Exam

You have signed in as **tianqiy@berkeley.edu**. Log out if this is not the right account.

Q0 Preliminaries

You can complete and submit these questions before the exam starts.

Q0.1

Points: 5

Read the following honor code and sign your name. *Failure to do so will result in a grad*
this exam.

> I understand that I may not collaborate with anyone else on this exam, c
> any way. I am aware of the Berkeley Campus Code of Student Conduct
> acknowledge that academic misconduct will be reported to the Center
> Student Conduct and may further result in partial or complete loss of cr

Tianqi Yang

Saved

Q0.2

What is your student ID number?

3034051336

Saved

Q1 True/false

Each true false is worth 2 points.

Q1.1

Points: 2

True or false: If a pseudorandom number generator (pRNG) is secure, then an attacker
sees the output of the pRNG is unable to learn its internal state.

- (•) True
- ( ) False

Saved

Q1.2

Points: 2

True or false: A primary advantage of a host-based intrusion detection system (HIDS) c
network-based intrusion detection system (NIDS) is that traffic can be analyzed in plai
the host can access decrypted TLS traffic.

- ( ) True
- (•) False

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q1.3

Points: 2

True or false: Sending all DNS requests and responses over TLS/HTTPS (DNS over HTTPS) can be used as an effective defense against censorship by preventing censors from knowing what websites you are visiting.

- ○ True
- ◉ False

Saved

Q1.4

Points: 2

True or false: Alice decides to use Tor to protect herself from tracking and surveillance Tor circuit contains three Tor nodes: an entry node, a relay node, and an exit node. Ass nodes do not collude. The exit node knows Alice's IP address but not the domain of the website she is visiting.

- ○ True
- ◉ False

Saved

Q1.5

Points: 2

True or false: Specification-based detection uses a blacklist.

- ○ True
- ◉ False

Saved

Q1.6

Points: 2

Consider two different detectors with the same false positive rate and false negative ra that false negatives and false positives are equally costly.

True or false: A website with a high volume of users but a low volume of attacks would benefit more from placing the detectors in series rather than in parallel.

- ◉ True
- ○ False

Saved

Q1.7

Points: 2

True or false: For organizations with a large number of network devices, network-based detection systems (NIDS) are easier to deploy and manage than host-based intrusion detection systems (HIDS).

- ○ True
- ◉ False

Saved

Q1.8

Points: 2

True or false: WPA2 is a protocol that translates IP addresses to MAC addresses.

- ○ True

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Saved

Q1.9

Points: 2

True or false: The UDP protocol guarantees that packets are delivered to the destination server by detecting dropped packets and retransmitting them until they are acknowledged.

- ○ True
- ◉ False

Saved

Q1.10

Points: 2

True or false: Publicly accessible stairs, walkways, and elevators can be considered pa
physical equivalent of a trusted computing base for airport security.

- ○ True
- ◉ False

Saved

Q1.11

Points: 2

True or false: Clickjacking refers to a class of attacks where the attacker manipulates t
interface of a website to convince the user to click something that they did not intend

- ◉ True
- ○ False

Saved

Q1.12

Points: 2

True or false: Cryptographically secure MACs can be constructed using secure cryptog
functions.

- ○ True
- ◉ False

Saved

Q1.13

Points: 2

True or false: Argon2 and PBKDF2 are appropriate algorithms to use when hashing and
passwords in a database.

- ◉ True
- ○ False

Saved

Q1.14

Points: 2

True or false: All forms of two-factor authentication (2FA) are resistant to phishing atta

- ○ True
- ◉ False

Saved

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Q1.15

Points: 2

True or false: One-time pads, as long as they are used correctly, are secure against an adversary with infinite computational power.

- ○ True
- ◉ False

Saved

Q1.16

Points: 2

True or false: Logging is a method of intrusion detection in which server log files are pr they can be asynchronously scanned to detect malicious activity.

- ○ True
- ◉ False

Saved

Q1.17

Points: 2

True or false: Signature-based intrusion detection systems are good at identifying nove attacks that have not been previously seen.

- ○ True
- ◉ False

Saved

Q1.18

Points: 2

True or false: TLS is able to prevent on-path attackers from learning metadata about you communications (e.g. request and response times, message length) by encrypting communications from a client to a server.

- ○ True
- ◉ False

Saved

Q1.19

Points: 2

True or false: When analyzing a cryptographic hashing scheme, preimage resistance (c implies collision resistance.

- ○ True
- ◉ False

Saved

Q1.20

Points: 0

True or false: `EvanBot is a real bot.`

- ○ True
- ◉ False

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q2 Mutuality

Recall the TLS handshake:

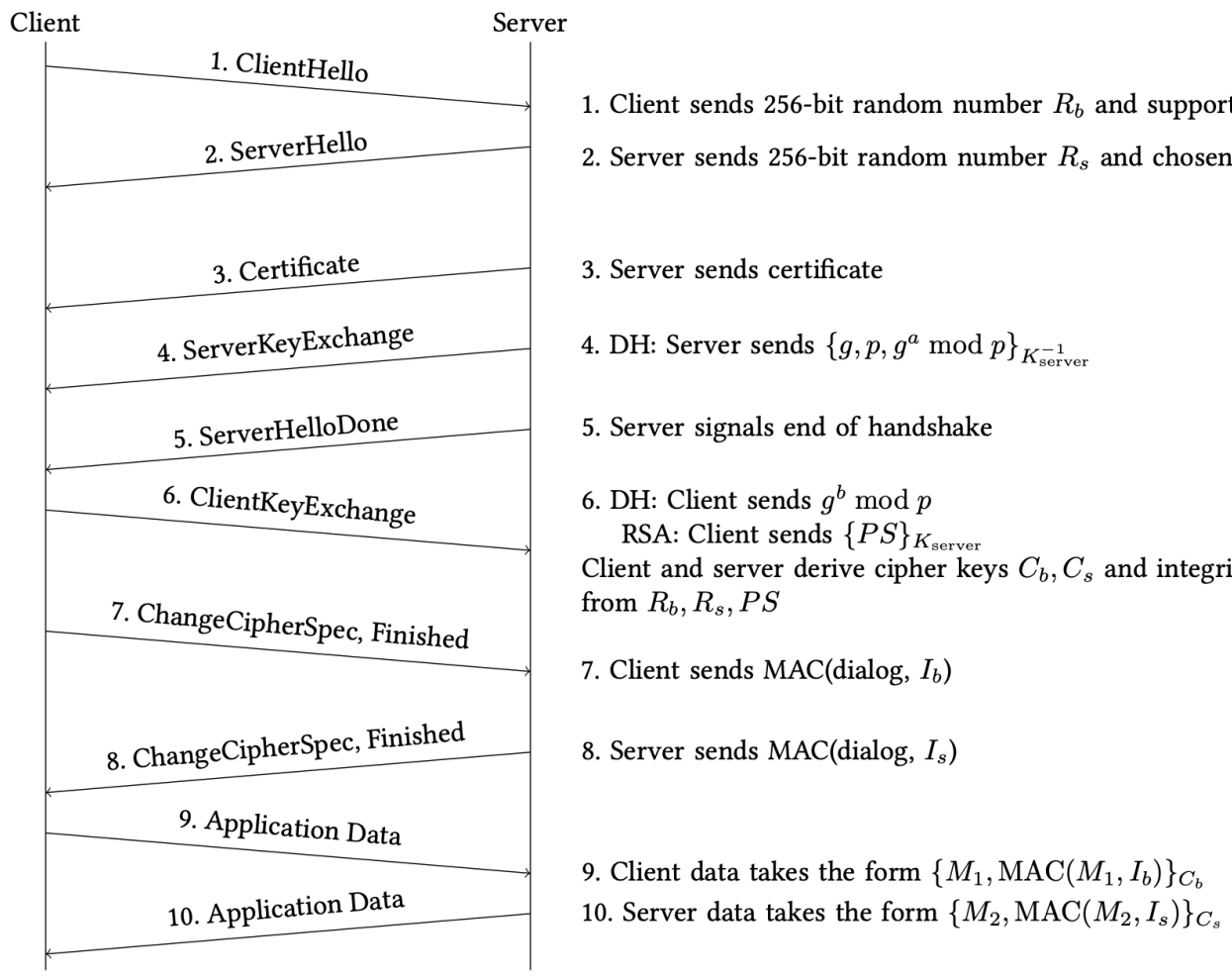


Diagram of the TLS handshake

In TLS, we verify the identity of the server, but not the client. How would we modify TL verify the identity of the client?

Q2.1

Points: 3

Which of these additional values should the client send to the server?

- ○ A certificate with the client's private key, signed by a certificate authority's private k
- ◉ A certificate with the client's public key, signed by a certificate authority's private ke
- ○ A certificate with the client's public key, signed by the server's private key
- ○ A certificate with the client's public key, signed by the client's private key

Saved

Q2.2

Points: 3

How should the client send the premaster secret in RSA TLS?

- ○ Encrypted with the server's public key, signed by a certificate authority's private ke
- ○ Encrypted with the client's public key, signed by a certificate authority's private key
- ◉ Encrypted with the server's public key, signed by the client's private key
- ○ Encrypted with the client's public key, signed by the server's private key

Saved

Q2.3

Points: 3

EvanBot argues that the key exchange protocol in Diffie-Hellman TLS doesn't need to l to support client validation. Is EvanBot right?

- ○ Yes, because the server has already received and verified the client's certificate
- ○ No, the client must additionally sign their part of the Diffie-Hellman exchange with t certificate authority's private key
- ◉ No, the client must additionally sign their part of the Diffie-Hellman exchange with the client's private key
- ○ Yes, because only the client knows the secret a, so the server can be sure it's talking to the

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Saved

Q2.4

Points: 2

True or false: The server can be sure that they're talking to the client (and not an attacker impersonating the client) immediately after the client and server exchange certificates.

- ○ False
- ◉ True

Saved

Q2.5

Points: 3

At what step in the TLS handshake can both the client and server be sure that they have derived the same symmetric keys?

- ○ Immediately after the TCP handshake, before the TLS handshake starts
- ○ Immediately after the ClientHello and ServerHello are sent
- ○ Immediately after the client and server exchange certificates
- ○ Immediately after the client and server verify signatures
- ◉ Immediately after the MACs are exchanged and verified

Saved

Q2.6

Points: 4

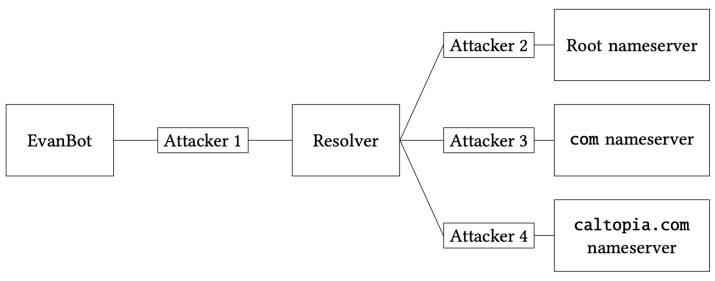
Which of these keys, if stolen individually, would allow the attacker to impersonate the Select all that apply.

- ☐ Private key of the server
- ☐ Private key of a certificate authority
- ☑ Private key of the client
- ☐ Public key of a certificate authority
- ☐ None of the above

Saved

Q3 Caltopia DNS

EvanBot is trying to determine the IP address of `caltopia.com` with DNS. However, sor on the network want to provide EvanBot with the wrong answer.



DNS network layout. Attacker 1 is between the client and resolver. Attacker 2 is betwee resolver and root nameserver. Attacker 3 is between the resolver and .com namserver. is between the resolver and caltopia.com nameserver.

Assumptions:

- Each attacker is a man-in-the-middle (MITM) attacker between their two neighbo diagram above.
- No attackers can perform a Kaminsky attack.
- Standard DNS (not DNSSEC) is used unless otherwise stated.
- been compromised unless otherwise stated.
- In each subpart, both EvanBot's cache and the local resolver's cache start empty.
- Each subpart is independent.

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

In each subpart, EvanBot performs a DNS query for the address of `caltopia.com`.

Q3.1

Points: 4

In this subpart only, assume the attackers only passively observe messages.

Which of the attackers would observe an `A` record with the IP address of `caltopia.com` as a result of EvanBot's query? Select all that apply.

- [x] Attacker 1
- [x] Attacker 2
- [ ] Attacker 3
- [ ] Attacker 4
- [ ] None of the above

Saved

Q3.2

Points: 3

Which of the attackers can poison the local resolver's cached record for `cs161.org` by record into the additional section of the DNS response? Select all that apply.

Note: Attacker 1 has intentionally been left out as an answer choice.

- [x] Attacker 2
- [ ] Attacker 3
- [ ] Attacker 4
- [ ] None of the above

Saved

Q3.3

Points: 4

Assume that the resolver and the name servers all validate DNSSEC, but EvanBot does DNSSEC. Which of the attackers can poison EvanBot's cached record for `caltopia.com` by modifying the DNS response? Select all that apply.

- [x] Attacker 1
- [ ] Attacker 2
- [ ] Attacker 3
- [ ] Attacker 4
- [ ] None of the above

Saved

Q3.4

Points: 5

In this subpart only, assume the attackers only passively observe messages.

Assume that everyone validates DNSSEC. Which of the following records would Attack observe as a result of EvanBot's query? Select all that apply.

- [ ] `A` record with the IP address of the `caltopia.com` name server
- [ ] `A` record with the IP address of `caltopia.com`
- [x] `DS` record with hash of the `.com` name server's public KSK
- [x] `DNSKEY` record with the `.com` name server's public KSK
- [ ] `DS` record with hash of the `caltopia.com` name server's public KSK
- [ ] None of the above

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q3.5

Points: 3

Assume that everyone validates DNSSEC, and the `caltopia.com` name server's private KSK has been compromised (i.e. all attackers know the `caltopia.com` name server's private KSK). No other private keys have been compromised.

Can EvanBot trust that they received the correct IP address of `caltopia.com`?

- ○ Yes, because the trust anchor (the root's KSK) has not been compromised
- ○ No, because the compromised KSK can be used to sign a malicious `A` record
- ◉ No, because the compromised KSK can be used to sign a fake ZSK that is used to s malicious `A` record
- ○ Yes, because the ZSK that signs the `A` record has not been compromised

Saved

Q3.6

Points: 2

True or false: DNSSEC prevents Attacker 4 from learning the IP address of `caltopia.c`

- ○ True
- ◉ False

Saved

Q4 UnicornBox v2

UnicornBox decides to implement 2-factor authentication (2FA).

The server stores a table of active codes with the following schema:

```
CREATE TABLE IF NOT EXISTS codes (
    username TEXT,
    code TEXT,
    -- Additional fields not shown.
);
```

When a user wants to log in:

1. The user logs in by making a POST request with their username and password.
2. The server randomly generates a 10-digit numerical code and stores it in the cod
3. The server sets a cookie with name = `login_user_cookie` and value = the user's the user's browser. The server also sends a text to the user's phone with the cod
4. The user makes a GET request to `https://unicornbox.com/confirm?code=$cod` `$code` is the code that was entered.
5. The server runs the SQL query `SELECT username FROM codes WHERE code = '$c` where `$code` is the value submitted by the user.
6. The server checks that the value returned by the SQL query matches the usernar the `login_user_cookie` cookie in the request submitted by the user.

Q4.1

Points: 5

Assume that `evan` is the name of an account in CalCentral with an entry in the `codes` ta

Construct an input for `$code` that would cause the SQL query in step 5 to return `evan`.

```
'; SELECT username FROM codes WHERE username = 'evan
```

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q4.2

Points: 4

How can you log in as `evan` without knowing their password? You may use `PAYLOAD` to reference your answer from the previous part.

Hint: You will need 2 steps. List both.

we try to log in as evan and make a GET request to https://unicornbox.com/confirm?code='; SELECT username FROM codes WHERE username = 'evan

we can use the returned login_user_cookie in the PAYLOAD to log in as evan.

Saved

Q4.3

Points: 4

Which of these defenses would stop your exploit from above? Select all that apply.

- [ ] Putting the hash of the username in the cookie instead of the username
- [x] Rate limiting requests to the UnicornBox server
- [ ] Using a 20-digit code instead of a 10-digit code
- [x] Using SQL prepared statements
- [ ] None of the above

Saved

Q4.4

Points: 2

Consider a modification to Steps 5 and 6. If there are any rows returned by the SQL qu
verification succeeds without checking the value of the returned username. However, t
returns an error without executing the query if the format of the code is not exactly 10 numerical
digits.

True or false: The modified scheme is no longer exploitable using SQL injection.

- (•) True
- ( ) False

Saved

Q4.5

Points: 2

Briefly (1 sentence) justify your answer from the previous part.

if they are exactly 10 numerical digits, they do not work as SQL sentences and canno
executed.

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q5 Plaintext Feedback

Consider the "plaintext feedback" (PFB) mode where the encryption formula for ciphertext block C_i is given as follows:

$$C_0 = IV$$
$$C_i = E(K, P_i) \oplus C_{i-1}$$

E is AES encryption and D is AES decryption.

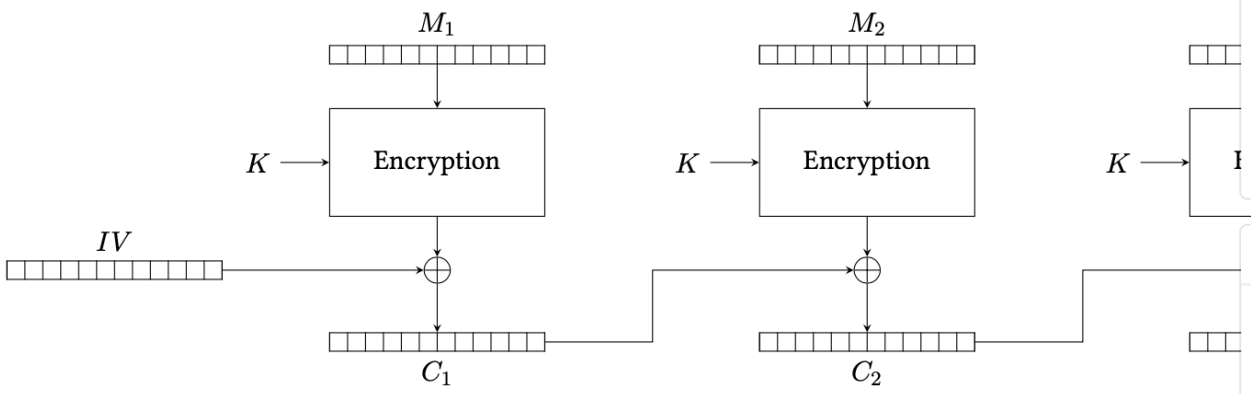


Diagram of the PFB mode of operation

Q5.1

Points: 3

Which of these is the corresponding decryption equation?

- ○ $P_i = E(K, C_i \oplus P_{i-1})$
- ○ $P_i = E(K, P_i \oplus P_{i-1})$
- ○ $P_i = D(K, C_i \oplus P_{i-1})$
- ○ $P_i = E(K, C_i \oplus C_{i-1})$
- ● $P_i = D(K, C_i \oplus C_{i-1})$
- ○ $P_i = D(K, P_i \oplus P_{i-1})$

Saved

Q5.2

Points: 3

Alice and Bob are communicating using PFB mode. Alice encrypts and sends a 10-block message encrypted using PFB. Bob receives the message, but the 6th ciphertext block C_6 is los transmission. Which blocks of plaintext can Bob recover? Assume Bob is aware that $C_$ transmission.

- ● Bob can recover all blocks except for P_6 and P_7.
- ○ Bob can recover all blocks up to and including P_5, but no block after that.
- ○ Bob can recover all blocks of the message.
- ○ Bob can recover all blocks up to and including P_6, but no block after that.
- ○ Bob cannot recover any block of the message.
- ○ Bob can recover all blocks except for P_6.

Saved

Q5.3

Points: 3

PFB mode is not IND-CPA secure. To prove this, the adversary will win the IND-CPA ga… against the challenger as follows:

First, the adversary sends two messages, P and P'. The first message P is 3 unique, r generated blocks, $P = P_1 || P_2 || P_3$. Which of the following values of P' would allow th… adversary to win the IND-CPA game?

- ○ $P' = P'_1 || P'_1 || P'_1$, where P'_1 is a randomly generated block
- ○ …re P'_i is the same as P_i, but with the last bit flipped
- ○ $P' = P'_1 || P'_2 || P'_3$, where P'_i is the same as P_i, but every bit flipped

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

- ○ $P' = P_1 || P_2 || P_3$
- ○ $P' = P_1' || P_2' || P_3'$, where P_1', P_2', and P_3' are unique, randomly generated blocks

Saved

Q5.4

Points: 3

The challenger sends back a ciphertext $C = C_0 || C_1 || C_2 || C_3$, which is an encryption of either P or P'. Describe a strategy that the adversary should use to deduce whether P or P' was encrypted that would allow them to win the IND-CPA game with probability greater tha

We can use C_0 xor C_1 to get encrypted P_0, C_1 xor C_2 to get encrypted P_1, C_2 get encrypted P_2. If the end of the bit of the encrypted P_0, P_1, P_2 has more ones, it as P, otherwise, it is P prime. If the win rate is less than 1/2, we guess it reversely.

Saved

Q5.5

Points: 3

Which of the following are true about PFB mode? Select all that apply.

- ☑ The plaintext must be padded to a multiple of the block length
- ☐ PFB provides integrity
- ☑ Decryption is parallelizable
- ☐ None of the above

Saved

Q6 TC sPeedy

Q6.1

Points: 3

To improve the speed of TCP, Alice suggests modifying the TCP protocol to allow data in the SYN and SYN-ACK packets during the 3-way handshake. The data in the SYN packet is immediately accepted by the server during the initial handshake (before the 3-way han finishes).

Which of the following attacks are possible on this modified scheme? Select all that ap

- ☑ An off-path attacker can fool the server into accepting some spoofed data.
- ☐ An off-path attacker can reliably execute a RST injection attack.
- ☐ An off-path attacker can reliably inject packets after a connection has been establis
- ☐ None of the above

Saved

Q6.2

Points: 2

Alice notices that her modified scheme may be vulnerable to a DoS attack where the a sends a large data payload in the SYN packet without completing the TCP handshake. okies as part of her modification.

True or false: SYN cookies provide a valid defense against the proposed DoS attack.

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

- ○ True
- ◉ False

Saved

Q6.3

Points: 4

Alice uses her modified 3-way handshake to form a TCP connection with a server. Assume that source port randomization is not in use.

What fields would an **on-path** attacker have to guess in order to inject some data from client to the server?

- ☐ Client IP address and port
- ☐ Server sequence number
- ☑ Client sequence number
- ☐ Server IP address and port
- ☐ None of the above

Saved

Q6.4

Points: 3

Alice modifies her protocol to use a cryptographic token. When a client and server con
first time:

1. The client sends a SYN packet with a token request.
2. The server generates a token with a MAC function using a key known only to the
   responds with a SYN-ACK packet to the client containing the token. The client an
   both store the token.
3. The client responds with an ACK packet, as in normal TCP.

In subsequent connections, the client skips the 3-way handshake by sending the SYN
both the token and data (similar to Alice's modification from previous parts). The server verifies
the value of the token and acknowledges both the SYN and the data. The server may b
sending data to the client before receiving the client's ACK as part of the handshake. T
rejects the SYN and data if the token is invalid.

Here are diagrams detailing the protocol:

Initial connection:

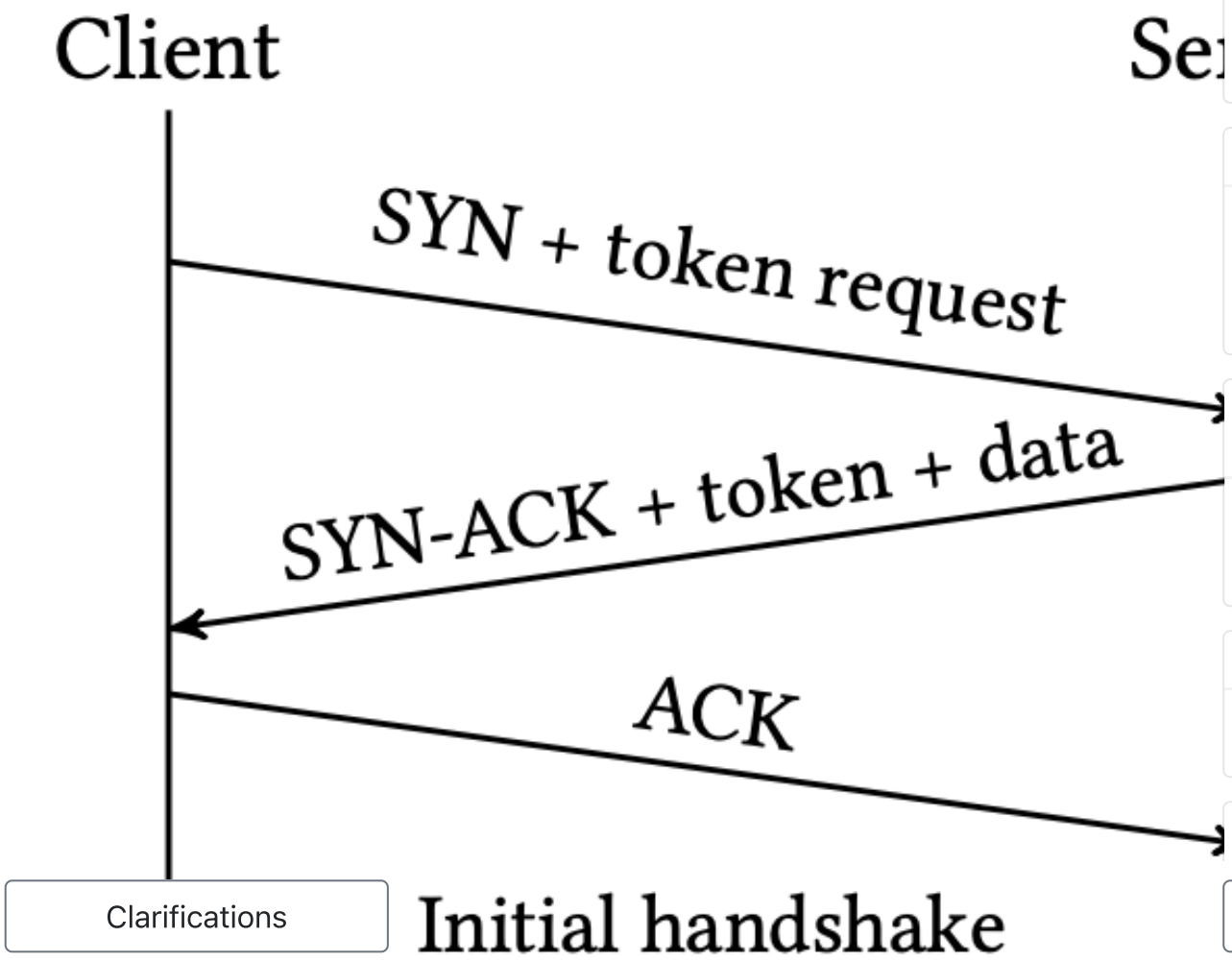


Diagram of the initial connection of the TFO protocol

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Subsequent connections:

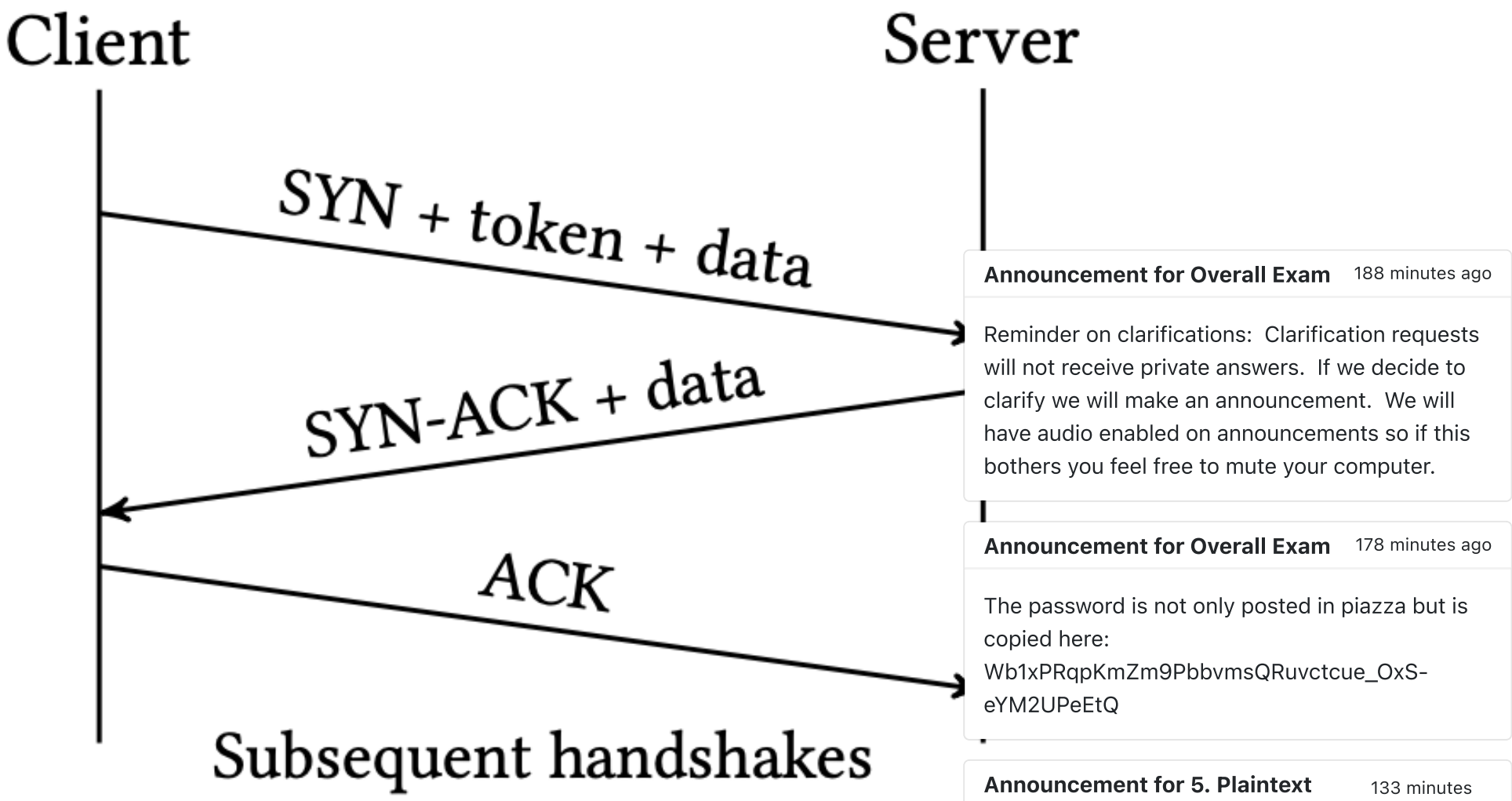


Diagram of subsequent connections of the TFO protocol

Which of the following attacks on TCP becomes more difficult with the addition of the t
Select all that apply.

- [x] RST injection
- [x] MITM hijacking
- [ ] Blind hijacking
- [ ] None of the above

Saved

Q6.5

Points: 3

A major issue with this protocol is that it is vulnerable to replay attacks, as an adversary can spoof a connection by replaying the token. A potential workaround is to modify the TTL (time the token. Name **one** benefit and **one** drawback of using a shorter TTL rather than a lo

Benefit: we can make sure the token would not be used for a long time by other peop they steal it.

Drawback: the client-side has to get the token after it expired if it too short, it would be poise

Saved

Q7 Full-Stack Security

Examtool is a test-taking website located at `https://exam.cs161.org/`. Assume that a connections are made over HTTPS, unless otherwise specified.

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Examtool uses session tokens for user authentication. Session tokens are stored as cookies with `Domain=exam.cs161.org` and no other cookie attributes (no `Secure` flag, no `HttpOnly` flag, `Path=/`).

When a student fills out or changes an answer, their browser makes a POST request to `https://exam.cs161.org/submit_question` with the student's updated answers.

Q7.1

Points: 5

Which of the following attacks could allow an adversary to read the session token cookie? Select all that apply.

- [x] Stored XSS attack at `https://exam.cs161.org/`
- [x] Reflected XSS attack at `https://exam.cs161.org/`
- [ ] Root access to the Wi-Fi access point that the student is using
- [ ] Root access to another device on the same Wi-Fi network that the student is using
- [ ] Exploitable buffer overflow vulnerability in browser
- [ ] None of the above

Saved

Q7.2

Points: 4

For a question on an exam, Alice first submits "A" and then later changes her answer ar
"B". What could a MITM attacker between Alice's computer and the `exam.cs161.org` ser
Select all that apply.

- [ ] Perform a replay attack to restore Alice's saved answer to "A"
- [ ] Modify Alice's submitted answer choice to "C"
- [x] Run JavaScript in Alice's browser
- [x] Perform a DoS attack to prevent Alice from submitting an answer choice
- [ ] None of the above

Saved

Q7.3

Points: 4

Suppose the MITM attacker has identified a vulnerability in HTTPS that allows them to
read and modify data in transit without detection. Alice submits another answer. What
MITM attacker between Alice's computer and the `exam.cs161.org` server do? Select al

- [ ] Redirect Alice's browser to `https://evil.com/`
- [x] Change Alice's answer choice without detection
- [x] Set cookie values for the page at `https://exam.cs161.org/`
- [ ] Access any file on Alice's computer
- [ ] None of the above

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q7.4

Points: 2

This subpart and following subparts are independent of previous subparts.

An instructor uploads an exam to Examtool by applying some cryptography to the exam and sending it over an insecure channel.

Assumptions:

- m is the message to encrypt (i.e. the exam).
- $||$ is concatenation.
- k_1 and k_2 are two different secret keys known only to the Examtool server and th
- $E(k, m)$ is the encryption function of an IND-CPA secure symmetric encryption s
- $\mathrm{MAC}(k, m)$ is a secure MAC function.

For each pair of cryptographic schemes, select the scheme with fewer potential vulner

Select the more secure scheme:

- ○ $C = C_1||C_2$, where $C_1 = E(k_1, m)$ and $C_2 = \mathrm{MAC}(k_1, C_1)$
- ◉ $C = C_1||C_2$, where $C_1 = E(k_1, m)$ and $C_2 = \mathrm{MAC}(k_2, C_1)$

Saved

Q7.5

Points: 2

Select the more secure scheme:

- ○ $C = C_1||C_2$, where $C_1 = E(k_1, m)$ and $C_2 = \mathrm{MAC}(k_2, C_1)$
- ◉ $C = E(k_1, m||\mathrm{MAC}(k_2, m))$

Saved

Q8 "Bank-Grade" Security

Bear Bank is using a third-party analytics service called ABtesters. To use it, the bank v
includes a tag to load the ABtesters JavaScript library.

Bear Bank's website is located at `https://bearbank.com` and contains the following HTML:

```
<script src="https://cdn.abtesters.com/lib.js"></script>
<form name="login" action="/login" method="POST">
  <input type="text" name="username" />
  <input type="password" name="password" />
</form>
```

Q8.1

Points: 5

In the same-origin policy, which of the following are used in determining the origin of a
webpage? Select all that apply.

- ☑ Server port
- ☐ None of the above
- ☑ Request path
- ☑ Domain name
- ☐ Server IP
- ☐ Protocol

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q8.2

Points: 3

Bear Bank is concerned that the ABtesters JavaScript library could steal customer passwords from the login form if the JavaScript library were compromised. Is this a valid concern?

- ○ No, because the ABtesters JavaScript library can only execute specific JavaScript functions required for its basic functionality.
- ◉ Yes, because the ABtesters JavaScript library executes with the origin of Bear Bank's webpage.
- ○ No, because `https://cdn.abtesters.com` uses a certificate that is signed for different domain name.
- ○ Yes, because the ABtesters JavaScript library executes with the origin of ABtester's

Saved

Q8.3

Points: 3

Bear Bank decides to move the login form to `https://auth.bearbank.com` and embed homepage (`https://bearbank.com/`) in an iframe.

Can the ABtesters JavaScript library running on Bear Bank's homepage steal customer from the login form in the iframe?

- ○ No, because the ABtesters JavaScript library has a different origin than the login fo
- ◉ Yes, because the ABtesters JavaScript library can execute any JavaScript it wants o Bank's homepage.
- ○ No, because the ABtesters JavaScript library is not developed by Bear Bank itself.
- ○ Yes, because the ABtesters JavaScript library is running on the same page as the if

Saved

Q8.4

Points: 3

After a user successfully logs into their account, Bear Bank's website sets a `session_t` to track the user's logged in status and allows users to transfer transfer funds by makin request to `https://bearbank.com/transfer`.

Which of the following cookie attributes would cause the `session_token` cookie to be s request to `https://bearbank.com/transfer`? Select all that apply.

- ☑ Domain=auth.bearbank.com; Path=/login; HttpOnly; Secure
- ☑ Domain=bearbank.com; Path=/transfer; Secure
- ☑ Domain=bearbank.com; Path=/transactions
- ☐ None of the above

Saved

Q8.5

Points: 3

Bear Bank realizes that there are no CSRF protections on the transfer form, which mea can steal money from users' accounts.

Which of the following methods are are reliable defenses against CSRF attacks? Select apply.

- ☐ Move the transfer form to an iframe hosted at `https://transfer.bearbank.com`
- ☐ Check the referrer header on the server when processing the transfer form submission
- ☑ Add a random CSRF token to the transfer form each time the page loads
- ☐ None of the above

Saved

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Q8.6

Points: 4

The following subparts are independent of the previous subparts.

Tree Bank is a different bank considering alternative security methods. Once a user is logged in, they can send HTTP requests to Tree Bank to make transactions. Each request contains a session token set by the server when the user first logged in. The requests do not contain any counters or timestamps. The requests are sent over HTTP (not HTTPS).

Eve is an on-path attacker.

Eve observes a single request from EvanBot to Tree Bank, which contains a transactior Eve do? Select all that apply.

- [x] Learn the contents of EvanBot's transaction
- [x] Repeat EvanBot's transaction
- [x] Learn EvanBot's session token
- [ ] Learn EvanBot's password
- [ ] None of the above

Saved

Q8.7

Points: 4

Assume that the user knows Tree Bank's public key, and Tree Bank's corresponding pri has not been compromised.

Suppose that Tree Bank requires that the user encrypt the entire HTTP request (includ transaction and token) with the ElGamal scheme from lecture before sending it to the bank.

Eve observes a single encrypted request from EvanBot to Tree Bank, which contains a What can Eve do? Select all that apply.

- [x] Repeat EvanBot's transaction
- [ ] Learn EvanBot's password
- [ ] Learn the contents of EvanBot's transaction
- [ ] Learn EvanBot's session token
- [ ] None of the above

Saved

Q8.8

Points: 3

What is the best way for the bank to defend against Eve's attacks, and what concept b describes the design flaw that allowed Eve to compromise EvanBot's requests?

- ( ) Use TLS. Security is economics.
- ( ) Use TLS. Least privilege.
- ( ) Use TLS. Don't build your own crypto.
- ( ) Use DNSSEC. Security is economics.
- ( ) Use DNSSEC. Least privilege.
- ( ) Use DNSSEC. Don't build your own crypto.

Saved

Q9 Storefront

Definitions for the relevant C functions are given below:

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

```
int strncmp(const char *s1, const char *s2, size_t n);

       The  strncmp()  function  compares  the  first (at most) n bytes of two
       strings s1 and s2. It returns  an  integer  less  than,  equal  to,  or
       greater  than  zero  if  s1 is found, respectively, to be less than, to
       match, or be greater than s2.

char *fgets(char *s, int size, FILE *stream);

       fgets()  reads in at most one less than size characters from stream and
       stores them into the buffer pointed to by s.  Reading  stops  afte
       EOF  or a newline.  If a newline is read, it is stored into the bu
       A terminating null byte ('\0') is stored after the  last  characte
       the buffer
```

Consider the following vulnerable C code:

```
 1  void copy_string(char *dst, const char *src, size_t n) {
 2      for (size_t i = 0; i < n + 1; i++) {
 3          dst[i] = src[i];
 4          if (src[i] == '\0') {
 5              break;
 6          }
 7      }
 8  }
 9
10  void add_to_store(char *lst) {
11      char listing[256];
12
13      copy_string(listing, lst, 256);
14
15      printf("Contacting server to add: %s...\n", listing);
16      contact_server_and_wait(listing); // Implementation not shown.
17  }
18
19  void invoke(char *lst) {
20      add_to_store(lst);
21  }
22
23  int main(void) {
24      char buf[4096];
25      do {
26          fgets(stdin, buf, 4096);
27          invoke(buf);
28      } while (strcmp(buf, "exit") != 0);
29      return 0;
30  }
```

Assume you are on a little-endian 32-bit x86 system. Assume that there is no compiler padding or saved additional registers in all questions. For the first four parts, assume that **no mem defenses** are enabled.

Q9.1

Points: 3

Which of the following memory safety vulnerabilities is present in this code?

- ○ Format string vulnerability
- ○ Signed/unsigned vulnerability
- ○ Off-by-one
- ◉ None of the above

Saved

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

“Reliably” means that the attacker doesn’t have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements

Q9.2

Points: 3

Which of the following values on the stack can be partially or completely overwritten by the call to `copy_string` at line 13? Select all that apply.

Hint: Draw a stack diagram.

- [ ] SFP of `add_to_store`
- [ ] RIP of `add_to_store`
- [x] `listing`
- [ ] None of the above

Saved

Q9.3

Points: 5

Assume that the address of `listing` is 0xf2e6f630. Construct an input at Line 26 that an attacker to execute malicious shellcode. You may reference the variable `SHELLCODE` byte shellcode in your answer. Write your answer in Python 2 syntax (just like in Project

```
223 * 'a' + '\37\f7\e6\f2' + SHELLCODE
```

Saved

Q9.4

Points: 3

Your exploit from above may not necessarily work with all possible addresses of `listing`. Provide **one** such address that would prevent your exploit from working. Write your answer in a `0xdeadbeef`.

```
0x00000000
```

Saved

Q9.5

Points: 3

Which of the following techniques could an attacker use to execute malicious shellcod and no other defenses are enabled? Select all that apply.

- [ ] Server-side request forgery
- [x] ret2esp
- [ ] Return-oriented programming
- [ ] None of the above

Saved

Q9.6

Points: 2

True or false: Stack canaries with no other defenses would prevent an attacker from ex malicious shellcode in this code (not necessarily using your exploit from above). Assum bytes of the stack canary are randomized.

- ( ) True
- (•) False

Saved

Q9.7

Clarifications

he previous part.

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Attacker still can find out the canaries and skip it then executing malicious shellcode.

Saved

Q9.8

Points: 2

True or false: ASLR with no other defenses would prevent an attacker from executing malicious shellcode in this code (not necessarily using your exploit from above).

- ○ True
- ◉ False

Saved

Q9.9

Points: 2

Justify your answer from the previous part.

Attacker still can execute malicious shellcode since the ASLR is only randomized to the layout.

Saved

Q10 Cat

Clarifications

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Q10.1

Points: 0

What is the name of Nick's gray cat?

nunu

Saved

🎉Congratulations!🎉

You have reached the end of the exam! Your answers will all be automatically save

Clarifications

Q6.4 ✓

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here: Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

"Reliably" means that the attacker doesn't have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Hide Announcements

Q6.5 ✓

7. Full-Stack Security ✓

Q7.1 ✓

Q7.2 ✓

Q7.3 ✓

Q7.4 ✓

Q7.5 ✓

8. "Bank-Grade" Security ✓

Q8.1 ✓

Q8.2 ✓

Q8.3 ✓

Q8.4 ✓

Q8.5 ✓

Q8.6 ✓

Q8.7 ✓

Q8.8 ✓

9. Storefront ✓

Q9.1 ✓

Q9.2 ✓

Q9.3 ✓

Q9.4 ✓

Q9.5 ✓

Q9.6 ✓

Q9.7 ✓

Q9.8 ✓

Q9.9 ✓

10. Cat ✓

Q10.1 ✓

Announcement for Overall Exam 188 minutes ago

Reminder on clarifications: Clarification requests will not receive private answers. If we decide to clarify we will make an announcement. We will have audio enabled on announcements so if this bothers you feel free to mute your computer.

Announcement for Overall Exam 178 minutes ago

The password is not only posted in piazza but is copied here:
Wb1xPRqpKmZm9PbbvmsQRuvctcue_OxS-eYM2UPeEtQ

Announcement for 5. Plaintext Feedback 133 minutes ago

IVs are always randomly generated and never reused in this question.

Announcement for 3. Caltopia DNS 132 minutes ago

Assume that bailiwick checking is in use for this entire question.

Announcement for 6.1. 127 minutes ago

“Reliably” means that the attacker doesn’t have to guess any values.

Announcement for 5. Plaintext Feedback 126 minutes ago

M_i in the encryption diagram refers to plaintext block P_i.

Announcement for 2. Mutuality 123 minutes ago

All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Announcement for 4. UnicornBox v2 120 minutes ago

In step 1, the server verifies the password and will not proceed if the password is wrong.

Announcement for 9. Storefront 109 minutes ago

Line 26 should be fgets(buf, 4096, stdin).

Announcement for 4. UnicornBox 102 minutes

Clarifications

Hide Announcements