An overview of common TLS vulnerabilities

Pasi Niininen[1]

Abstract— **TLS (Transport Layer Security) is a cryptographic protocol that provides privacy and authenticity to client-server communications and is widely to secure HTTP connections as well as web services such as email. Flawed implementations can still result in vulnerabilities and in this paper some common issues are examined by reviewing scientific literature on the topic.**

I. INTRODUCTION

The TLS protocol provides authentication (the server is who they say they are), confidentiality (data is only visible at its endpoints), and integrity (data cannot be modified by attackers after it's sent without detection) [1].

Perhaps the most famous example of a TLS vulnerability is the Heartbleed bug, discovered in 2014, which was a flawed implementation of the protocol in the OpenSSL library, which allowed a malicious actor unauthorised access to data on the host machine.

In this paper some common vulnerabilities are examined for TLS 1.3 as well as its previous versions. This is not meant to be an exhaustive list but rather an overview of the topic.

II. TLS 1.3 VULNERABILITIES

Even tech giants like Microsoft and Apple are not impervious to TLS exploits, as shown by S. Lee et al. in 2020, who were able to perform a downgrade attack, which causes the host to use an older and more vulnerable version of TLS [2].

Broadly though, H. Lee t al. found that TLS 1.3 gained rapid adoption compared to its predecessor, TLS 1.2, especially among third party providers like Cloudflare, which has contributed to the overall safety of the Internet [3]. They also found that while a competent implementation of TLS 1.3 provides enhanced security, almost one in five providers have unstable implementations of the upgraded protocol which cause security concerns.

Actual vulnerabilities in TLS 1.3 seem to be rare. Most attacks appear to target lackluster protocol implementation to downgrade to a less secure version, but at least one TLS 1.3 vulnerability was identified in 2019 by Drucker & Gueron [4]. They propose a man in the middle attack which leverages Pre Shared Keys, an authentication method which does not use certificates. Their Selfie attack tricks the clients into believing they are communicating with a server when in reality their own messages (including the PSK, which the client assumes only they and the server know) are echoed back to them. The usefulness of this attack seems dubious, but it does violate the property stated in RFC 8446, appendix E, which states that "The client's view of the peer identity should reflect the server's identity".

III. VULNERABILITIES IN EARLIER VERSIONS OF TLS

Since downgrade attacks are possible and not all hosts even use TLS 1.3, it is worthwhile to mention known attacks against TLS 1.2 and earlier. Satapathy & Livingston have collated such a list, which shall be summarised here [5].

- BEAST: a brute force technique to guess the secret key which is used to encrypt plaintext. Affects TLS 1.0, fixed in later versions.
- CRIME: a brute force technique to guess the secret key, made possible by weakening encryption in favor of compressing headers. Affects TLS 1.0, fixed in later versions.
- Time: this attack is performed without eavesdropping to network traffic and instead utilises session cookie response time and size to guess the content. Mitigated with different encryption methods.
- BREACH: circumvents TLS by targeting HTTP compression instead. Mitigated by disabling HTTP compression.
- LUCKY 13: a technique which utilises a time difference server responses depending on whether or the padding in the cipher message is true or not. Possible mitigation methods include random time delays to responses.
- RC4 BIASES: a weakness in the RC4 cipher makes brute force decryption possible. TLS 1.3 prohibits the use of RC4 cipher suites.
- SSL Renogiation: a technique which utilises blocked and captured packets from the client to be sent after the attacker's own request. TLS 1.3 prohibits renegotiation.
- POODLE: a man in the middle attack which relies on a downgrade to TLS 1.0.
- FREAK: a man in the middle attack which relies on downgrading ciphers. Mitigated by removing support for insecure ciphers.
- Bar Mitzvah: another attack against RC4 cipher. TLS 1.3 prohibits the use of RC4 cipher suites.
- TLS Truncation: abnormal termination of a connection which causes the client to believe it has logged out when in reality the connection is kept alive. RFC 8446 specifies connection closure alerts to mitigate against a Truncation attack [1].

IV. CONCLUSIONS

Overall, TLS 1.3 seems to be significantly more secure than previous versions, with most vulnerabilities stemming from unstable implementation or misconfiguration and even in earlier versions of the protocol, many threats can be mitigated by using modern ciphers and disabling some features that can be exploited for an attack.

References

[1] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, August 2018.

[2] S. Lee et al., Return of Version Downgrade Attack in the Era of TLS 1.3., CoNEXT '20: Proceedings of the 16th International Conference on emerging Networking EXperiments and Technologies, November 2020, pp 157–168.

[3] H. Lee et al., TLS 1.3 in Practice:How TLS 1.3 Contributes to the Internet, WWW '21: Proceedings of the Web Conference 2021, April 2021, pp. 70–79.

[4] N. Drucker & S. Gueron, Selfie: reflections on TLS 1.3 with PSK, Journal of Cryptology 34, May 2021, Article number: 27.

[5] A. Satapathy & J. Livingston, A Comprehensive Survey on SSL/ TLS and their Vulnerabilities, International Journal of Computer Applications Volume 153, November 2016, pp 31-38.