Peyrin & Ryan
Summer 2020

CS 161 Computer Security

HW7

To prepare you for the final format, Homework 7 is formatted exactly like the final. Please fill in your answers on the Homework 7 assignment on Gradescope.

The biggest difference from the midterm format is that the answer sheet is on Gradescope instead of on paper.

For questions with **circular bubbles**, you may select exactly *one* choice on the answer sheet.

○ Unselected option

● Only one selected option

For questions with **square checkboxes**, you may select *one* or more choices on the answer sheet.

■ You can select

■ multiple squares

For questions with a **large box**, you need to write a short answer in the corresponding text box on the answer sheet.

You have 1 week (170 minutes for the actual exam). There are 4 questions of varying credit (60 points total).

[NOTE: The Gradescope HW7 assignment is untimed, but the real final will be a timed assignment. See the "Sample Timed Answer Sheet" on Gradescope for an example.]

The Gradescope answer sheet assignment has a time limit of 170 minutes. Do not click "Start Assignment" until you're ready to start the exam. The password to decrypt the PDF is at the top of the answer sheet.

[NOTE: Most questions on this homework are from past exams, so we will grade the homework on completeness. These questions are similar to what you should expect on the final exam, so we recommend trying the questions as a practice exam before checking the solutions.]

The exam is open note. You can use an unlimited number of handwritten cheat sheets, but you must work alone.

Clarifications will be posted at https://cs161.org/clarifications.

Q1 *MANDATORY – Honor Code* (2 points)

Read the honor code on the Gradescope answer sheet and type your name. *Failure to do so will result in a grade of 0 for this exam.*

Q2 *True/False* (16 points)

[NOTE: The first question on the exam will always be True/False.]

Each true/false is worth 2 points unless otherwise specified.

[NOTE: On Gradescope, every question will be labeled as being worth 1 point–you should ignore this. The real point values are on the exam PDF.]

Q2.1 TRUE or FALSE: If a victim is logged into a session on `https://bank.com/` in one tab and visits an attacker's website in another, the attacker can run JavaScript to load a form at `https://bank.com/transfer` and extract the CSRF token from it.

○ TRUE ○ FALSE

Q2.2 TRUE or FALSE: An on-path attacker can learn the request parameters of a GET request loaded over HTTPS.

○ TRUE ○ FALSE

Q2.3 TRUE or FALSE: TLS has end-to-end security, so it is secure against an attacker who steals the private key of the server.

○ TRUE ○ FALSE

Q2.4 TRUE or FALSE: If the entire Internet stopped using HTTP POST requests and only allowed HTTP GET requests, CSRF attacks would still be possible.

○ TRUE ○ FALSE

Q2.5 TRUE or FALSE: It is secure for a server to generate session tokens based only on timestamp to the nearest second, as long as every user receives a unique token.

○ TRUE ○ FALSE

Q2.6 TRUE or FALSE: If every website uses TLS and every cookie has the secure flag set, clickjacking attacks are still possible.

○ TRUE ○ FALSE

Q2.7 Assume you've set up a 3-relay Tor circuit to access some websites over HTTPS. A malicious adversary takes control of the entry relay, but the other two are honest and uncompromised. The adversary can now learn which website you are visiting.

○ TRUE ○ FALSE

Q2.8 TRUE or FALSE: In Bitcoin, once your transaction is successfully added to a block that lives on the longest chain, you can be guaranteed that it will never be lost.

○ TRUE ○ FALSE

This is the end of Q2. Proceed to Q3 on your answer sheet.

Q3 *Infrastructure Week* **(18 points)**

For each public-key infrastructure (PKI) scheme, mark whether it provides the same trust guarantees as the standard PKI from lecture for all certificates, some certificates, or no certificates at all. Assume that everyone has the root certificate hardcoded into their machines.

Q3.1 (3 points) Each server can only sign the public keys of its grandchildren (two descendants below the current level). For example, the root server can sign the public key of `berkeley.edu` but not `.edu`, and the `.edu` server can sign the public key of `eecs.berkeley.edu` but not `berkeley.edu`.

[NOTE: Your answer sheet has six answer choices for every subpart, but not every question will have six answer choices. For example, for Q2.1 here, you should not use options (D), (E), and (F) on your answer sheet.]

○ (A) All certificates ○ (C) No certificates ○ (E) ——

○ (B) Some certificates ○ (D) —— ○ (F) ——

Q3.2 (3 points) As in the previous part, each server can only sign the public keys of its grandchildren. However, the root is additionally allowed to sign the public key of its direct children. For example, the root server can sign the public key of `.edu` and `berkeley.edu`. The `.edu` server can sign the public key of `eecs.berkeley.edu` but not `berkeley.edu`.

[NOTE: The answer choices on this subpart are circular bubbles, so you should only bubble in one option out of (G), (H), (I), on your answer sheet for Q2.2.]

○ (G) All certificates ○ (I) No certificates ○ (K) ——

○ (H) Some certificates ○ (J) —— ○ (L) ——

Q3.3 (3 points) Same setup as the previous part, but an attacker has compromised a server one level below the root (e.g. `.edu`).

○ (A) All certificates ○ (C) No certificates ○ (E) ——

○ (B) Some certificates ○ (D) —— ○ (F) ——

Q3.4 (3 points) The root handles all requests and sends the requested public key and a certificate directly through a TLS connection.

○ (G) All certificates ○ (I) No certificates ○ (K) ——

○ (H) Some certificates ○ (J) —— ○ (L) ——

Q3.5 (3 points) Instead of signing, use a cryptographic hash to create a certificate. For example, the root server signs the public key of `.edu` by hashing it.

- ◯ (A) All certificates
- ◯ (C) No certificates
- ◯ (E) ——
- ◯ (B) Some certificates
- ◯ (D) ——
- ◯ (F) ——

Q3.6 (3 points) Instead of signing, use HMAC to create a certificate. For example, the root server signs the public key of `berkeley.edu` by applying `HMAC`(K, `berkeley.edu`), where K is the root's private signing key.

- ◯ (G) All certificates
- ◯ (I) No certificates
- ◯ (K) ——
- ◯ (H) Some certificates
- ◯ (J) ——
- ◯ (L) ——

[NOTE: You may not need all blanks on the answer sheet for a question. You should leave Q2.5 and Q2.6 blank on your answer sheet. Also, since none of the subparts of this question asked for a short answer, you should leave the space below Q2 on your answer sheet blank.]

This is the end of Q3. Proceed to Q4 on your answer sheet.

Q4 *Network Security* (24 points)

Answer the following questions about network security.

Q4.1 (3 points) Bob connects his laptop to the DeCafe coffee shop's Wifi, which anyone nearby can join without a password. He browses to the website `http://www.foocorp.com`. At the table next to him is an evil attacker, Mallory, who has also joined the DeCafe Wifi network. What kind of threat model best describes Mallory when she first joins the network, with respect to Bob's connection with DeCafe router's?

○ (A) Off-path attacker

○ (C) In-path attacker

○ (E) ——

○ (B) On-path attacker

○ (D) None of the above

○ (F) ——

Q4.2 (4 points) Bob returns home and types into his browser `www.foocorp.com`. Suppose that Mallory has managed to poison the DNS cache on Bob's laptop, such that it now thinks the IP address of `www.foocorp.com` is 6.6.6.6, which is the IP address of a server that Mallory controls.

Which of the following statements are true? Select all that apply.

[NOTE: The answer choices on this subpart are square bubbles, so you should bubble in any of options (G), (H), (I), (J) you think are correct, or only option (K) if you think all options are incorrect. You should leave option (L) on your answer sheet blank.]

☐ (G) Mallory will be unable to steal Bob's cookies for `http://www.foocorp.com` if `http://www.foocorp.com` uses HTTP-Only cookies.

☐ (H) Mallory will be unable to steal Bob's cookies for `http://www.foocorp.com` if `http://www.foocorp.com` uses a CSP policy that only allows scripts to be loaded from sources on `foocorp.com`

☐ (I) Mallory will be unable to steal `foocorp.com` cookies marked with the `secure` flag.

☐ (J) Mallory will be unable to inject JavaScript into `http://www.foocorp.com`

☐ (K) None of the above

☐ (L) ——

Q4.3 (5 points) Suppose that `foocorp.com` domain has the following four subdomains: (`www`, `alphabet`, `sushi`, `money`).
The attacker knows that `foocorp.com` has only four subdomains but does not know any of their names, and wishes to discover the subdomains using the zone enumeration attack discussed in class.

Assuming every DNS server uses plain NSEC, what is the minimum number of queries the attacker needs to make to `foocorp.com`'s nameservers in the worst-case for the attacker?

[NOTE: If a question asks for a short answer (empty box below the question on the exam), you should type your answer in the corresponding text box on Gradescope.]

○ (A) —— ○ (B) —— ○ (C) —— ○ (D) —— ○ (E) —— ○ (F) ——

Q4.4 (4 points) Suppose that a user Alice is browsing the Internet at home and Mallory is an on-path attacker.

In which of the following scenarios will Mallory be able to identify whether or not Alice is visiting a website on `foocorp.com`? Select all that apply.

☐ (G) Alice's machine and local DNS resolver randomize the source port of DNS queries; `foocorp.com`'s NS server use DNS (without DNSSEC); `foocorp.com` does not use HTTPS

☐ (H) Alice's machine and local DNS resolver use a fixed source port for every DNS query; `foocorp.com`'s NS server uses DNSSEC with plain NSEC; `foocorp.com` does not use HTTPS

☐ (I) Alice's machine and local DNS resolver use a fixed source port for every DNS query; `foocorp.com`'s NS server uses DNSSEC with NSEC3; `foocorp.com` does not use HTTPS

☐ (J) Alice's machine and local DNS resolver use a fixed source port for every DNS query; `foocorp.com`'s NS server uses DNSSEC with NSEC3; `foocorp.com` uses HTTPS

☐ (K) None of the above

☐ (L) ——

Q4.5 (5 points) `FooCorp` has chosen to use very short TTLs in all of their DNS responses. Which of the following statements are true? Select all that apply.

☐ (A) Short TTLs help protect against attacks where `FooCorp`'s DNS servers have been compromised

☐ (B) Assuming all DNS servers used DNSSEC with plain NSEC, then `FooCorp`'s decision to use short TTLs will increase the amount of work that the DNS servers of `FooCorp`'s parent zone need to perform

☐ (C) Short TTLs increase the number of requests `FooCorp`'s DNS servers need to support

☐ (D) Short TTLs help protect against DNS cache poisoning attacks by an on-path attacker

☐ (E) Short TTLs help protect against blind-spoofing attacks

☐ (F) None of the above

Q4.6 (5 points) `FooCorp` hosts *all* of its servers on machines provided by CheapCloud: a large, but unreliable, cloud hosting provider. CheapCloud suffers from two major problems: (i) they have frequent data breaches; and (ii) they often need to assign new IP addresses to their customers' servers. Nevertheless, CheapCloud promptly notifies their customers whenever either of these events occurs.

Which of the following designs or techniques can `FooCorp` use to help mitigate some of the security issues caused specifically by CheapCloud's poor environment? Select all that apply.

☐ (G) `FooCorp` uses plain DNS and sets short TTLs for all of its DNS responses

☐ (H) `FooCorp` uses RSA-based TLS

☐ (I) `FooCorp` uses DNSSEC with plain NSEC

☐ (J) `FooCorp` uses DHE-based TLS

☐ (K) `FooCorp` uses DNSSEC with NSEC3

☐ (L) None of the above

This is the end of Q4. You have reached the end of the exam.