# Spring 2020
# CYB 404 – NETWORK SECURITY
# MIDTERM EXAM II
# COVERSHEET

| | |
|---|---|
| LAST NAME | Alamoudi |
| FIRST NAME | Abdulrahman |
| NAU EMAIL | aaa858@nau.edu |

Please only write your name and any other identifying information on this coversheet. This will allow me to grade your exam via a single-blind process.

I confirm that I have completed this exam using my own knowledge and have not committed any acts considered “academic dishonesty” according to the University’s Academic Dishonesty Policy.

Abdulrahman Alamoudi
Signature:

21/03/2021
Date:

Instructions: Provide your answer to each question in the box below the question. The provided space should be more than enough for a complete answer. **If you are printing this PDF and writing your answers with pen or pencil, be sure to write very darkly and legibly so the scanned version with your answers appears clearly in Gradescope.**

You must upload your completed exam to BbLearn in a PDF. Failure to do so will result in a zero grade on your exam. You must also ensure that the uploaded PDF has the same page numbers and formatting as the blank exam form you download. Failure to do so will result in half the points from your exam being removed.

Q0. [10 points] Describe what man-in-the-middle attacks could learn from the unencrypted HTTP message below:

```
GET /kurose_ross_sandbox/interactive/quotation6.htm HTTP/1.1
Host: gaia.cs.umass.edu
Accept: text/plain, text/html, text/xml, image/gif, image/png, audio/vnf.wave,
audio/basic, video/mp4, video/mpeg,
Accept-Language: en-us, en-gb;q=0.6, en;q=0.8, fr, fr-ch, da, fi
If-Modified-Since: Mon, 30 Nov 2020 13:52:24 -0800
User Agent: Mozilla/5.0 (Windows NT 5.1; rv:11.0) Gecko/20100101 Firefox/11.0
```

The main-in-the-middle attacks could learnt the following information from the unencrypted HTTP message shown above:

Name of the file that is being retrieved in the GET message which is quotation6.htm

Version of HTTP which the client is running: 1.1

Formats of text, images, audio and videos client browser prefer to recieve:

text : plain, html, xml
image : gif, png
audio: vnf.wave, basic
video : mp4, mpeg

Client's preferred version of English: Accept-Language: en-us, en-gb;q=0.6, en;q=0.8

The information that the client already have a copy of the requested file.

Type of the client's browser and operating system:

Browser : Mozilla Firefox 5.0
Operating System : Windows NT 5.1

Q1. [15 points] Describe how SSL/TLS uses both asymmetric and symmetric encryption. Which CIA + Authenticity + Accountability objectives do these processes contribute to and how?

SSL/TLS uses a combination of symmetric and asymmetric cryptography, as this provides a good compromise between performance and security when transmitting data securely.

With symmetric cryptography, data is encrypted and decrypted with a secret key known to both sender and recipient; typically 128 but preferably 256 bits in length. Symmetric cryptography is efficient in terms of computation, but having a common secret key means it needs to be shared in a secure manner.

Asymmetric cryptography uses key pairs – a public key, and a private key. The public key is mathematically related to the private key, but given sufficient key length, it is computationally impractical to derive the private key from the public key. This allows the public key of the recipient to be used by the sender to encrypt the data they wish to send to them, but that data can only be decrypted with the private key of the recipient.

It contributes to ensure the confidentiality, Integrity and Authenticity from the CIA + Authenticity + Accountability triad.

Q2. [5 points] Discuss some of the unique properties of wireless networks that make them uniquely vulnerable from a security perspective.

Because packets of data in wireless networks are sent through the air, they can be intercepted and modified quite easily by malicious users. This means that wireless networks are more vulnerable to attacks on the integrity of data.

Other properties include:

Lack of Physical Security Controls
Use of Untrusted Networks
Use of Applications created by unknow parties
Use of untrusted content
Use of location services
Interaction with other systems

Q3. [10 points] Diagram the TLS handshake, including the steps involved, how they are ordered, and the purpose for each of the steps.

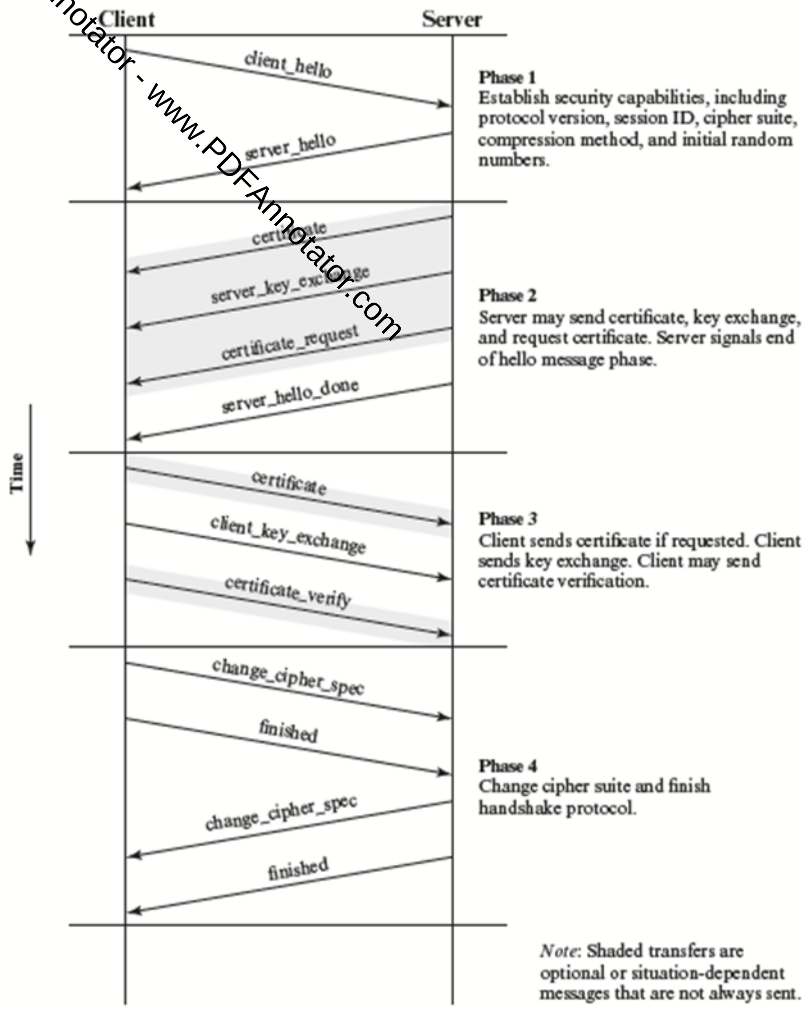
Client
Server
client_hello
server_hello
Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.
certificate
server_key_exchange
certificate_request
server_hello_done
Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.
Time
certificate
client_key_exchange
certificate_verify
Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.
change_cipher_spec
finished
change_cipher_spec
finished
Phase 4
Change cipher suite and finish handshake protocol.
Note: Shaded transfers are optional or situation-dependent messages that are not always sent.

Figure 6.6 Handshake Protocol Action

Q4. [10 points] In your own words, discuss why TLS is critical for securing application traffic and how the benefit of the modular TCP/IP layer design amplifies the usefulness of TLS.

TLS encryption can help protect web applications from data breaches and other attacks. It provides Encryption, Authentication, and Integrity.

For a website or application to use TLS, it must have a TLS certificate installed on its origin server. A TLS certificate is issued by a certificate authority to the person or business that owns a domain. The certificate contains important information about who owns the domain, along with the server's public key, both of which are important for validating the server's identity.

TLS) protocol adds a layer of security on top of the TCP/IP transport protocols.Because of TCP/IP's modular design layer, the TCP/IP protocol stack can adapt easily to specific hardware and operating environments. Breaking the networking software into specific, well designed components also makes it easier to write programs that interact with the protocol system.