Can you trust your work computer?

Amon Harris
Computer Science
North Carolina Central University
aharr187@eagles.nccu.edu

Orlando Arias
Department of ECE
University of Central Florida
oarias@knights.ucf.edu

Dr. Yier Jin
Department of ECE
University of Florida
yier.jin@ece.ufl.edu

Dr. Shaojie Zhang
Department of Computer Science
University of Central Florida
shzhang@cs.ucf.edu

Abstract

Modern secure communication is done using Transport Layer Security (TLS). As an upgrade to Secure Sockets Layer (SSL), TLS provides a secure channel over an entrusted network between two different endpoints. Although TLS provides a secure channel against eavesdroppers, it does not guarantee the security of endpoints. In this work, we demonstrate how a minor modification in a client can be used to transparently expose potentially confidential information that is being transmitted over a secure channel. By installing a new root certificate on the client, we can decapsulate all transmitted data from a remote proxy. We demonstrate the privacy and security implications of this attack in large enterprises, where a network administrator or an IT department can deploy this system to eavesdrop on employee communication . We also discuss applications of this system such as legitimate traffic monitoring for security research such as in IoT devices.

Background

Secure Sockets Layer (SSL):

- Security protocol that establishes encrypted links between a web server and browser during online communication
- Ensures data transmitted between web server and browser remains encrypted

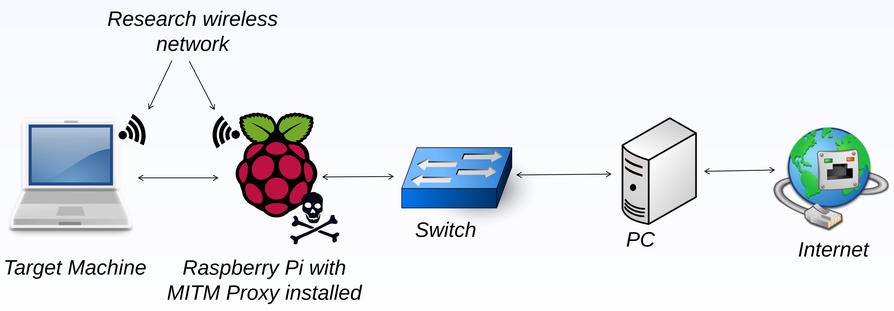
Transport Layer Security (TLS):

- Improved version of SSL
- Provides secure communications over the internet for things such as email, faxing, etc.
- Has two layers: TLS handshake and TLS record protocols
- TLS Handshake: Responsible for authentication and key exchanges that are necessary to establish secure sessions
- TLS Record: Secures application data using the keys created during the handshake protocol

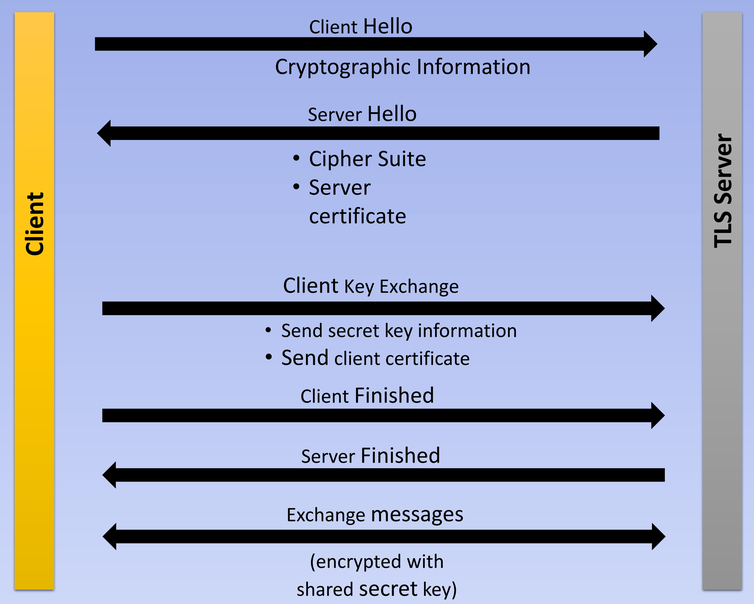
Man-In-The-Middle Proxy (MITM Proxy):

- HTTPS proxy used for privacy measurements and penetration testing
- Intercepts and modifies web traffic, including SSL/TLS-protected protocols

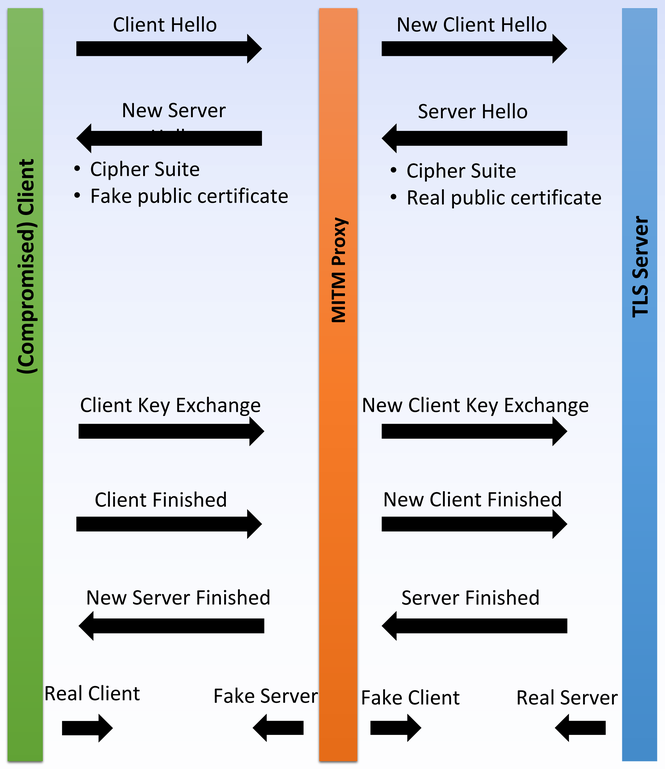
Setup



Application



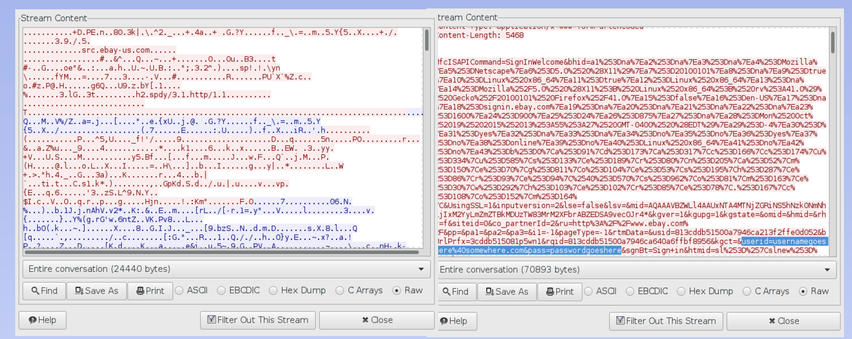
Normal SSL/TLS handshake



SSL/TLS Handshake with MITM Proxy involved. Fake server/client is invisible to both parties.

Results

Using MITM on the Raspberry Pi, we were able to decrypt traffic from a compromised client. We show a demonstration below.



On the left, we have encrypted network traffic captured through Wireshark. The decrypted traffic is on the right showing login credentials for eBay.

This same technique can be employed to study the behavior of IoT devices by monitoring their communication to ensure there is no data leakage and capture firmware updates for further security analysis.

While there is no solution to guarantee 100% protection from a Man-In-The-Middle attack, there are a few preventative measures that can be taken. These measures include certificate pinning, utilizing an encrypted tunnel and local device security. Local device security can be as simple as not leaving passwords around for other individuals to access

References

mitmproxy is a free and open source interactive HTTPS proxy. mitmproxy - an interactive HTTPS proxy Available at: https://mitmproxy.org/. (Accessed: 3rd July 2018)

The Transport Layer Security (TLS) Protocol Version 1.2. IETF Available at: https://www.ietf.org/rfc/rfc5246.txt. (Accessed: 1st July 2018)

Acknowledgements

The support for this work was provided by the National Science Foundation REU program under Award No. 1560302. Any opinions, findings, and conclusions and recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation