CS 155: Spring 2005
June 2005

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	Total
Score									
Max	16	16	12	12	12	12	10	10	100

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

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

(a) (*4 points*) Control hijacking attack (say, due to a format string vulnerability).

(b) (*4 points*) Web cache poisoning attack.

(c) (*4 points*) SQL Injection attack

(d) (*4 points*) Power analysis attack

2. (*16 points*) .... Short Answer

(a) (*4 points*) How does traffic shaping improve the security of a local area network?

(b) (*4 points*) What is an “anonymizing proxy”? Who is it intended to protect? From what kind of threats? What related threats does it *not* protect against?

(c) (*4 points*) What is a polymorphic virus? What is a metamorphic virus? Which one is harder to block?

(d) (*4 points*) Can memory leaks lead to security vulnerabilities?

3. (*12 points*) .... Sandboxing

(a) (*3 points*) What is the purpose of sandboxing?

(b) (*3 points*) Describe two limitations of the `jail` sandbox?

(c) (*3 points*) Explain how a system call interposition sandbox works.

(d) (*3 points*) What are some of the benefits and disadvantages of a system call interposition sandbox?

4. (*12 points*) . . . .

Intel Hyper-Threading Technology enables multiple threads of software applications to be run simultaneously on a single processor. In effect, hyper-threading makes a single processor behave like multiple processors. This is achieved by duplicating the architectural state on each processor, while sharing a single set of processor execution resources. For example, all threads running simultaneously, share the same L1 and L2 caches.

Now, suppose a low security process wants to eavesdrop on a high security process to obtain the memory access pattern of the high security process. By memory access pattern we mean the list of times at which the high security process read from memory (i.e. from the L1 cache). We are not interested in which memory locations were actually read. The resulting list should look something like $0, T_1, T_2, \ldots$ where 0 is the time for the first monitored memory access, T_1 is the elapsed time until the next memory access, etc.

(a) (*6 points*) Explain how the shared L1 cache enables this type of eavesdropping. Hint: think of a low security process that causes all memory reads from the high security process to generate an L1 cache miss. How can this be done and how can it be used? You may assume an LRU cache replacement policy.

(b) (*6 points*) Can you suggest some way by which the high security process can ensure that no useful information is leaked as a result of such eavesdropping?

Note: It was recently shown that this type of eavesdropping on an RSA decryption function enables the low security process to completely expose the RSA private key of the high security process.

5. (*12 points*) .... PhatBot

WASTE is a tool that was originally designed to permit secure distributed collaboration and communications for small groups of people who trust each other. WASTE clients provide an execution platform and secure networking that can be used to build other services. Some base services provided by WASTE are: a variant of instant messaging, group chat, distributed presence (a user at one site can see what other WASTE users are doing at other sites), file browsing, distributed file search across connected machines, and file transfer from one machine running WASTE to another. WASTE routes all data through a distributed peer-to-peer network, using encryption to provide secrecy. Given all of these features, it is not too surprising that WASTE and similar software have been used to build bots.

(a) (*4 points*) Assume that you are able to get WASTE installed on a set of compromised machines. What features of WASTE, identified in the list of functions services built on top of WASTE, would be useful for collecting passwords that are typed in by unsuspecting users? Briefly explain the architecture and operation of a network of WASTE-based bots that monitors keystrokes and transport "interesting" key sequences to a central collection point.

(b) (*2 points*) Why are bots used for distributing spam?

(c) (*3 points*) WASTE does not provide a way to install itself on other machines, since this kind of malicious behavior was not a goal of the well-meaning WASTE designers. Suppose you want to use WASTE to build a self-propagating bot network. Referring to mechanisms that we covered in class, explain what steps your bots might follow to identify vulnerable targets, compromise target machines, and so on.

(d) (*3 points*) If you want to use SNORT to detect intrusions of a WASTE-based bot as described in the previous part of this question, what sort of actions will be identified in the SNORT signature?

6. (*12 points*) .... VoIP Security

Voice-over-IP (VoIP) allows telephone calls to be carried over regular IP networks. Currently, most corporate VoIP installations use VoIP within an office building or set of buildings to connect telephones, but do not use the Internet to carry calls outside the company. Stanford uses VoIP in this way.

(a) (*4 points*) In organizations like Stanford, a person making a long distance call has to pay for the call in some way. Explain what requirements this places on the VoIP protocol. Choose from among these terms, or others like them, in writing your answer: *secrecy, authentication, integrity, denial-of-service, non-repudiation.*

(b) (*2 points*) Suppose that VoIP phones are used inside the Computer Science Building, but all calls leaving the building are carried on an ordinary phone line. What simple firewall configuration does this suggest? Can this be done using a stateless packet filter, or is stateful filtering needed?

(c) (*2 points*) VoIP uses signaling protocols and media transport protocols. Signaling protocols are used to locate a user, set up a session, and close a session. Media transport protocols digitize voice input, allocate digital data to packets, and reassemble digitized voice signals. Which form of protocol is more susceptible to denial-of-service from an external attacker, even if VoIP is being used behind a firewall? Explain.

(d) (*2 points*) What kind of cryptography (encryption, signatures, hashing, etc.) would you try to use to protect VoIP calls from eavesdropping? Would you add cryptography to the signaling protocol or the media transport protocol to achieve this goal?

(e) (*2 points*) What if you are not just concerned about protecting the content of a conversation, but also the list of calls made by each caller in the Computer Science Building? What kind of steps might you use, and which class of VoIP protocol is involved?

7. (*10 points*) .... Race conditions

Suppose a setuid root program takes a filename as input and performs some operation on the file that only root can perform. The program first checks that the calling process is allowed to access the file. The following standard code is used for this:

```
if (access(filename, R_OK))
  return ERROR;

fp = fopen(filename, "r");
```

Note that calling `access` returns 0 only if the *real uid* (i.e. the calling process' uid) is allowed to read the file.

(a) (*4 points*) Explain why this sequence of instructions is vulnerable to a race condition attack.

(b) (*2 points*) Describe a simple solution (that could involve kernel changes) to fix the problem.

(c) (*4 points*) Consider the following code instead:

```
fp = fopen(filename, "r");

for (i=0; i<10; ++i) {
  if (access(filename, R_OK))
    return ERROR;

  tfp = fopen(filename, "r");
  if (tfp points to a different file than fp)
    return ERROR;
}
```

Does this method prevent the race condition from part (1)? Justify your answer.

8. (*10 points*) .... Digital Rights Management (DRM)

In Windows Media Player, content may be distributed in an encrypted form. When a user wishes to play a song or view a video, the player needs to acquire a license for encrypted content. In addition to encryption keys, licenses may also contain stipulations on use of the content. Some stipulations that make sense for songs, for example, are the number of times a song may be played or the number of days the song may be played. There are several ways that musicians or music companies might wish to use this kind of content protection system. For example, a musician might want to distribute licenses that allow a user to play a song four times over a two-week period for free. This allows anyone to hear the song a couple times. Then, unlimited-use licenses could be sold to anyone who wants to play the song after that.

A program called `freeme` appeared on the web in 2001. This program allowed users to decrypt encrypted content intended for Microsoft Windows Media Digital Rights Management version 7.

(a) (*2 points*) What distribution advantages are there in separating content from licenses? (*Hint:* Which is larger, an encrypted song or a license?)

(b) *(2 points)* The `freeme` program used encrypted content and a license to produce decrypted content. Why is a program like this considered a threat to Windows Media security?

(c) *(2 points)* Suppose you had Windows Media Player, an encrypted song, and a license that allows you to play the song until January 1, 2005. How might you try to play the song now, in June 2005, without using a program like `freeme`? Recall that Windows Media Player may consult an online time server.

(d) *(2 points)* In the Windows Media Player system, what is the trusted computing base? Explain.

(e) *(2 points)* Is the Windows Media Player access control method more like capability-based access control, or access control lists? Explain.