Department of Electrical Engineering and Computer Science

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.566 Spring 2026

Quiz I

You have 80 minutes to answer the questions in this quiz. The questions are worth 80 points in total.

For multiple-choice and true-false questions, we subtract points for incorrect answers, so as to make random guessing not change your expected score.

Some questions are harder than others. You may want to first skim through all of them, and attack them in the order that allows you to make the most progress. If you find a question ambiguous, be sure to write down any assumptions you make. Be neat and legible. If we can't understand your answer, we can't give you credit!

Write your name and Gradescope email address on this cover sheet.

This is an open book, open notes, open laptop exam.
Internet access limited to public static content.
No communication, no web searches, no LLM use.

This quiz is printed double-sided.

Name:

Gradescope email address:

You can answer the feedback questions on the back of the quiz before the official start time.

I OS/VM isolation [12 points]

Suppose that Ben Bitdiddle discovers a bug in how the Linux file system deals with file deletion and creation: if a file is created with some file name, deleted, and then another file is created with the same file name, the file turns out to contain 4KB of data from a random unallocated disk block, rather than being empty. For example:

```
int fd = open("newfile", O_CREAT | any other flags, 0666);
close(fd);
unlink("newfile");

fd = open("newfile", O_CREAT | any other flags, 0666);
char buf[4096];
int n = read(fd, buf, 4096);
// Surprise: n=4096 and buf contains data from some
// unallocated disk block.
```

1. [6 points]: What isolation/security guarantees could Ben potentially bypass using this bug on a standard Linux system (e.g., the Athena dialup machines)? Be specific about what could go wrong.

2. [6 points]: For each of the following isolation schemes discussed in lecture, can Ben bypass the isolation guarantees of that scheme using his bug?

(Circle True or False for each choice.)

A. True / False Ben can bypass LXC isolation.

B. True / False Ben can bypass gVisor isolation.

C. True / False Ben can bypass Firecracker isolation.

II BitLocker [7 points]

Ben Bitdiddle considers the following potential attack against his friend's laptop that uses BitLocker: he will steal his friend's laptop and replace the CPU with a modified chip. The modified CPU works just like the original CPU with one difference: when it detects the instruction sequence used by Windows to check the user's password, it executes and produces results as if the password is correct, regardless of whether the password is actually correct. Ben plans to power up the stolen laptop, boot Windows normally, enter "123" as the password, and log in to access the data in the user's account stored on the laptop.

3. **[7 points]:** Will Ben's attack work? Explain why or why not.

III OpenSSH [7 points]

Consider the paper "Preventing Privilege Escalation" about privilege-separating OpenSSH, and the corresponding lecture.

Ben Bitdiddle wants to modify OpenSSH to allow users to log in without a password when connecting from a specific IP address. (This is probably a bad idea in general, but let's assume that Ben uses a network where it's not possible to spoof connections from another IP address.) Ben's plan is to modify the monitor to add a new type of request, `MONITOR_REQ_AUTHIP`, which works much like `MONITOR_REQ_AUTHPASSWORD`, except that instead of sending the user's password, the worker/slave sends the client's IP address. Ben also modifies the pre-auth worker/slave process to send this request to the monitor.

4. [7 points]: Why is this a bad design given OpenSSH's privilege separation architecture? Propose a better way to achieve Ben's goal.

IV Buffer overflow defenses [14 points]

5. [6 points]: Consider the paper "Baggy Bounds Checking" by Akritidis et al, with the `slot_size` value set to 16 (as in the paper). For the following code, which line will trigger a panic?
(Circle the one best choice.)

```
0 char *p = malloc(40);
1 char *q = p + 46;
2 char *r = q + 24;
3 char *s = r - 20;
4 char  t = *s;
5 char *u = s - 56;
```

A. Line 1.

B. Line 2.

C. Line 3.

D. Line 4.

E. Line 5.

F. No panic.

6. [8 points]: Which of the following attacks are still possible with a fat-pointer scheme as described in lecture?

(Circle True or False for each choice.)

A. True / False Overflowing a buffer on the stack to corrupt the return address.

B. True / False Overflowing a buffer within an allocated array of structs to corrupt other parts of the struct.

C. True / False Overwriting a buffer after it has been freed.

D. True / False Overflowing a heap-allocated buffer to corrupt other heap-allocated memory.

V Web security [18 points]

Ben Bitdiddle includes the following code on his web page at `https://bitdiddle.com`:

```
var req = new XMLHttpRequest();
req.addEventListener("load", function() { console.log("loaded"); });
req.addEventListener("error", function() { console.log("error"); });
req.open("GET", "https://www.bankofamerica.com/account/balance");
req.send();
```

7. [8 points]: Alice installs a fresh web browser on her computer, and visits Ben's site. Which of the following will happen?

(Circle True or False for each choice.)

A. True / False Alice's web browser will send an HTTP request to `bankofamerica.com`.

B. True / False Alice's web browser Javascript console will print `loaded`.

Ben Bitdiddle sets up a blog web site at `https://bitdiddle.com/` where visitors can post and view comments, and Ben uses cookies to keep track of logged-in users (such as himself, which allows him to post new articles). Alyssa figures out that Ben's blog has a cross-site scripting vulnerability, and posts a comment containing a Javascript snippet, as in `Hi Ben, great blog! <SCRIPT>...</SCRIPT>`. Ben visits his blog, from his web browser, by typing in `https://bitdiddle.com/` in his browser's URL bar, after Alyssa posts her comment.

8. [10 points]: Which of the following security mechanisms will prevent Alyssa's attack from being able to post a new article on Ben's behalf?

(Circle True or False for each choice.)

A. True / False Marking the cookie on Ben's site as `HttpOnly`.

B. True / False Marking the cookie on Ben's site as `Secure`.

C. True / False Marking the cookie on Ben's site as `SameSite`.

D. True / False Requiring a CSRF token when posting a new article.

E. True / False Setting content security policy that disables inline scripts.

VI Symbolic execution [4 points]

9. [4 points]: Ben Bitdiddle changes the STP constraint solver used by EXE such that, if STP was about to time out, it returns a random result (either "satisfiable" or "unsatisfiable") instead of returning a timeout. What effect might this have on bugs that EXE finds, if Ben lets EXE run to completion, and EXE does not require any concretization?

(Circle True or False for each choice.)

A. True / False Ben's modified EXE could find a bug that the original EXE system does not find.

B. True / False Ben's original EXE could find a bug that the modified EXE system does not find.

VII Lab 1 [8 points]

Ben Bitdiddle wants to write shellcode that will invoke the `SYS_migrate_pages` system call on Linux, which happens to be syscall number 256 (`0x100` in hexadecimal). He writes the following code in `shellcode.S`:

```
        mov     $SYS_migrate_pages,%ax /* set up the syscall number */
```

but when he compiles it, he discovers that the resulting instruction contains a zero byte in it:

```
$ objdump -d shellcode.o
...
  11:        66 b8 00 01                 mov    $0x100,%ax
...
```

This is a problem because the buffer overflow he was planning to use with this shellcode uses a string-copy function that stops copying data after seeing a zero byte.

10. [8 points]: How can Ben fix his shellcode to get `SYS_migrate_pages` (256) into the `%ax` register without having a zero in his compiled instructions?

VIII Lab 2 [8 points]

Suppose that Ben Bitdiddle discovers a vulnerability in the final privilege-separated lab 2 implementation, which allows an adversary to see internal network traffic between all of zoobar's containers except for `main`, and does not allow the adversary to modify the network traffic or directly send their own packets to specific containers.

11. [8 points]: Can the adversary leverage this vulnerability to log in as another user into the Zoobar web application? Explain how, or explain why not.

IX 6.566 [2 points]

We'd like to hear your opinions about 6.566. Any answer, except no answer, will receive full credit.

12. [2 points]: Out of the papers that we have covered so far, listed below, mark the one that you think we should remove next year (or mark none if you think all papers should stay).

- ☐ OS/VM isolation: Firecracker, gVisor, comparison study.
- ☐ WebAssembly: wasm design paper, rWasm/vWasm paper.
- ☐ BitLocker.
- ☐ OpenSSH privilege separation.
- ☐ Google security architecture, BeyondProd whitepaper.
- ☐ iOS security.
- ☐ Web security readings.
- ☐ Baggy bounds checking.
- ☐ EXE symbolic execution.
- ☐ Do not remove any papers.

End of Quiz

Double-sided quiz: check the back of this page!