Popa & Wagner
Spring 2020

CS 161
Computer Security

Midterm 2

This exam was generated for `foo@bar.com`.

For questions with **circular bubbles**, you may select exactly *one* choice on Gradescope.

○ Unselected option

● Only one selected option

For questions with **square checkboxes**, you may select *zero* or more choices on Gradescope.

■ You can select

■ multiple squares

For questions with a **large box**, you need to provide justification in the text box on Gradescope.

You have 80 minutes. There are 10 questions of varying credit (200 points total).

The exam is open book. You can use any resources on the Internet, including course notes, as long as you are working alone.

We will not be answering any clarifications about the exam. If there are any glaring problems with wording, we will consider dropping the question from the exam after solutions/grades are released.

Q1 *MANDATORY – Honor Code* (3 points)

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

This is the end of Q1. Proceed to Q2 on your Gradescope answer sheet.

Q2 *True/False* (48 points)

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

Q2.1 TRUE or FALSE: If Bob uses the authenticate-then-encrypt paradigm, the integrity of his plaintext is guaranteed.

○ TRUE ○ FALSE

Q2.2 TRUE or FALSE: A hash function must be collision-resistant to be considered safe for password hashing.

○ TRUE ○ FALSE

Q2.3 TRUE or FALSE: Alice wants to use authenticated encryption to send a message to Bob. She should use Enc(M), MAC(H(Enc(M))) over Enc(M), MAC(H(M)).

○ TRUE ○ FALSE

Q2.4 Suppose we increase the entropy of the DNS ID field to 128 bits. It is infeasible for an on-path adversary to spoof a DNS answer.

○ TRUE ○ FALSE

Q2.5 TRUE or FALSE: By default, in a TLS connection, both the server and client are authenticated to each other.

○ TRUE ○ FALSE

Q2.6 TRUE or FALSE: If weak passwords are salted and hashed before being stored, then the attacker cannot easily learn the plaintext values of the weak passwords.

○ TRUE ○ FALSE

Q2.7 TRUE or FALSE: A DNS lookup for `en.wikipedia.org` will always force the recursive resolver to send at least 3 DNS queries.

○ TRUE ○ FALSE

Q2.8 TRUE or FALSE: If the server's random number a in Diffie-Hellman TLS is the same in every handshake, Diffie-Hellman TLS no longer has forward secrecy. Assume the value a is stored on the server along with its secret key.

○ TRUE ○ FALSE

Q2.9 TRUE or FALSE: If Bob is an on-path attacker who can guarantee that his spoofed response arrives before the legitimate response, Bob only needs the victim to make one request for a nonexistent domain in order to successfully execute a Kaminsky attack with 100% probability.

○ TRUE ○ FALSE

Q2.10 TRUE or FALSE: Randomizing the client port helps defend TCP against on-path attackers.

○ TRUE ○ FALSE

Q2.11 TRUE or FALSE: TLS provides end-to-end security, so it is secure even if the server has a buffer overflow vulnerability.

○ TRUE ○ FALSE

Q2.12 TRUE or FALSE: Suppose we modified TCP so that the sequence number increases by 2 for every byte sent, but the initial sequence numbers are still randomly chosen. This modified protocol has the same security guarantees as standard TCP.

○ TRUE ○ FALSE

Q2.13 TRUE or FALSE: If IP spoofing is eliminated from the Internet (all attackers must send messages from their real IP), then an on-path attacker is no longer more powerful than an off-path attacker.

○ TRUE ○ FALSE

Q2.14 TRUE or FALSE: Consider a modified version of DHCP, where in the server offer step, the server signs its message and sends its public key along with the signed message. This version of DHCP is secure against the DHCP spoofing attack.

○ TRUE ○ FALSE

Q2.15 TRUE or FALSE: TCP is secure against a DoS attack by a man-in-the-middle (MITM) because TCP guarantees delivery and will re-send messages until they are delivered.

○ TRUE ○ FALSE

Q2.16 TRUE or FALSE: RSA-TLS is still secure if we use publically known lottery numbers as the value of the premaster secret (PS).

○ TRUE ○ FALSE

Q2.17 TRUE or FALSE: Under the SOP, it is possible for two webpages with different origins to communicate through narrowly defined APIs.

○ TRUE ○ FALSE

Q2.18 TRUE or FALSE: Under the SOP, the webpage at `https://example.com/randompic.html` cannot fetch the image at `https://cute-cats.com/cutest.jpg` because they have different origins.

○ TRUE ○ FALSE

Q2.19 TRUE or FALSE: Suppose the webpage at `https://example.com/index.html` contains a child frame that loads `https://another-example.com/index.html`. Under the SOP, the parent frame can read and modify the properties of the child frame.

○ TRUE ○ FALSE

Q2.20 (2 points) TRUE or FALSE: Suppose the webpage at `https://example.com/index.html` contains a child frame that loads `https://example.com/views.html`. Under the SOP, the child frame can read and modify the properties of the parent frame.

○ TRUE ○ FALSE

Q2.21 TRUE or FALSE: Suppose the webpage at `https://example.com/index.html` loads and runs an external script from `https://sample.com/script.js`. Under the SOP, the script runs with the same origin as `https://sample.com/script.js`.

○ TRUE ○ FALSE

Q2.22 TRUE or FALSE: Mallory convinces Alice to connect to her private Wi-Fi network. Webpages that Alice visits while on this network may no longer be subject to the SOP.

○ TRUE ○ FALSE

Q2.23 TRUE or FALSE: Mallory convinces Alice to try out her custom browser, FireFaux. Webpages Alice visits using this browser may no longer be subject to the SOP.

○ TRUE ○ FALSE

Q2.24 TRUE or FALSE: Consider a modified version of Diffie-Hellman TLS where the server does not include the signature when sending $g^a \bmod p$. This version of TLS does not provide confidentiality against a MITM.

○ TRUE ○ FALSE

Q2.25 (0 points) TRUE or FALSE: EvanBot is a bot.

○ TRUE ○ FALSE

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

Q3 (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`.

○ (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`.

○ (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) ——

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

Q4 **(29 points)**

Alice is using a DNS resolver to perform a DNS lookup for `www.google.com`. A single, valid nameserver is authoritative for each of the following zones:

Zone	*Nameserver*
`.`	`a.root-servers.net`
`.com`	`a.gtld-servers.net`
`google.com`	`ns1.google.com`

Assume no other legitimate clients will query the resolver (but the adversary can query it if they wish), the resolver's cache is initially empty, and the resolver uses iterative querying.

Assume that in DNSSEC, no one will accept a record unless it has a valid signature.

The attacker is on-path between the resolver and `ns1.google.com`, but off-path to the other name servers. The attacker also knows when Alice makes a request. **Assume DNS uses a static source port known to the attacker**.

For each part, select all of the records that the attacker can poison.

Q4.1 (4 points) Standard DNS is used.

□ (A) Alice's cached A record for `www.google.com`

□ (B) Resolver's cached NS record for `.com`

□ (C) Resolver's cached NS record for `google.com`

□ (D) Resolver's cached NS record for `.`

□ (E) ——

□ (F) ——

Q4.2 (3 points) Standard DNS is used. Also, the resolver has a hardcoded NS record that maps the `google.com` zone to `ns1.google.com`, and a hardcoded A record with the IP address of `ns1.google.com`.

□ (G) Alice's cached A record for `www.google.com`

□ (H) Resolver's cached NS record for `.com`

□ (I) Resolver's cached NS record for `google.com`

□ (J) ——

□ (K) ——

□ (L) ——

Q4.3 (3 points) The resolver and nameservers use DNSSEC, and Alice uses standard DNS.

□ (A) Alice's cached A record for `www.google.com`

□ (B) Resolver's cached NS record for `.com`

□ (C) Resolver's cached NS record for `google.com`

□ (D) ——

□ (E) ——

□ (F) ——

Q4.4 (3 points) The resolver and nameservers use DNSSEC, and Alice uses standard DNS. The adversary compromises `a.gtld-servers.net`.

□ (G) Alice's cached A record for `www.google.com`

□ (H) Resolver's cached NS record for `.com`

□ (I) Resolver's cached NS record for `google.com`

□ (J) ——

□ (K) ——

□ (L) ——

Q4.5 (3 points) The resolver and nameservers use DNSSEC, and Alice uses standard DNS. The adversary compromises `ns1.google.com`.

□ (A) Alice's cached A record for `www.google.com`

□ (B) Resolver's cached NS record for `.com`

□ (C) Resolver's cached NS record for `google.com`

□ (D) ——

□ (E) ——

□ (F) ——

Q4.6 (3 points) All parties use standard DNS, but the resolver and Alice encrypt their DNS messages with TLS.

□ (G) Alice's cached A record for `www.google.com`

□ (H) Resolver's cached NS record for `.com`

□ (I) Resolver's cached NS record for `google.com`

□ (J) ——

□ (K) ——

□ (L) ——

Q4.7 (3 points) All parties use standard DNS, but Alice, the resolver, and `ns1.google.com` encrypt their DNS messages with TLS.

□ (A) Alice's cached A record for `www.google.com`

□ (B) Resolver's cached NS record for `.com`

□ (C) Resolver's cached NS record for `google.com`

□ (D) ——

□ (E) ——

□ (F) ——

Q4.8 (3 points) All parties use standard DNS, but everyone encrypts their DNS messages with TLS.

□ (G) Alice's cached A record for `www.google.com`

□ (H) Resolver's cached NS record for `.com`

□ (I) Resolver's cached NS record for `google.com`

□ (J) ——

□ (K) ——

□ (L) ——

Q4.9 (4 points) Alice and the resolver use standard DNS, but encrypt their DNS messages with TLS. The resolver and nameservers use DNSSEC.

□ (A) Alice's cached A record for `www.google.com`

□ (B) Alice's cached NS record for `google.com`

□ (C) Resolver's cached NS record for `.com`

□ (D) Resolver's cached NS record for `google.com`

□ (E) ——

□ (F) ——

This is the end of Q4. Proceed to Q5 on your Gradescope answer sheet.

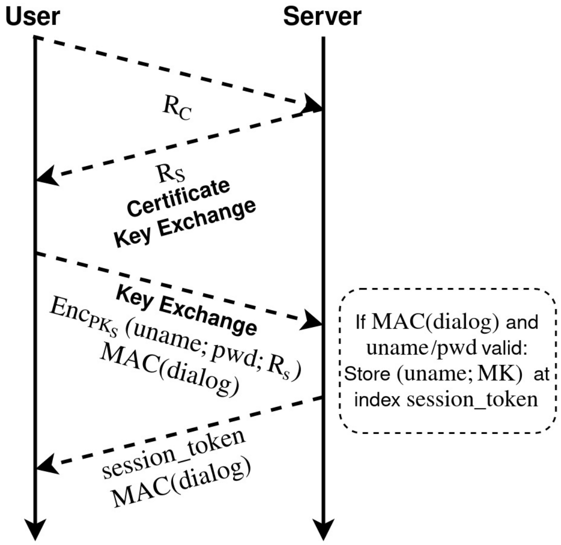
Q5 **(37 points)**

FastCash is a fast banking service which requires users to log in before making a transfer, and uses TLS with ephemeral Diffie Hellman and RSA certificates to secure all their connections. They implemented a TLS extension called *0-Round Trip (0-RTT)* to speed up the connection process. 0-RTT changes the initial handshake as follows:

- Users authenticate themselves during the second round of the handshake
- If the user authenticates correctly, the server stores a session_token for that user

(Recall that in TLS, PS, $\mathsf{R_S}$, *and* $\mathsf{R_C}$ *generate a master key set* MK *which contains all the symmetric keys.* $\mathsf{Enc}_{\mathsf{PK_S}}$ *denotes RSA encryption using the server's public RSA key.)*

A user only needs to perform the modified TLS handshake once. To send an HTTP request after the initial connection ends, a user encrypts it using the keys derived in the initial handshake and attaches the session_token. The server verifies that the entry session_token : (uname, MK) exists and, if so, decrypts and executes the request as the user uname using the keys derived from MK.


User
Server
R_C
R_S
Certificate
Key Exchange
Key Exchange
Enc_{PK_S} (uname; pwd; R_s)
MAC(dialog)
If MAC(dialog) and uname/pwd valid: Store (uname; MK) at index session_token
session_token
MAC(dialog)

Simplified diagram of modified initial TLS handshake

Assume that any on-path TCP injection attacks are impossible, and that once a user makes the initial modified TLS handshake, they will use the 0-RTT extension for future requests to the server.

Q5.1 (6 points) An on-path attacker observes an initial TLS handshake between a user and server, as well as a subsequent 0-RTT packet which contains an encrypted HTTP request. What can they do?

□ (A) Read the user's future communications

□ (B) Break forward secrecy for that user's communications

□ (C) Pretend to be the server to the user

□ (D) Pretend to be the user to the server in a new handshake

□ (E) Replay the encrypted HTTP request to the server

□ (F) Learn the master key set

Q5.2 (6 points) Suppose we removed R_S from the user's KeyExchange in the third step of the handshake. After observing an initial handshake between a user and the server, what can an on-path adversary do?

□ (G) Read the user's future communications

□ (H) Break forward secrecy for that user's communications

□ (I) Pretend to be the server to the user

□ (J) Pretend to be the user to the server in a new handshake

□ (K) Learn the premaster secret

□ (L) Learn the master key set

Q5.3 (6 points) Due to a bug, an on-path adversary is able to choose the server's R_S. After observing an initial handshake between a user and the server, what can they do?

□ (A) Read the user's future communications

□ (B) Break forward secrecy for that user's communications

□ (C) Pretend to be the server to the user

□ (D) Pretend to be the user to the server in a new handshake

□ (E) Learn the premaster secret

□ (F) Learn the master key set

Q5.4 (6 points) An on-path adversary observes a user and the server communicating using 0-RTT for some time (without observing the initial handshake). At some point in the future, the adversary manages to learn all of the server's session_token : (uname, MK) entries. What can they do?

□ (G) Read the user's future communications

□ (H) Break forward secrecy for that user's communications

□ (I) Pretend to be the server to the user

□ (J) Pretend to be the user to the server in a new handshake

□ (K) Learn the premaster secret

□ (L) Learn the master key set

Q5.5 (10 points) Consider a MITM adversary during the initial handshake between a user and the server. Describe how this adversary can send a malicious HTTP request that appears to come from the legitimate user (Be specific with what is sent). Disregard any bugs from previous parts.

Q5.6 (3 points) Because of the vulnerability from the previous part, the company decides that it's too dangerous to allow all web pages to be accessible via 0-RTT. suppose they support the following three HTTP requests:

1. `GET` request for bank's homepage
2. `GET` request for bank's transfer page
3. `POST` request to execute a transfer

Below are different possible combinations of pages which will be made accessible via 0-RTT. Select the combination with no vulnerability or None if they are all vulnerable.

○ (G) 2, 3 ○ (I) 1, 3 ○ (K) ——

○ (H) 1,2 ○ (J) None ○ (L) ——

This is the end of Q5. Proceed to Q6 on your Gradescope answer sheet.

Q6 (8 points)

Q6.1 (2 points) TRUE or FALSE: A NIDS always provides the most insight about ongoing network traffic.

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

Q6.2 (3 points) An edgy hacker, xXOskiTheHackerXx, downloads a ransomware tool on GitHub and, without modifying it, tries to target the CDC. Which is the best detection strategy to detect this type of hacker?

○ (G) Signature based ○ (J) Specification based

○ (H) Behavior based ○ (K) ——

○ (I) Anomaly based ○ (L) ——

Q6.3 (3 points) Andrew needs to decide between two burglar alarm systems - system A and system B. System A has a false positive rate of 0.05% and a false negative rate of 1%. System B has a false positive rate of 1% and a false negative rate of 0.05%.
The cost of a false positive is $100, because his parents fine him for causing a ruckus, and the cost of a false negative is $10000, because the burglar steals all his stuff. Which system should Andrew pick?

○ (A) System A ○ (D) ——

○ (B) System B ○ (E) ——

○ (C) Not enough information ○ (F) ——

This is the end of Q6. Proceed to Q7 on your Gradescope answer sheet.

Q7 **(15 points)**

Q7.1 (3 points) Alice clears all her network settings and broadcasts a DHCP discover message. What information should she expect to receive in the DHCP offer in response?

□ (A) DNS server

□ (B) Source port

□ (C) Lease time

□ (D) Premaster secret

□ (E) Gateway router

□ (F) IP address

Q7.2 (6 points) After receiving the DHCP offer, Alice tries connecting to `www.cutecats.com`, but instead of pictures of cats, the site she gets is filled with dog photos.
How did the attacker compromise DHCP to accomplish this?

Which of the following could the attacker have replaced?

□ (G) DNS server

□ (H) Source port

□ (I) Lease time

□ (J) Premaster secret

□ (K) Gateway router

□ (L) IP address

Q7.3 (3 points) Alice clears all her network settings and starts a new connection to `www.cutecats.com` with TCP. Now an off-path attacker wants to send a packet to the server to interfere with Alice's connection. What information do they need to know?

□ (A) Server sequence number

□ (B) Source port

□ (C) Client sequence number

□ (D) Destination IP address

□ (E) Destination port

□ (F) Source IP address

Q7.4 (3 points) At some point, Alice's connection with `www.cutecats.com` is suddenly terminated. Assuming some information was leaked and the attacker correctly guessed the fields from the previous part, how was the attacker able to execute this attack?

○ (G) —— ○ (H) —— ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

This is the end of Q7. Proceed to Q8 on your Gradescope answer sheet.

Q8 **(18 points)**

Q8.1 (4 points) Write a stateful firewall rule that would allow all TLS traffic from an external host `161.20.2.0` into your network `16.120.20.0/24`.

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

Q8.2 (4 points) Recall that an attacker can spoof source IPs to hide themselves while executing a DoS attack. Assume the attacker securely randomly generates these IPv4 addresses. Describe a pattern in the packets that a network operator could observe to best discern whether or not their network is a victim of a DoS attack.

○ (G) —— ○ (H) —— ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

Q8.3 (6 points) What intrusion detection method would be *best* fit to perform the previous analysis? Justify your answer.

○ (A) HIDS ○ (C) Logging ○ (E) ——

○ (B) NIDS ○ (D) —— ○ (F) ——

Q8.4 (4 points) Describe a major drawback or exploit to the intrusion detection method you described above.

○ (G) —— ○ (H) —— ○ (I) —— ○ (J) —— ○ (K) —— ○ (L) ——

This is the end of Q8. Proceed to Q9 on your Gradescope answer sheet.

Q9 (12 points)

EvanBot has decided to switch career paths and pursue creating new cryptographic hash functions. EvanBot proposes two new hash functions, E and B:

$$E(x) = H(x_1 x_2 \dots x_{M-1})$$
$$B(x) = H(x_1 x_2 \dots x_M || 0)$$

where H is a preimage-resistant and collision-resistant hash function, $x = x_1 x_2 \dots x_M$, $x_i \in \{0, 1\}$ and $||$ denotes concatenation.

In other words, $E(x)$ calls H with the last bit of x removed, and $B(x)$ calls H with a 0 bit appended to x.

Q9.1 (3 points) Is $E(x)$ preimage-resistant? Provide a counter-example if it is not.

○ (A) Yes ○ (C) —— ○ (E) ——

○ (B) No ○ (D) —— ○ (F) ——

Counterexample:

Q9.2 (3 points) Is $E(x)$ collision-resistant? Provide a counter-example if it is not.

○ (G) Yes ○ (I) —— ○ (K) ——

○ (H) No ○ (J) —— ○ (L) ——

Counterexample:

Q9.3 (3 points) Is $B(x)$ preimage-resistant? Provide a counter-example if it is not.

○ (A) Yes ○ (C) —— ○ (E) ——

○ (B) No ○ (D) —— ○ (F) ——

Counterexample:

Q9.4 (3 points) Is $B(x)$ collision-resistant? Provide a counter-example if it is not.

○ (G) Yes ○ (I) —— ○ (K) ——

○ (H) No ○ (J) —— ○ (L) ——

Counterexample:

This is the end of Q9. Proceed to Q10 on your Gradescope answer sheet.

Q10 **(12 points)**

Alice comes up with a couple of schemes to securely send messages to Bob. Assume that Bob and Alice have known RSA public keys.

For this question, Enc denotes AES-CBC encryption, H denotes a collision-resistant hash function, $||$ denotes concatenation, and $\bigoplus$ denotes bitwise XOR.

Consider each scheme below independently and select whether each one guarantees confidentiality, integrity, and authenticity in the face of a MITM.

Q10.1 (3 points) Alice and Bob share two symmetric keys k_1 and k_2. Alice sends over the pair $[Enc(k_1, Enc(k_2, m)), Enc(k_2, m)]$.

□ (A) Confidentiality　□ (C) Authenticity　□ (E) ——

□ (B) Integrity　□ (D) ——　□ (F) ——

Q10.2 (3 points) Alice and Bob share a symmetric key k, have agreed on a PRNG, and implement a stream cipher as follows: they use the key k to seed the PRNG and use the PRNG to generate message-length codes as a one-time pad every time they send/receive a message. Alice sends the pair $[m \bigoplus \text{code}, HMAC(k, m \bigoplus \text{code})]$.

□ (G) Confidentiality　□ (I) Authenticity　□ (K) ——

□ (H) Integrity　□ (J) ——　□ (L) ——

Q10.3 (3 points) Alice and Bob share a symmetric key k. Alice sends over the pair $[Enc(k, m), H(Enc(k, m))]$.

□ (A) Confidentiality　□ (C) Authenticity　□ (E) ——

□ (B) Integrity　□ (D) ——　□ (F) ——

Q10.4 (3 points) Alice and Bob share a symmetric key k. Alice sends over the pair $[Enc(k, m), H(k||Enc(k, m))]$.

□ (G) Confidentiality　□ (I) Authenticity　□ (K) ——

□ (H) Integrity　□ (J) ——　□ (L) ——

This is the end of Q10. You have reached the end of the exam.

Fun Thing on Final Page

Here's a fish

```
><=>
```

Here's a phish

> Congratulations, you are the 100,000th visitor to our website! Click here to claim your prize.

Here's a spearphish

> <from no-reply@grapescope.com>
>
> Hi Foo,
>
> Your Midterm 2 for CS161, Spring 2020 has been graded! You can access your graded submission using the link below.
>
> View your graded work
>
> If you have never logged in to this site before, you can set your password. The login for your Grapescope account is `foo@bar.com`. (If you have any problems accessing the site, please contact help@grapescope.com.)
>
> Statistics:
> ...