Introduction to Data and Cyber-Security (DCS3101) - Assignment 3

Q1 - Advantages of firewalls)

A firewall is a check point that protects the internal networks against attack from outside network and the check point decides which traffic can pass in & out based on different rules. And this is where its biggest advantage comes from, the ability to monitor the network traffic and prevent unauthorized access from entering the network by filtering the information that comes from the internet.

Out on internet, there is always going to be hackers and malicious traffic that may try to penetrate into a private network to cause harm, and the advantage of firewalls is that they are a main component on a network to prevent this by creating a safety barrier between a private network and the public internet. This is true especially when we are talking about large organizations with lots of computers, servers and other resources. In that case, you don't want those resources accessible to everyone on the internet and a firewall will help prevent this.

Furthermore, a firewall will make sure that communication within the networks such as messaging remain secure since it will use a distinct, secure port for the communication and by forcing the communication through this firewall where we check for evil packets and intruders. This port control contributes in increasing the security.

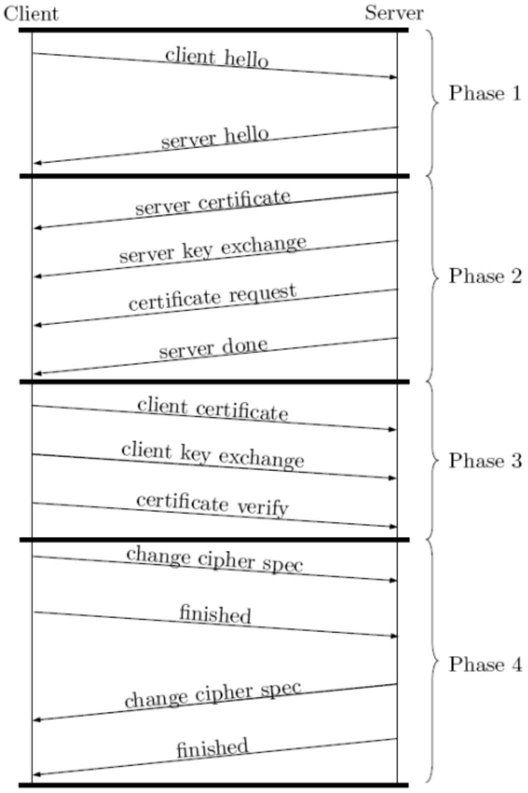
Q2 - TLS handshake)

The diagram shows the TLS handshake where the two communicating sides, the client and server exchange messages to acknowledge each other, verify each other, establish the encryption algorithms they will use, and agree on session keys.

The statement that "the algorithms used inside a session are negotiated between client and server" is true as we see from the diagram. The exact steps within a TLS handshake will vary depending upon the kind of key exchange algorithm, an example with the RSA key exchange during phase 1:

- The client initiates the handshake by sending a "hello" message to the server. This can include the clients TLS version, the cipher suites supported, and a string of random bytes known as the "client random."
- Following this, we see that the server sends a "hello" message. This can contain the server's SSL certificate, cipher suite and the "server random," another random string of bytes that's generated by the server.

We now see how the interactions can occur between server and client and the algorithms used. This is important to note since TLS handshakes are a foundational part of how HTTPS works.



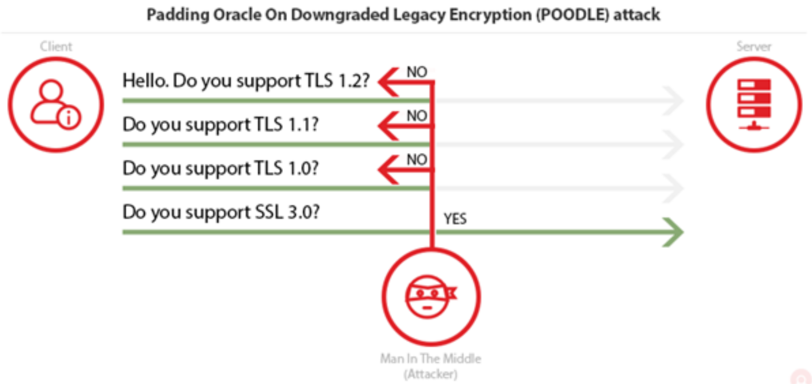
Q3 - Attacks on TLS)

The attack we discussed in the class was the heart bleed bug. Heartbleed is a security bug in the OpenSSL cryptography library, which is a widely used implementation of TLS. It was introduced into the software in 2012 and publicly disclosed in April 2014.

An important part of the TLS/SSL protocols is what's called a heartbeat option. Basically, it's how to computers communicating let each other know that they're still connected, and not idle for a long period of time. Using this heartbeat protocol, one computer can send some encrypted data to another computer called a heartbeat request. The receiving computer will answer back with the same encrypted data in order to confirm that the connection between them is still active, and it will also include information abouts its own length.

The fault lies in the fact that when a computer receives a heartbeat request it doesn't check to make sure that the request is actually as long as it is claimed to be. So, when someone tells it that a random message has 10 characters, the computer will automatically reply with 10 characters. If we have a request that is 100 kb, but in reality is only 50kb, the computer receiving the request would allocate the 100 kb of memory to a buffer, then store the 50 kb it actually received, then send back that 50 kb and whatever happened to be in the next 50 kb of memory. That extra 50 kb of data is information that the attacker has now extracted from the web server. We quickly see how this can become a big scaled problem, because we can exploit the computer to send us large amounts of information.

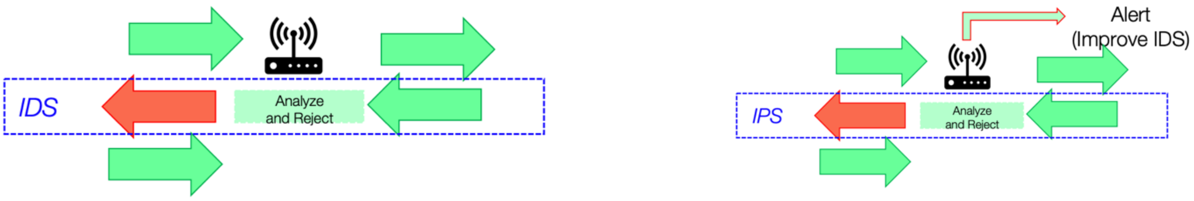
Furthermore, another attack on TLS is known as the “padding oracle on downgraded legacy encryption” (POODLE). “This attack was published in October 2014 and takes advantage of that some servers/clients still support SSL 3.0. The second factor is a vulnerability that exists in SSL 3.0, which is related to block padding”. The attacker takes advantage of that many browsers will revert to SSL 3.0 when a TLS connection is unavailable, and by exploiting the vulnerability in SSL3’s cipher block chaining, an attacker can use automated tools without knowing the encryption method or key and still be able to decipher the text. This MITM (man in the middle) attack will allow the attacker to eavesdrop on the communication between the client and the server.


Padding Oracle On Downgraded Legacy Encryption (POODLE) attack
Client
Server
Hello. Do you support TLS 1.2?
NO
Do you support TLS 1.1?
NO
Do you support TLS 1.0?
NO
Do you support SSL 3.0?
YES
Man In The Middle (Attacker)

Q4 - IDS and IPS)

Intrusion detection systems (IDS) is a system to monitor network traffic for suspicious activity. As with other fundamentals of security, IDS revolve around confidentiality, integrity, availability. While IDS only detect intrusions and alerts the administrator of the network about the activity, intrusion prevention systems (IPS) monitors, detect and alerts when such activity is discovered.

Both systems read network packets and compare the contents to a database of known threats, but the main difference between the two systems is what happens after this. As, mentioned IDS is a detection and monitoring tool and requires someone to analyze the findings and take action from there. IPS on the other hand will take action and try to prevent the attack by intercepting dangerous packets and drop them before they reach their target.



We have different types of IDS and methods of detection, such as:

- Host Intrusion Detection Systems (HIDS)
- Network Intrusion Detection System (NIDS)

Host-based collects data from sources internal to a computer, usually at the operating system level (various logs etc.). It monitors user activities and the executions of system programs.

On the other hand, the network-based intrusion detection system will collect network packets. By having sensors deployed at strategic locations, the system can inspect network traffic and monitor user activities on the network.

Moving on, the taxonomy of IDS and IPS can be divided into three different categories. All the categories detect dangerous traffic, but they do it in different ways. Rule-based is done by determining whether the traffic is dangerous or not. Knowledge-based does it by comparing the signatures of the traffic, and learning-based does it by using artificial intelligence.

Q5 - Biometrics)

In biometrics we use automated methods to recognize or verify the identity of a living person based on biological or behavioural characteristics. It is becoming an increasingly popular form of authentication and characteristics for biometric authentication include:

- Fingerprints
- Facial recognition
- Retina or Iris patterns
- Voice recognition
- DNA

All of these modalities have their advantages and disadvantages, some are more reliable, and others are more costefficient. In other words, when choosing a biometric modality, there are a lot of factors to consider. Some of the key factors when choosing a biometrics modality are:

- **Universality:** Each person should possess the biometric characteristic
- **Distinctiveness**: Different persons should have different biometric characteristics
- **Permanence:** The properties should be sufficiently invariant over a period of time
- **Performance:** Should be accurate
- **Cost:** How costefficient is it?
- **Acceptability:** To which extend are users willing to accept the use of it?

If we take an example of iris recognition, disguising as someone else using iris is very hard because an eyeball almost remains the same throughout one's lifetime. In addition to this the iris pattern are known to be very accurate. This modality is therefore good in performance, permanence and distinctiveness, but on the other side it is relatively expensive with modern technology.

Q6 - Attacks on biometrics)

Most modern facial biometric systems are vulnerable to simple attacks using spoofing techniques. "A spoofing attack is when a malicious party impersonates another device or user on a network in order to launch attacks against network hosts, steal data, spread malware or bypass access controls".

There are mainly two types of attacks used on the facial recognition system:

- Presentation attacks
- Indirect attacks

Presentation attacks are done at the sensor level and they exploit biometric vulnerabilities. This can be some sort of artificial fingerprint or a face photo where the attacker tries to disguise himself as the actual user to gain access to the system.
Indirect attack on the other hand can be performed at the database, the communication channels etc. In contrast to presentation attacks, indirect attack requires the attacker to have access to the inner system.

References:
https://usn.instructure.com/courses/22192/files/folder/Slides-Compact-Version
For Q1
https://www.researchgate.net/publication/324646511_A_Review_on_Firewall_Its_Advantages_and_Disadvantages
For Q2:
https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/
For Q3:
https://www.csoonline.com/article/3223203/what-is-the-heartbleed-bug-how-does-it-work-and-how-was-it-fixed.html
https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/
For Q4:
https://www.varonis.com/blog/ids-vs-ips/
For Q5:
https://www.m2sys.com/blog/biometric-hardware/5-factors-consider-choosing-best-biometric-modality/
For Q6:
https://towardsdatascience.com/facial-recognition-types-of-attacks-and-anti-spoofing-techniques-9d732080f91e
https://www.veracode.com/security/spoofing-attack