nonces" to avoid replay attack. Each host places a randomly chosen nonce in the first message it sends, and expects to receive the same nonce back in the next message it receives. Explain why nonces prevent replay and explain why replay would be a problem for route optimization.

7. (*8 points*) .... Virus throttle

In class we discussed a virus throttle technique for slowing down worm and virus propagation. Suppose the throttle is implemented as a kernel patch on the user's machine. Describe two methods by which a worm can defeat this throttling mechanism and propagate rapidly.

(a) (*3 points*) Describe one method assuming the worm is able to become root on an infected machine.

(b) (*5 points*) Describe another method assuming the worm does not become root on an infected machine.

8. (*14 points*) .... DNS Covert Channel

The Java security manager enforces the following policy on network access: an untrusted applet can only connect to the site from which it was downloaded. Older versions of the security manager enforce this policy as follows. When the applet is first downloaded the security managers notes the IP address of the host from which it was downloaded. When the applet tries to open a connection to some host, say `www.xyz.com`, the security manager queries DNS to get the IP address of that host and compares the result to the IP address from which the applet was downloaded. If the two are different the connection request is refused.

(a) (*4 points*) Explain the rationale behind this security policy. What were the designers of the security manager trying to defend against?

(b) (*6 points*) Show that an applet downloaded from `www.xyz.com` can bypass the security manager and send messages to some site, say `www.badguy.com`, via a covert channel based on DNS. Explain exactly how this would work. You may assume that site `www.badguy.com` is cooperating with the applet.
Hint: think of an applet that is constantly trying to open new network connections.

(c) (*4 points*) How would you fix the security manager so that it correctly enforces its network access policy, but prevents the covert channel from part (b)?

9. (*12 points*) .... Firewalls

(a) (*3 points*) Explain the difference between a stateless and a stateful firewall.

(b) (*3 points*) Can a firewall be used to block all incoming email containing the phrase "low mortgage rates"? Explain how or why not.

(c) (*3 points*) Can a firewall be used to block all incoming email from Nigeria? Explain how or why not.

(d) (*3 points*) Can a firewall installed at a web site protect the web site from a DDoS SYN flood attack? Assume web servers at the site do not use SYN cookies. Explain how or why not.