Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Introductory talk for the Master 's Thesis

Detection and Characterization of TLS interception in ISP networks

Name:	Johannes **Schleger**
Advisor:	Jonas Jelten
Supervisor:	Prof. Dr.-Ing. Georg Carle
Begin:	03/2018
End:	09/2018

Topic

This Master's Thesis shall implement the detection and characterization of TLS interceptions in ISP networks.

We aim to detect different interception behaviour of deployed middleboxes. Simple middleboxes intercept the traffic and use their own settings to establish the second TLS connection. The behaviour of more sophisticated devices aims to be transparent, meaning that the TLS handshake has as few changes as possible. One common used proxy that offers such transparent behaviour is Squid [1]. The TLS Client Hello contains information such as the TLS version, a random, the session-id, ciphersuites, compression method and extensions [2]. Those are used to determine a characterization of the middlebox.

Approach

Related work has shown that TLS connections are intercepted. However, related work focuses only on one side of the connection (server or client). Using a single viewpoint there is no clear identifier for an intercepted connection, which is why different approaches are used. A server-side approach is to use a heuristic for the detection (e.g. mismatch between HTTP User Agent and TLS handshake fingerprint [3]). A client-side approach is generally browser-based and relies on applets such as Flash or Java [4], the transmission of the results relies on a possibly compromised connection.

Our approach eliminates those deficiencies by being in control of both client and server (see Figure 1). This approach ensures that we can capture each byte transmitted and therefore get a full picture of the possible interception. This information ensures to provide a detailed characterization of the middlebox.

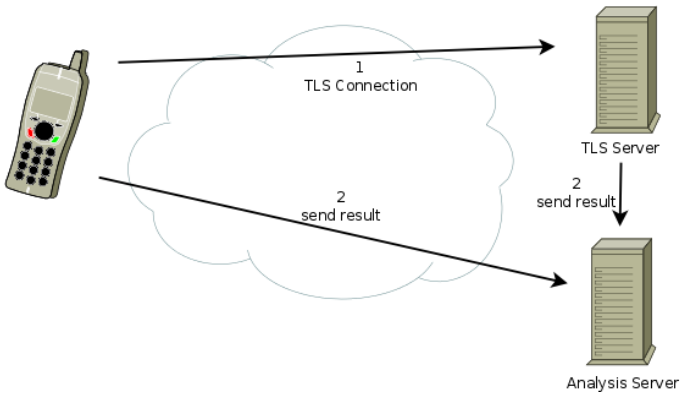

Figure 1: Main test scenario

For data collection this study relies on a broad range of vantage points located in different networks. Therefore, we rely on crowd-sourced measurements. An android application will be created and made publicly available. Interested users can download the app and help gather data. This crowd-sourced measurement offers different viewpoints and supports the traceability where and how TLS connections are intercepted. To get data regularly and from as many viewpoints as possible, the application has the option to automatically scan again when the client connects to a new network.

After the completion of the application the crowd-measurements can begin. Therefore the application will be made available to the public (or at least selected users such as chair members). Because we cannot be sure to find intercepted connections, in the meantime the detection is evaluated on basis of custom deployed interception software using e. g. Squid and mitmproxy.

Previous work

This project was initiated as part of an IDP [5]. In this IDP I implemented a proof of concept, which consisted of the three components TLS Client, TLS Server and TLS Analysis Server (as shown in Figure 1). This thesis aims at the completion of those components, such that they can be provided to the public.

Milestones

1. Definition of detection scenarios
2. Implementation of TLS Client, TLS Server, TLS Analysis Server
3. Rollout of demo application to selected users (e. g. chair members)
4. Evaluation
    - data collected by crowd-measurements
    - custom deployed interception (e. g. Squid, mitmproxy)

References

[1] D. Wessels *et al.*, “Squid: Optimising web delivery,” http://www.squid-cache.org/, last seen on 2018-02-15.

[2] T. Dierks and E. Rescorla, “The Transport Layer Security (TLS) Protocol Version 1.2,” Internet Requests for Comments, RFC Editor, RFC 5246, August 2008, http://www.rfc-editor.org/rfc/rfc5246.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5246.txt

[3] Z. Durumeric *et al.*, “The security impact of https interception,” *NDSS*, 2017. [Online]. Available: https://jhalderm.com/pub/papers/interception-ndss17.pdf

[4] L. S. Huang, A. Rice, E. Ellingsen, and C. Jackson, “Analyzing forged ssl certificates in the wild,” in *Proceedings of the 2014 IEEE Symposium on Security and Privacy*, ser. SP ’14. Washington, DC, USA: IEEE Computer Society, 2014, pp. 83–97. [Online]. Available: http://dx.doi.org/10.1109/SP.2014.13

[5] J. Schleger, “Detecting TLS interception in ISP networks,” Jul. 2017, Interdisciplinary Project in Electrical Engineering.