Spring 2020 CYB 404 – NETWORK SECURITY MIDTERM EXAM II COVERSHEET

LAST NAME	MUSKU
FIRST NAME	KRUSHITH REDDY
NAU EMAIL	km3248@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.

__________KRUSHITH REDDY MUSKU__ ________________3/27/2022
Signature: 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 man-in-the middle attacks could learnt the following information from the unencrypted HTTP message shown above:

Name of the file that is being retrived 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 receive:

Text: plain,html, xml

Image: gif, png

Audio: vnf, wave, basic

Video: mp4.mpeg

Client's preferred version of english: Accepted-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?

TLS (Transport Layer Security) is a technique for encrypting network communications. It is also known as SSL. Both asymmetric and symmetric encryption algorithms are included in TLS. The client and server agree on new "session keys" during a TLS handshake, which are used for symmetric encryption. Each communication session starts with a new TLS handshake and session keys.

Data is encrypted and decrypted with symmetric cryptography using a secret key that is known by both the sender and the recipient; the key is normally 128 but preferably 256 bits long. Symmetric cryptography is fast in terms of computing, but it requires a secure way to share a common secret key.

Key pairs — a public key and a private key – are used in asymmetric cryptography. The public key is mathematically related to the private key, however deriving the private key from the public key is computationally prohibitive given sufficient key length. This allows the sender to encrypt data and deliver it to the recipient using the recipient's public key, but the data can only be decrypted using the recipient's private key

- **Authentication**
    - TLS verifies the identity of the communicating parties, which normally be clients and servers.
    - With the help of asymmetric cryptography, TLS makes sure that we will go to the authentic website, and not a fake one.
- **Confidentiality**
    - TLS protects the exchanged data from unauthorized access by encrypting it with symmetric encryption algorithms.
- **Integrity**
    - TLS recognizes any alteration of data during transmission by checking the message authentication code, which we will learn about in a moment.
- **Authenticity**
    - For server authentication, the client uses the server's public key to encrypt the data that is used to compute the secret key. The server can generate the secret key only if it can decrypt that data with the correct private key.
    - For client authentication, the server uses the public key in the client certificate to decrypt the data client sends. The exchange of finished messages that are encrypted with the secret key confirms that authentication is complete.
    - If any of the authentication steps fail, the handshake fails and the session terminates.
- **Accountability**
    - Accountability mechanisms deals with trust-related security incidents of certification authorities (CAs) in SSL/TLS public-key infrastructure.

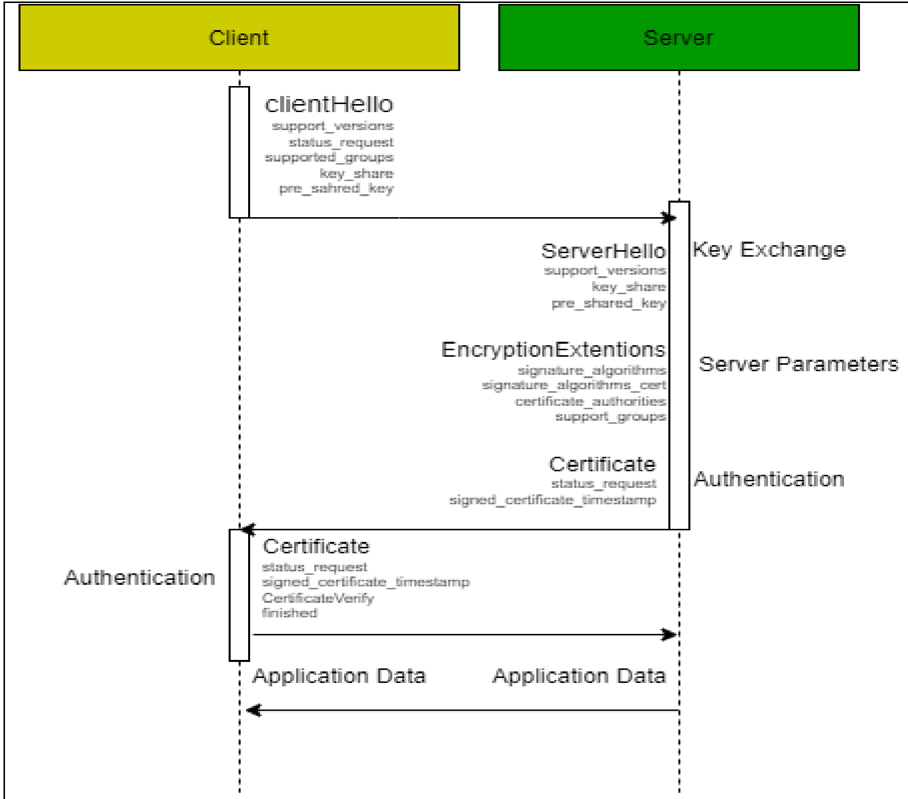
Q2. [5 points] Discuss some of the unique properties of wireless networks that make them uniquely vulnerable from a security perspective.

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.

Properties:

- Lack of physical security controls.
- Use of untrusted networks.
- Misconfigurations in network.
- Use of applications created by unknown parties.
- Use of location services.
- Browsing websites which doesn’t have HTTPS.

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



1) Key exchange:

   a) The client sends a ClientHello message to server.

   b) The server processes the ClientHello message and determines the appropriate cryptographic parameters for the connection. It then responds with its own ServerHello message, which indicates the negotiated connection parameters. For TLS 1.3, the ServerHello message determines the key and cipher options only. Other handshake parameters may be determined later.

2) Server parameters: The server sends two messages to establish server parameters:

   a) EncryptedExtensions: This message contains responses to ClientHello extensions that are not required to determine the cryptographic parameters, other than those that are specific to individual certificates.

   b) CertificateRequest: If certificate-based client authentication is desired, then the server sends this message, which contains the desired parameters for that certificate. This message is omitted if client authentication is not desired.

3) Authentication:

   a) The server sends these authentication messages:

      i) Certificate: This message contains the authentication certificate and any other supporting certificates in the certificate chain. This message is omitted if the server is not authenticating with a certificate.

      ii) CertificateVerify (optional): This message contains a signature over the entire handshake using the private key corresponding to the public key in the Certificate message. This message is omitted if the server is not authenticating with a certificate.

      iii) Finished: a MAC (Message Authentication Code) over the entire handshake.

   b) The client responds with its own Certificate, CertificateVerify, and Finished messages. The Certificate message is omitted if the server did not send a CertificateRequest message. The CertificateVerify message is omitted if the client is not authenticating with a certificate.

The client and server can now securely send application data to each other.

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

The secure sockets layer is added between the transport layer and the application layer in the standard TCP/IP protocol stack. TLS 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 int specific, well designed components also makes it easier to write programs that interact with the protocol system.