Nick Weaver
Fall 2018

CS 161
Computer Security

Midterm 2

PRINT your name: ______________________, ______________________
(last) (first)

I am aware of the Berkeley Campus Code of Student Conduct and acknowledge that academic misconduct will be reported to the Center for Student Conduct.

SIGN your name: ______________________

PRINT your class account login: `cs161-`______________________ and SID: ______________________

Name of the person sitting to your left: ______________________

Name of the person sitting to your right: ______________________

You may consult one sheet of paper of notes. You may not consult other notes, textbooks, etc. Calculators, computers, and other electronic devices are not permitted. We use Gradescope for grading so please write your answers in the space provided.

If you think a question is ambiguous, please come up to the front of the exam room to the staff. If we agree that the question is ambiguous we will add clarifying assumptions to the central document projected in the exam rooms.

You have 110 minutes. There are 9 questions, of varying credit (120 points total). The questions are of varying difficulty, so avoid spending too long on any one question. Use a #2/hb or softer pencil. For bubble questions, fill the bubble completely and clearly erase any mistakes.

Some of the test may include interesting technical asides as footnotes. You are not responsible for reading the footnotes.

Do not turn this page until your instructor tells you to do so.

Problem 1 ***The Pot that keeps Pouring: Potpourri*** **(10 points)**

(a) TRUE or FALSE: Since the world wide web's inception 28 years ago, web technologies have exemplified implementing security from the start.

- ◯ TRUE
- ◯ FALSE

(b) TRUE or FALSE: Using HTTPS protects against browser extensions which seek to tamper with your web requests.

- ◯ TRUE
- ◯ FALSE

(c) Nick's Halloween costume was...

- ☐ Cozy Bear
- ☐ The 10th Doctor
- ☐ A Responsible Adult
- ☐ Severus Snape

(d) While monitoring dark web forums, you see Dr.Eggwoman touting Shadedoe: a malicious **on-path server that can always out-race packets** in Sonic Corp's internal network. Which protocols/systems may Shadedoe compromise?

- ☐ DNS
- ☐ DHCP
- ☐ DNSSEC
- ☐ ARP

(e) Which of the following attacks *can be executed* by an in-path attacker *but can* ***not*** *be reliably executed* by an on-path attacker in the same location?

- ☐ Decrypt TLS traffic encrypted with RSA when the attacker knows the private key for the server.
- ☐ Decrypt TLS traffic encrypted with DHE when the attacker knows the private key for the server.
- ☐ Execute a CSRF attack
- ☐ Execute an XSS attack
- ☐ Block TCP connections to a targeted site
- ☐ Block UDP packets sent to a targeted site

(f) TRUE or FALSE: If an attacker obtains Boogle's certificate, they can impersonate Boogle.

- ◯ TRUE
- ◯ FALSE

(g) TRUE or FALSE: An on-path attacker in the local network may become a man-in-the-middle attacker after applying ARP spoofing attacks.

- ◯ TRUE
- ◯ FALSE

(h) TRUE or FALSE: An otherwise off-path attacker who controls a different autonomous system may become a man-in-the-middle attacker after applying BGP hijacking.

- ◯ TRUE
- ◯ FALSE

Problem 2 ***DJ MC*** **(10 points)**

(a) Which of the following would ensure confidentiality of communications with a website?

☐ DNSSEC ☐ TCP ☐ SYN Cookies

☐ TLS ☐ UDP ☐ BGP

(b) Which of the following would increase the availability of a website?

☐ DNSSEC ☐ TCP ☐ SYN Cookies

☐ TLS ☐ UDP ☐ BGP

(c) Is TCP or UDP more appropriate for a low-latency application, such as a video game server?

○ TCP ○ UDP ○ Equally appropriate

(d) Protocols built on ______ are more susceptible for use in an amplification attack.

○ TCP ○ UDP ○ Either (equally susceptible)

(e) Which protocol is easier to spoof?

○ TCP ○ UDP ○ Equally easy

(f) Which of TCP and UDP are used when you go to visit `http://example.com`? (Assume all caches are empty.)

○ TCP ○ UDP ○ Both

(g) Which of the following defend against XSS attacks?

☐ Input Sanitization ☐ ARP Spoofing ☐ Framebusting

☐ Prepared Statements ☐ A strong CSP ☐ HTTPS

Problem 3 ***Jokers to the Left of Me...*** **(14 points)**

During the feedback process some students decided to provide some "humorous" responses in the form of fake "attacks". We appreciated the jokes enough to turn them into a midterm question, to see if the students understood the attacks behind the jokes.

(a) One response for a comment was:
`'; drop table MIDTERM_GRADES --`

What type of attack would this comment be?

How would the data need to be interpreted by a vulnerable system for this to be an actual attack?

Why is there a `--` in the attack?

What is the *robust* mitigation for this attack?

(b) Another response was:
`<script>alert("Gimme An A")</script>`

What type of attack would this comment be?

How would the data need to be interpreted by a vulnerable system for this to be an actual attack?

What is the *robust* mitigation for this attack?

(c) A final response was:
`<IMG SRC="https://calcentral.berkeley.edu/assigngrade?sid=11167570&grade=A+++">`

What is the type of vulnerability on `calcentral` that needs to be present for this attack?

What is the *robust* mitigation `calcentral` can deploy to mitigate this attack?

Problem 4 ***TLS Fuckups to the Right...*** **(18 points)**

Consider the following bugs in a TLS implementation.

(a) Consider a pseudorandom number generator which has the property that the next output or previous output is predictable from the current output. The browser is using this pRNG but the server is using a secure pRNG.

TRUE or FALSE: This would break confidentiality of RSA TLS, even if the attacker *cannot* make the user connect to an attacker-controlled site.

○ TRUE ○ FALSE

Explain (be concise):

(b) TRUE or FALSE: The attack above would apply to TLS using Ephemeral Diffie-Hellman.

○ TRUE ○ FALSE

Explain (be concise):

(c) Now consider where the server, not the browser, has the bad pRNG. TRUE or FALSE: This would break confidentiality of RSA TLS, even if the attacker *cannot* make the user connect to an attacker-controlled site.

○ TRUE ○ FALSE

Explain (be concise):

(d) TRUE or FALSE: The attack above would apply to TLS using Ephemeral Diffie-Hellman.

○ TRUE ○ FALSE

Explain (be concise):

(e) A buggy Diffie-Hellman TLS browser implementation increments its secret value for a by 1 every connection. It connects to properly secure server implementations using ephemeral Diffie-Hellman. TRUE or FALSE: This would break confidentiality of DH TLS only if the attacker *can* make a user connect to an attacker-controlled site first.

○ TRUE ○ FALSE

Explain (be concise):

(f) TRUE or FALSE: This would have forward secrecy.

○ TRUE ○ FALSE

Explain (be concise):

(g) Google uses a hierarchical certificate structure. They operate their own root CA whose private key is used to sign individual server certificates for Google servers. This CA certificate is trusted by the browser just like any other root certificates. If an attacker can get the private key corresponding to Google's root certificate, which of the following are true?

☐ An on-path attacker can decrypt all future traffic to Google.

☐ An in-path attacker can modify content a user sees from Google.

☐ An on-path attacker who stored all old Diffie-Hellman TLS traffic to Google can decrypt this traffic.

☐ If DNSSEC is enabled, a man-in-the-middle attacker can impersonate Google.

☐ An in-path attacker can impersonate other secure websites that use certificate pinning.

☐ An in-path attacker can impersonate other secure websites that do not use certificate pinning.

☐ An on-path attacker who stored all old RSA TLS traffic to Google can decrypt this traffic.

Problem 5 ***Know your ABBCs*** **(18 points)**

Suppose you are the webmaster for the Anti-Blockchain Blockchain Club (ABBC). You're creating a website `abbc.berkeley.edu`.

(a) Your friend Eric from ABBC notices that when he goes to `http://blockchain.berkeley.edu?q=whatsupdawg`, their website redirects to the search results page, at the top of which are the words: **Showing results for: whatsupdawg**. What is a potential vulnerability in this code?

(b) How can you exploit this vulnerability? Provide a specific URL that you could enter to steal the cookie of the person logged into `blockchain.berkeley.edu`. Assume that you have a script to record inputs from the URL at `http://abbc.berkeley.edu/save?message=<input>`. You can open a website in JS using window.open("URL") and that you can concatenate strings in javascript using the + operator.

(c) Blockchain @ Berkeley fixes this before you can exploit it. However, your friend Austin has joined Blockchain @ Berkeley to give you some insider info. He notices that the Blockchain @ Berkeley cookie is scoped to `berkeley.edu`. How can you exploit this when Blockchain @ Berkeley users visit the `abbc.berkeley.edu` site to spy on who they view as their competition?

(d) Which policy allows `abbc.berkeley.edu` to launch this attack?

(e) How would Blockchain @ Berkeley prevent this attack?

(f) Suppose you go home and open your personal website, `imsogoodathacking.com`. You have a similar script at this website to store inputs. Can you launch the same attack as in part (c) using your personal website instead of `abbc.berkeley.edu`?

Problem 6 ***Wi-Fi (in)-Security*** **(13 points)**

Berkeley is under attack! A rogue agent from Leland Stanfraud Junior College has penetrated the campus's security "perimeter" (aka, hopped on Bart and walked up hill) and is attempting to subvert Berkeley's students and networking in an attempt to launch psychological attacks to affect the Big Game.

(a) The campus has an open Wi-Fi service called CalVisitor; it does not use WPA, WPA2, or any security enhancements[1]. The hacker wants to attack Berkeley students who are using CalVisitor. What are some possible attacks?

- ☐ Identify which devices are browsing sites that use TLS.
- ☐ Block other users from visiting sites that do not use TLS.
- ☐ Block other users from visiting sites that use TLS.
- ☐ Identify which devices are browsing unencrypted sites.
- ☐ Steal cookies for sites that use TLS but don't mark cookies as `secure` and don't use HSTS or cert pinning.
- ☐ Steal cookies for sites that use TLS that don't mark cookies as `secure` but do use HSTS or cert pinning.
- ☐ "Rickroll" visitors of encrypted sites by causing a video to play of the infamous Roy "Wrong Way" Riegels play in the 1929 Rose Bowl.[2]
- ☐ "Rickroll" visitors of sites that do not use TLS by causing a video to play of the infamous Roy "Wrong Way" Riegels play in the 1929 Rose Bowl.

(b) Fortunately, within 15 seconds, the hacker was caught by the CS161 GSIs. *At the extremes* what are some possible consequences?

- ☐ UCPD arrests the hacker
- ☐ The hacker is prosecuted for violating the Wiretap act
- ☐ Campus decides to terminate CalVisitor

(c) After this crisis, most students realize that they are not well-prepared for the dangerous Internet. The campus decides to help the students, but still wants to keep CalVisitor for real visitors.

The campus does the following: if a student uses CalVisitor to visit Berkeley websites and logs in through the CalNet Authentication Service (CAS), the campus will:

- Send you a warning email: You should not use CalVisitor; instead, use AirBears2.
- Add CS161 into your next semester's course enrollment shopping cart.
- <u>Add this machine to a denylist/blacklist of CalVisitor; it can no longer connect to CalVisitor.</u>

To implement the underlined, the campus collects some information about the device. This information appears on the layer-2 (link layer), and it should be unique for each device. When it is added the denylist/blacklist, all CalVisitor access points will reject devices with this information.

What is this information? Write down its abbreviation or the full phrase (less than 5 words).

[1] In fact, CalVisitor deliberately blocks outbound `ssh`, so you can't use ssh to create a secure VPN onto a better network! So not only is it insecure but there are measures taken to deliberately prevent users from establishing a secure connection.

[2] This was when a Cal player, Roy "Wrong Way" Riegels, recovered a fumble and ran the wrong way. He was eventually tackled by a teammate at the 1 yard line and the next play resulted in a safety. Georgia Tech ended up winning the game 8-7 and winning the National Championship.

The idea above is actually broken for a reason that we won't discuss here. The campus has another idea: encourage the students to use the campus VPN for all Internet connections. If a student uses the campus VPN for at least 10 hours per week, the student gets a 50% tuition remission[3].

In more detail, a student can securely install campus VPN software on personal devices. The VPN software is *hardcoded with Berkeley's certificate* and by default will be turned on. To log in to the VPN, the user uses his/her CalNetID and passwords. *All* the user's traffic and requests are automatically routed through the VPN.

The campus will count the time a student uses the VPN. If a student satisfies the requirement for the whole semester, he/she will receive a check at the end of the final exam of CS161.

(d) Imagine the student now uses a password-less public Wi-Fi at Charbucks, the VPN is turned on, and the student connects to http://www.bank.com/ and types in their password. Is the student's password protected against a local attacker at the Wi-Fi network at Charbucks?

○ Yes, the student is protected.

○ No, the student is not protected.

(e) What information can Charbucks infer about the Cal VPN user, assuming Charbucks is doing sophisticated network analysis and doesn't care about legal restrictions:

☐ That the user is a regular customer based on a device identifier visible to the Charbucks network.

☐ That the user is probably affiliated with Cal.

☐ What sites the user is visiting based on IP address.

☐ That the user is *probably* watching a 4K video rather than visiting a class website.

[3]NOTE: This idea is also broken because the partial fee remission may encourage students to delegate their CalNet usernames/passwords to a friend who can help them satisfy the online requirement, which is never a secure practice.

Problem 7 *DNS, DNSSEC and its Discontents* (12 points)

(a) Write the firewall rule necessary to let all internal hosts on the interface `int` access just the Google Public DNS server (8.8.8.8) which validates DNSSEC. Reminder, DNS uses port 53, and requires both TCP and UDP.

(b) This allows clients to *potentially* validate DNSSEC using data received from Google Public DNS by querying with `DO` (DNSSEC-OK) set. To verify the DNSSEC signature for the valid A record for `www.stanfraud.com` which was queried with `DO` set and which returned just the answer and associated RRSIG (as `stanfraud.com` properly supports DNSSEC and they do have a record for `www.stanfraud.com`), a client would need to also request what information from the Google Public DNS server. If no record needs to be asked for of a given type, leave that part blank.

`DNSKEY` for:

`DS` for:

`NSEC` for:

(c) TRUE or FALSE: An on-path attacker between Google and the authority server for `stanfraud.com` can manipulate the results so that the a non-DNSSEC validating client will believe the wrong IP address for `www.stanfraud.com`.

○ TRUE ○ FALSE

Explain (be concise):

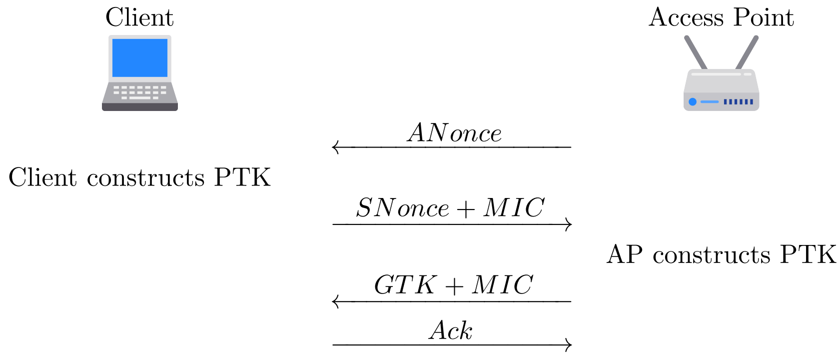
(d) TRUE or FALSE: An on-path attacker between the client and Google Public DNS can manipulate the results so that the a non-DNSSEC validating client will believe the wrong IP address for `www.stanfraud.com`.

○ TRUE ○ FALSE

Explain (be concise):

Problem 8 ***WPA2 Personal*** **(10 points)**

Consider the 4-way handshake used for the client to establish a connection to a Wi-Fi network, before receiving its network configuration.



Given a pre-shared key PSK, both client and access point compute the pairwise transient key as PTK = F(PSK, ANonce, SNonce, AP MAC, Client MAC).

(a) If the pre-shared key is not high entropy, an attacker who doesn't know the key but records this 4-way handshake can bruteforce the key in an offline attack.

○ TRUE ○ FALSE

(b) Even if the pre-shared key is high entropy and not known to the attacker, the attacker can still deploy a rogue access point that the client will trust as that network.

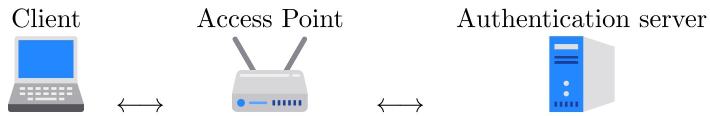
○ TRUE ○ FALSE

(c) If an adversary records the traffic for the whole session and only later is able to discover the value of the pre-shared key, the adversary can decrypt all data sent in both directions, since the protocol doesn't provide forward secrecy.

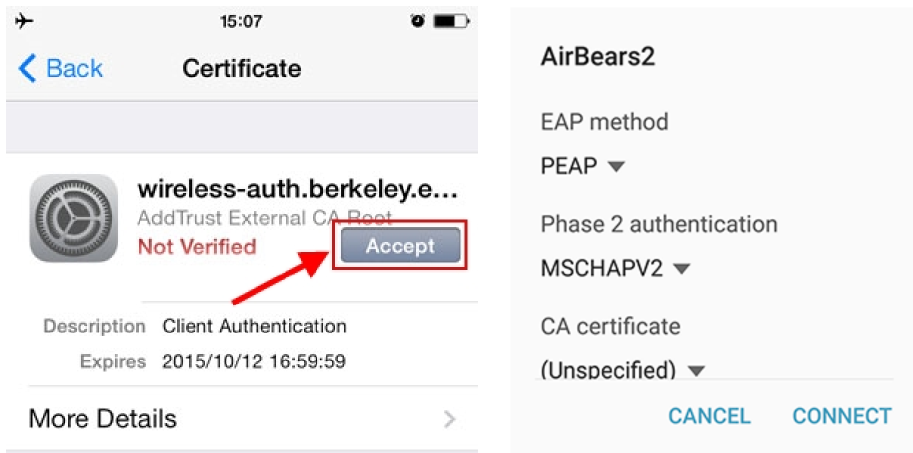
○ TRUE ○ FALSE

Problem 9 ***WPA2 Enterprise*** **(15 points)**

Now consider the network AirBears2, which uses PEAP, one variant of WPA2 Enterprise. Here, authentication is done by an authentication server (RADIUS server).



The official documentation provided by the university on how to connect to AirBears2 includes the following information:



iOS Device: If prompted with a **this security certificate has not been verified**, click **Accept**.

Android device: Make the following selection for CA certificate: **Do not validate**

(a) If a student follows the instructions provided for either iOS or Android, they will be vulnerable to an attacker that impersonates the authentication server when they first connect to the network.

○ TRUE ○ FALSE

Explain (be concise):

(b) Those two setups (iOS or Android) are equivalent in terms of security against impersonation of the authentication server after the first connection.

○ TRUE ○ FALSE

Explain (be concise):

(c) What are possible ways for an attacker to impersonate the authentication server during this initial connection?

- ☐ ARP spoofing
- ☐ Rogue Access Point
- ☐ BGP hijacking
- ☐ Rogue DHCP
- ☐ DNS poisoning

When connecting to AirBears2, the authentication server presents the following certificate chain.

Certificate	Summary
C1	Identity: wireless-auth.berkeley.edu Verified by: InCommon RSA Server CA
C2	Identity: InCommon RSA Server CA Verified by: USERTrust RSA Certification Authority
C3	Identity: USERTrust RSA Certification Authority Verified by: AddTrust External CA Root
C4	Identity: AddTrust External CA Root Verified by: AddTrust External CA Root

Assume that wireless-auth.berkeley.edu has a public/private key pair $K_w^{\text{pub}}, K_w^{\text{priv}}$ and assume that InCommon RSA Server CA has a public/private key pair $K_i^{\text{pub}}, K_i^{\text{priv}}$. Fill in the blanks in the following sentence:

Certificate C1 contains key (I)_________, (II)_________ by key (III)_________.

(d) Blank (I):

- ☐ K_w^{pub}
- ☐ K_i^{pub}
- ☐ K_w^{priv}
- ☐ K_i^{priv}

(e) Blank (II):

- ☐ encrypted
- ☐ signed

(f) Blank (III):

- ☐ K_w^{pub}
- ☐ K_i^{pub}
- ☐ K_w^{priv}
- ☐ K_i^{priv}

Outis decides to setup their Android connection to AirBears2 by choosing **Use system certificates** instead of **Do not validate**, and specifying the domain as wireless-auth.berkeley.edu. For their Linux laptop, Outis configures the connection to validate against the certificate C4, which is shipped with the Linux distribution. Assume that the AddTrust root certificate C4 is shipped with both Linux and Android.

(g) Do these measures prevent an adversary (without any additional knowledge) from being able to impersonate the authentication server?

○ Yes ○ No

(h) Is there a possible adversary that could impersonate the authentication server to Outis' Android phone, but not the Outis' Linux laptop?

○ Yes ○ No

Explain (be concise):

This Blank Deliberately Left Page

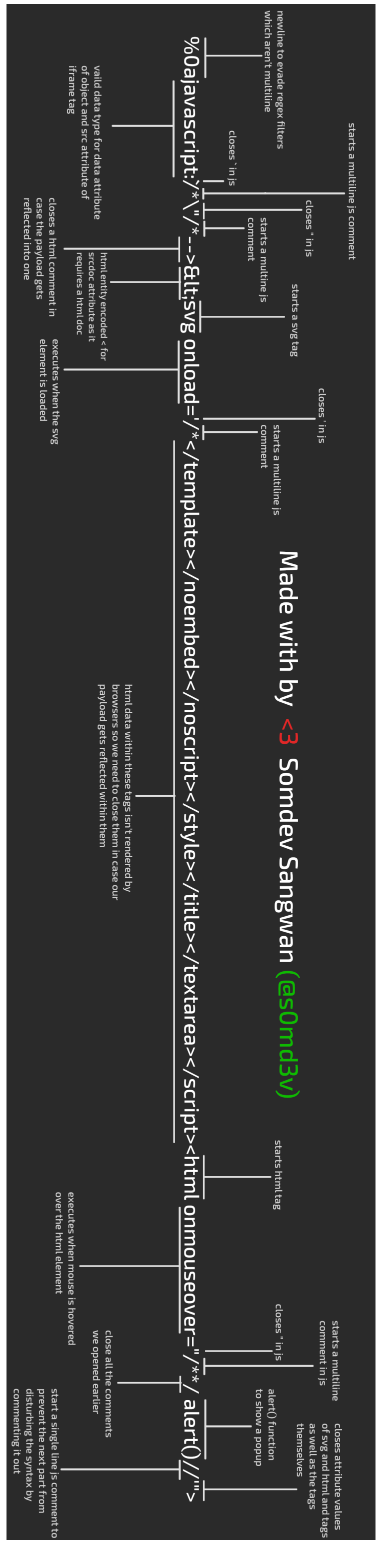


Figure 1: An amazing XSS polyglot payload