Final Exam

This exam is closed book and closed notes. However, you may consult a single two-sided reference sheet. You may not use any electronic devices or communicate with anyone other than course staff.

Print your answers legibly. The intended answers fit within the spaces provided on the question sheets. You may use the back of the preceding page for scratch work. If you run out of room for an answer, continue on the back of the page and clearly mark your answer.

This is a timed exam. You have **90 minutes**.

Write and sign the honor code pledge:

> "*I have neither given nor received unauthorized aid on this examination, nor have I concealed any violations of the Honor Code.*"

_____

_____

_____

_____
(Signature)

_____
(Print your name)

_____
(Uniqname)

Question:	1	2	3	4	5	Bonus	Total
Points:	10	10	10	10	10	0	50
Score:							

1. Short Answer

(a) [2 points] In a secure channel, why should the sender encrypt the plaintext first and then apply integrity protection (rather than the reverse order)?

(b) [2 points] What is Kerckhoffs's principle? What is the justification for it?

(c) [2 points] What anonymity protections does Tor attempt to provide? Be precise.

(d) [2 points] How are client puzzles used to defend against denial-of-service attacks?

(e) [2 points] What is the same-origin policy? What is its role in browser security?

2. Attacks and Defenses

Briefly describe each of the following attacks and give an example of the damage it can cause. Then describe a defense that can potentially mitigate it.

(a) [2 points] Shell injection

(b) [2 points] DNS cache poisoning

(c) [2 points] Length extension

(d) [2 points] Phishing

(e) [2 points] Null-prefix attacks against HTTPS

3. Applied Crypto

As a security engineer at Mozilla, you have been assigned to redesign the automatic update system for Firefox. You want to ensure that Firefox will only install authentic updates from Mozilla, and that the protocol will be resilient to active network attackers.

In your first design, Mozilla posts the latest update at a particular URL on mozilla.com, which Firefox checks periodically in the background. If the URL's content changes, Firefox automatically downloads and installs it.

(a) [2 points] Assuming that Mozilla's server is completely secure, how could a network-based attacker cause a client to install a Trojan update if the update URL is loaded over HTTP? Briefly outline two distinct attacks.

(b) [3 points] Suppose instead that the URL is loaded over HTTPS, and that mozilla.com uses a certificate issued by a browser-trusted certificate authority (CA). When Firefox makes the HTTPS connection, what checks should it perform to validate the server's public key?

(c) [4 points] Due to high server costs, management would prefer to distribute updates via an untrusted content distribution network (CDN) like BitTorrent that does not provide any integrity guarantees. Propose a correct and efficient design based on RSA digital signatures that protects against Trojan updates in this scenario. Be detailed and precise.

(d) [1 point] Compare the amount of time Mozilla's servers spend doing crypto for the approach in part (b) and the approach in part (c). Which is better?

4. Control Hijacking

You are developing a proof-of-concept exploit for a traditional stack-based buffer overflow. After trapping on a breakpoint inside the vulnerable function, `gdb` yields the following:

```
==> x/28wx $esp
0xbffee770:      0xbffee786  0xbffff4b3  0xbffee798  0x08048ef2
0xbffee780:      0x080c6008  0x00000000  0x00000000  0x00000000
0xbffee790:      0x00000000  0x00000000  0x00000000  0x00000000
0xbffee7a0:      0x00000000  0x00000000  0xbffee7b8  0x08048f5e
0xbffee7b0:      0xbffff4b3  0x00000000  0x00000000  0x00000000
0xbffee7c0:      0x00000000  0x00000000  0xbffff278  0x0804901f
0xbffee7d0:      0x00000002  0xbffff314  0xbffff320  0x00000000

==> x/2wx $ebp
0xbffee7a8:      0xbffee7b8  0x08048f5e
```

Make these assumptions:

- An unbounded buffer begins at `0xbffee784`. You can cause arbitrary data to be copied into the buffer by a call to `memcpy`, and the vulnerable function then immediately returns.
- The machine is a 32-bit little endian system that behaves like the VM from Project 4.
- There are no defenses such as ASLR, stack canaries, or non-executable stack (DEP).

(a) [7 points] You want to run a payload that is 24 bytes long and works like the shellcode provided in Project 4. Write the bytes (in hex) that should be copied to the buffer for the most concise possible exploit. For positions that will contain the payload, write shellcode.

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____ ____

(b) [1 point] Suppose instead that the machine does use a non-executable stack (DEP). What will go wrong when you attempt the attack from part (a)? Be precise.

(c) [2 points] Describe a technique you could use to exploit this vulnerability in spite of DEP.

5. Privacy and Surveillance

Consider a hypothetical classified order of the Foreign Intelligence Surveillance Court, ordering Verizon to supply to the National Security Agency, each day for a three-month period,

> an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [...] Telephony metadata includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call.

(a) [3 points] The NSA might point out that the order does not require Verizon to supply "the name, address, or financial information of [any] subscriber or customer." Is this sufficient to protect innocent Verizon customers from being personally identified? Explain.

(b) [7 points] The NSA might point out that the order does not require Verizon to supply the content of any phone calls. Does the order still raise privacy concerns, beyond those emphasized in part (a)? Explain. Be concrete.

6. [5 points (bonus)] **Extra Credit**

When Prof. Halderman was 12 years old, he chose a password for AOL Instant Messenger. It was very insecure: a common 4-letter noun starting with the letter **g**. It wasn't "geek" or "girl" or "game." Many people correctly guess it on the first try based only on the facts provided here.

What was the password? _____