Department of Electrical Engineering and Computer Science

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

6.566 Spring 2024

Quiz II

You have 180 minutes to answer the questions in this quiz. In order to receive credit you must answer each question as precisely as possible.

Some questions are harder than others, and some questions earn more points than others. You may want to skim them all through first, 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 submission website email address on this cover sheet.

This is an open book, open notes, open laptop exam.
NO COMMUNICATION OR COLLABORATION DURING THE QUIZ.

This quiz is printed double-sided.

Please do not write in the boxes below.

I (xx/32)	II (xx/32)	III (xx/42)	IV (xx/10)	V (xx/32)	VI (xx/20)	VII (xx/12)	Total (xx/180)

Name:

Submission website email address:

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

This page intentionally left blank.

I Guest lectures

According to Danny Weitzner, which of the following are major risks of key escrow?
(Circle True or False for each choice; we subtract points for incorrect answers.)

1. [8 points]:

A. True / False Key escrow undermines forward secrecy.

B. True / False Key escrow means it will be possible to guess private keys through brute force.

C. True / False Key escrow introduces complexity that leads to bugs.

D. True / False Key escrow has high overheads, reducing performance.

According to Danny Weitzner, which of the following is the main challenge in appropriately estimating the risk of losses due to computer security breaches:
(Circle the best choice; we subtract points for incorrect answers.)

2. [8 points]:

A. Computer attacks are unpredictable.

B. Administrators can configure the same software in different ways, leading to different vulnerabilities.

C. There is not enough data about losses due to computer security breaches.

D. There are too many different problems that lead to significant losses.

This page intentionally left blank.

According to Russ Cox, which of the following would be examples of a supply chain attack against Google (not necessarily "open-source supply chain attack"):

(Circle True or False for each choice; we subtract points for incorrect answers.)

3. [8 points]:

A. True / False An adversary bribes a software developer at Google to use a known-buggy old version of an open-source library.

B. True / False An adversary gets a job at Google working on their compiler infrastructure, and introduces a backdoor into Google's version of the Clang C compiler.

C. True / False An adversary bribes the maintainer of a popular open-source library to include an exploitable vulnerability, and this library is then downloaded and used by Google in its products.

D. True / False An adversary breaks into the web server hosting the Clang C compiler and replaces the latest version of the released source code with one that has a backdoor, which Google later downloads and uses in its systems.

4. [8 points]: According to Max Burkhardt, defenders are often thought to be at a disadvantage because attackers only need to find one way to break in, whereas defenders need to prevent all possible ways to break in. Why, then, did Max say that attackers are suddenly at a disadvantage after their initial break-in to gain access into some system?

This page intentionally left blank.

II TLS

Ben Bitdiddle is in charge of running a web server that supports TLS 1.3. He wants to log the plaintext HTTP requests sent to that web server, for debugging purposes. He has access to the TLS server certificate and the correspoding private key from the web server, but he does not want to make any changes to the web server machine or to the clients that are issuing these HTTP requests.

5. [10 points]: Ben sets up a second machine, with the TLS certificate and private key, and sends a copy of all network traffic to this second machine. Explain why Ben will not be able to log plaintext HTTP requests.

6. [10 points]: Explain what Ben needs to do in order to log plaintext HTTP requests without making any changes to the web server or the clients. Ben can change DNS records, though.

This page intentionally left blank.

Alyssa P. Hacker is building a mobile game that protects its network connections with TLS 1.3, and Alyssa is worried about latency in her game. While profiling the performance of her game, Alyssa notices that connections from her mobile device to her server use the P-256 EC Diffie-Hellman key agreement scheme, but that the X25519 EC Diffie-Hellman key agreement scheme is about twice as fast, both on the mobile device and on the server: P-256 takes about 60 microseconds, while X25519 takes 30 microseconds.

Alyssa changes her server to use X25519 instead of P-256. While the game still works, Alyssa is surprised to see that latency from her mobile device has increased substantially, by many milliseconds.

7. [12 points]: Explain why Alyssa observes higher latency with X25519 compared to P-256, and suggest what she should do to avoid this latency increase.

This page intentionally left blank.

III Network performance

Suppose you want to transfer a file by sending it over a TLS 1.3 connection; that is, you run:

```
cat file | openssl s_client -connect othermachine:443
```

where othermachine is the hostname of the machine you are sending the file to, listening on port 443. For the following scenarios, estimate how long it will take, from the time you run the above command, until the destination machine gets the contents of your file. Assume your local DNS resolver already has the name `othermachine` cached, that the server is already running and ready to accept connections, and that the client knows the server's DH scheme for TLS 1.3 1-RTT mode. You can ignore TCP slow-start and window effects. Your TLS 1.3 client and server are using X25519 for DH key exchange (which has a throughput of 33,000 key exchange computations per second), RSA-2048 for signatures (which has a throughput of 2000 signs per second and 60000 verifications per second), and AES-128-GCM for authenticated encryption (which has a throughput of 1 GByte/second).

(Circle the best choice; we subtract points for incorrect answers.)

Flip over to the back side of this page for the three scenarios you should analyze.

8. [14 points]: The other machine is your friend in Australia. The round-trip latency to Australia is 300 milliseconds (150 milliseconds one-way), and the available bandwidth is 100 Mbit/sec. You are sending a 16-byte file.

A. 300 milliseconds

B. 450 milliseconds

C. 750 milliseconds

D. 1200 milliseconds

9. [14 points]: The other machine is directly connected by a 10-Gigabit ethernet link. The round-trip latency is 10 microseconds (5 microseconds one-way), and the available bandwidth is 10 Gbit/sec. You are sending a 1 KByte file.

A. 20 microseconds

B. 30 microseconds

C. 60 microseconds

D. 600 microseconds

10. [14 points]: The other machine is in another datacenter in the same city. The round-trip latency is 2 milliseconds (1 milliseconds one-way), and the available bandwidth is 1 Gbit/sec. You are sending 1 GByte.

A. 6 milliseconds

B. 100 milliseconds

C. 1 second

D. 8 seconds

IV Certificates

Ben Bitdiddle wants to get a TLS certificate for his web server, but his web server doesn't support directories that start with a dot, like the `/.well-known/` directory required by the ACME HTTP challenge. Ben wants to propose to Let's Encrypt that the ACME client should be able to specify the full pathname for the challenge URL when requesting a certificate from Let's Encrypt, instead of having Let's Encrypt hard-code the `/.well-known/acme-challenge/` directory as part of the standard.

11. [10 points]: Explain what security problem would arise if Ben's proposal were adopted.

This page intentionally left blank.

V Signal

12. [12 points]: Alyssa P. Hacker somehow manages to get the private keys for Ben's ephemeral prekeys (denoted $eprek^B$ in the "Analysis of the Signal Messaging Protocol" paper) from the Signal app on Ben's phone (and no other secret state). Suppose that Ben's friend Carol already knows Ben's identity key ipk^B and starts a fresh conversaton with Ben. If Alyssa has control over Carol's network and Carol's connection to the Signal server, explain how Alyssa can decrypt Carol's message to Ben, or explain why she cannot do so.

In a separate scenario, unrelated to the above question, Carol keeps sending messages to Ben, Ben reads those messages, but does not reply. Alyssa P. Hacker monitors all encrypted messages sent between Carol and Ben. Alyssa breaks into Ben's phone and gets the current chaining key ck for Ben's conversation with Carol.

13. [10 points]: Explain how Alyssa can decrypt Carol's messages to Ben from before Alyssa obtained the chaining key, or explain why she cannot do so.

14. [10 points]: Explain how Alyssa can decrypt Carol's messages to Ben sent after Alyssa obtained the chaining key, or explain why she cannot do so.

This page intentionally left blank.

VI Differential privacy

Suppose that you are tasked with adding a feature to Gradescope that reveals various statistics about exam scores in a class (where each score is between 0 and 1). For each of the following, explain whether or not it would achieve differential privacy in all cases, and why.

15. [10 points]: Publishing the list of student scores with Laplace($1/\varepsilon$) noise added to each score.

16. [10 points]: Publishing the sum of exam scores of students that received a score of 0.5 or higher, with Laplace($1/\varepsilon$) noise added to the sum.

NOTE: The feedback question is on the back side of this page.

VII 6.566

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

17. [4 points]: Out of the papers and guest lectures that we covered in the second part of the semester, listed below, circle the one that you think we should definitely remove next year (or circle the last choice if you think all papers and guest lectures should stay).

- Supply chain security: guest lecture by Russ Cox.
- Network security: TCP/IP.
- Secure channels: TLS 1.3.
- Certificates: Let's Encrypt.
- User authentication: U2F.
- Messaging security: Signal.
- Key transparency: CONIKS.
- Anonymity: Tor.
- Cybersecurity policy: guest lecture by Danny Weitzner.
- Security economics: Spamalytics paper.
- Differential privacy: PINQ.
- Information security in real life: guest lecture by Max Burkhardt.
- Do not remove any papers.

18. [4 points]: Were the lab recitations helpful? Should we keep them next year?

19. [4 points]: What else would you suggest we improve next year?

End of Quiz