Trinity College Dublin

Coláiste na Tríonóide, Baile Átha Cliath

The University of Dublin

Security and Privacy

ER -4

Declaration: "I have read, and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year, found at http://www.tcd.ie/calendar. I have also completed the Online Tutorial on avoiding plagiarism 'Ready Steady Write,' located at http://tcdie.libguides.com/plagiarism/ready-steady-write."

Submitted By

Harsh Dhingra

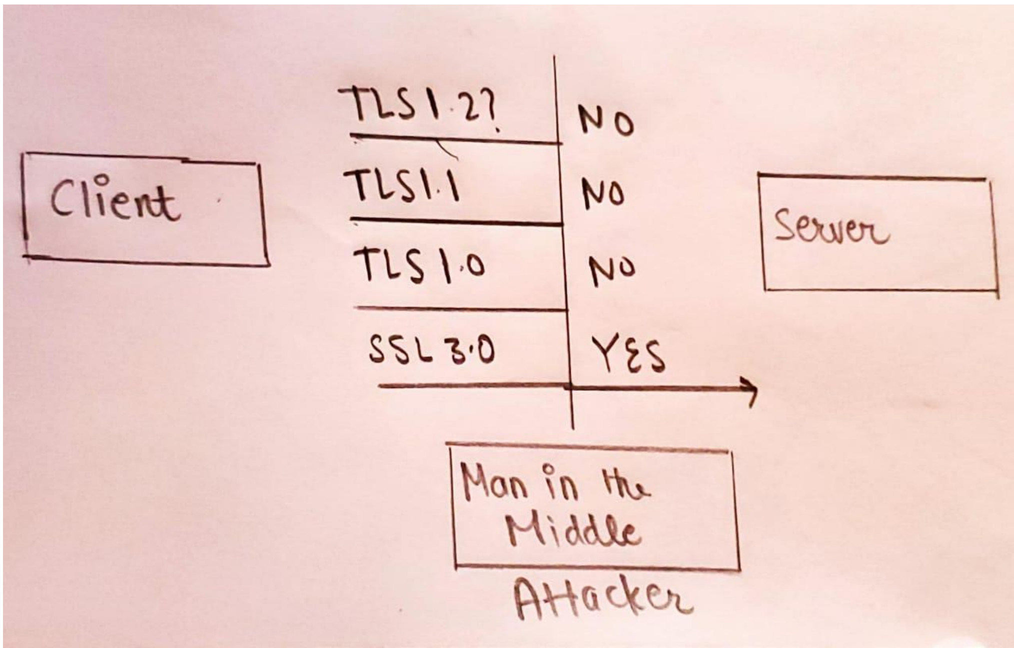
19323904

Q4 (a)

SSL (Secure Socket Layer) and TLS (Transport Layer Security) are cryptographic security protocols used to make a reliable connection. TSL is the successor of SSL and SSL is obsolete these days. The main aim of TLS is to provide data integrity and privacy in communication. Web browsers commonly use SSL and TLS to protect connections between web applications and web servers. Many vulnerabilities have been discovered over time. Some are 3SHAKE, POODLE, LOGJAM, FREAK, ROBOT, LUCKY13, BREACH, etc.

Three of the vulnerabilities are being briefly explained below

1) **POODLE attack**
   POODLE stands for Padding Oracle On Downgraded Legacy Encryption discovered on October 14, 2016, by the Google security team (Bodo Möller, Thai Duong, Krzysztof Kotowicz). This is a type of vulnerability in which the attacker (man in the middle) tries to downgrade the TLS connection to the version SSL v3. Then if the cipher suits, the attacker uses rc4 or block cipher in CBC (Cipher Block Chaining) mode, the attacker can retrieve partial bytes of the encrypted text and then get converted into the plaintext. In simple words, the attacker is trying to interrupt the communication and downgrade the TLS version on which the client and server will agree on. During the handshake, the attacker will try to reduce or downgrade the version of the protocol to retrieve the data in plaintext.



Understanding How does it happen, for this we need to understand TLS_FALLBACK_SCSV here SCSV stands for Signalling Cipher Suite Value it's a mechanism that ensure the downgrade of TLS/SSL version is valid and abort the connection when its not

The picture above depicts that it sends a list of SSL/TLS versions when the client initiates a handshake. An attacker comes in the middle (performing a MITM attack) and manipulates the server until the client agrees on the downgraded connection, i.e., SSL 3.0. It could be prevented if SSL3.0 is completely disabled on the server, and the browser should be upgraded to the latest versions.

2) **BREACH**
BREACH stands for Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext. It's a type of security exploit that targets HTTPS while using HTTP compression. It's similar to CRIME. HTTP web applications are the solution to the so-called bridge attack; as you may know, HTTPS is used to encrypt the web application traffic. This simply means that the traffic, even is if its intercepted by an attacker, can't be decrypted, and no secrets can be revealed. HTTPS is the primary defense against man-in-the-middle attacks. It is recommended for everyone who uses online banking or e-commerce on publicly available internet like airport or hotel hotspots, but just having HTTPS enable might not be as secure as we thought. BREACH takes place against HTTP compression; therefore, if the TLS compression is turned off it won't make any difference. To exploit the vulnerability: the server must use HTTP compression, user input should be reflected, and a secret(CSRF token) should be reflected in HTTP response bodies

3) **CRIME**
CRIME stands for Compression Ratio Info-leak Made Easy it's a type of security exploit that targets hidden web cookies over HTTPS (Hypertext Transfer Protocol Secure) and SPDY(deprecated open-specification communication protocol called speedy) protocols when data compression is used. It is a client-side attack. It allows an attacker to perform session hijacking. The CRIME attack will decrypt the HTTPS traffic, and its intended purpose is to steal cookies and hijack sessions. Preconditions of the attack are that the attacker must be able to sniff your network traffic, the victim must visit the malicious webpage controlled by the attacker, and third very important is that both the browser and the server support TLS compression or the SPDY protocols.
With the help of brute-force, CRIME decrypts HTTPS cookies which are set by websites to remember authenticated users; this will force the browser of the victim to send specially crafted HTTPS requests to the target website, which determine the value of the victim's session key (by analyzing the variation in length after being compressed). This is because TLS and SPDY use a compression algorithm called DEFLATE. CRIME works on the same principle and can decrypt the session cookie in few minutes.

Q4 (b)

Vulnerabilities can be separated into practical and academic use –

1) **Practical Vulnerability – Heartbleed**
Heartbleed bug is a critical security vulnerability in OpenSSL; it exploits a built-in feature of OpenSSL called heartbeat. OpenSSL is a popular cryptographic software library, it's an implementation of SSL/TLS protocol.
What is Heartbleed? – when a computer accesses a website, the website responds to the computer that it's active and is listening for requests. This is the heartbeat.this is a practical vulnerability and according to the web heartbleed bug has exposed anyone with a Yahoo, Amazon, Google, Facebook, and Pinterest account. Even the health care website healthcare.gov has urged its enrollees to change their passwords due to the heartbleed when the bug was discovered . Basically this attack tricks servers into

leaking the information stored in their memory. The heartbleed bug is very dangerous as it can expose login credentials such as username and password., credit card numbers, medical records, etc. In Heartbleed, if the client sends false data length, it responds with data received by the client and random data from its own memory to meet the length requirements specified by the user, therefore exposing its data[5]. This bug leaves no traces, so the victim has no idea about being hacked. Seeing the past examples and

2) **Academic Vulnerability – Raccoon attack**

Raccoon attack is a timing vulnerability attack, and it's recently discovered by a team of researchers – as an attack that affects HTTP and other services that utilize TLS. This attack affects TLS 1.2 and earlier versions.

The Raccoon attack allows the hacker to break an encrypted connection under very minute circumstances and timing measurement. This attack can be possible only and only if the server is configured for TLS 1.2 or below; connection uses a cipher suite that utilizes static Diffie-Hellman exchange keys; the attacker can observe individual connection to obtain the private key, and the attacker is close enough to the target server to get the timing right [1].

All these scenarios would be rarely met; therefore, it has no practical use and academic interest.

Q4 (c)

Web applications are on a boom from the past decade, and they will increase further even more exponentially. Web being a pool of information, is very susceptible to vulnerabilities. The web has a lot of evil influence, and I would suggest the following for the researchers/security scientist to work on:

They should work on Post-Quantum cryptography in TLS as the present asymmetric cryptography in TLS is vulnerable in :

- The server and client's key exchange algorithm
- Authentication – In this step, the server proves its identity using its public key.

Seeing the present flaws for the quantum world, I would suggest working on this; along with this, I would also put light on BlackBox testing

References

[1]https://www.ssls.com/blog/what-you-need-to-know-about-the-raccoon-attack-tls-vulnerability/

[2] https://www.acunetix.com/vulnerabilities/web/crime-ssl-tls-attack/

[3]https://www.jscape.com/blog/ssl-vs-tls-know-the-difference

[4] https://www.microsoft.com/en-us/research/project/post-quantum-tls/

[5] https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/