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

Introductory talk for the IDP 's Thesis

Detecting TLS interception in ISP networks

Name:	Johannes **Schleger**
Advisor:	Florian Wohlfart
Supervisor:	Prof. Dr.-Ing. Georg Carle
Begin:	03/2017
End:	08/2017

Topic

Recent papers [1], [2], [3] revealed that TLS connections are intercepted using proxies or so called middleboxes, e.g. corporate content filters. The objective of this interdisciplinary project is to find TLS proxies.

While related work focused on the presence of TLS interception, we also aim to characterize TLS proxies and their triggers in case of selective interception (e.g. domain name, destination IP, client fingerprints). Therefore, we want to deeply inspect the deployment and configuration of the proxies.

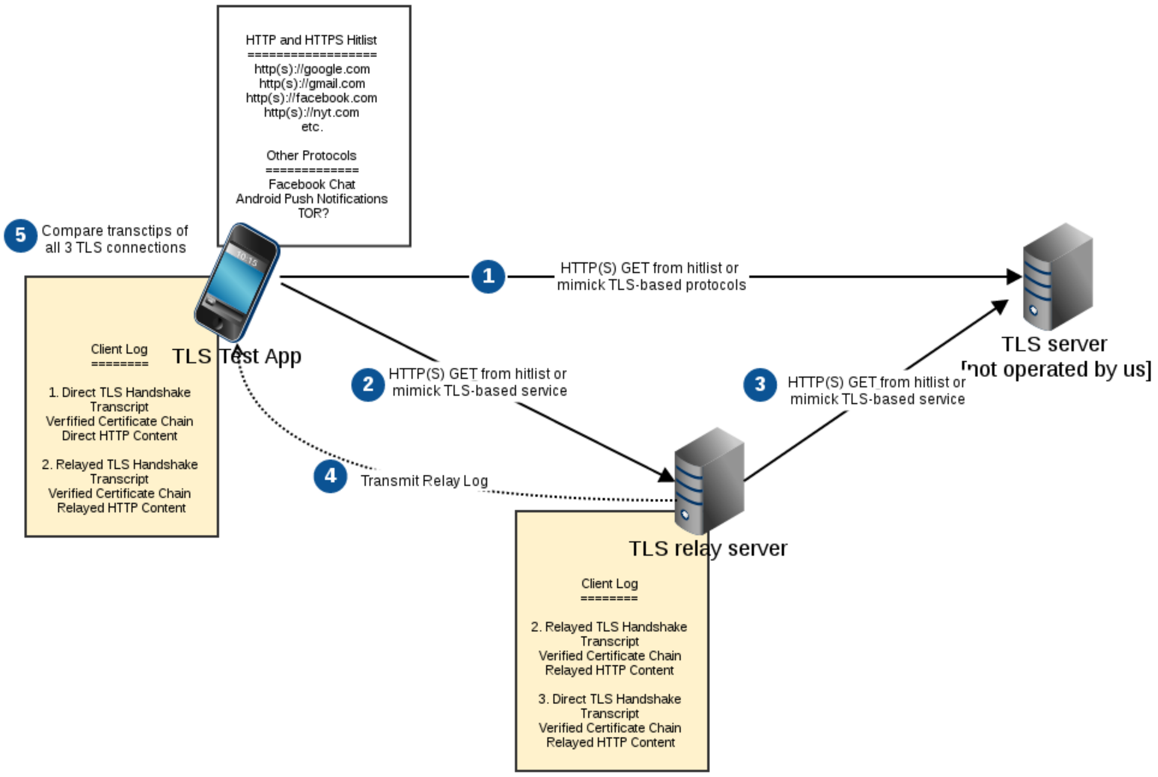
HTTP and HTTPS Hitlist
=================
http(s)://google.com
http(s)://gmail.com
http(s)://facebook.com
http(s)://nyt.com
etc.
Other Protocols
=============
Facebook Chat
Android Push Notifications
TOR?
5 Compare transctips of all 3 TLS connections
TLS Test App
Client Log
========
1. Direct TLS Handshake Transcript Verfified Certificate Chain Direct HTTP Content
2. Relayed TLS Handshake Transcript Verified Certificate Chain Relayed HTTP Content
1 HTTP(S) GET from hitlist or mimick TLS-based protocols
2 HTTP(S) GET from hitlist or mimick TLS-based service
3 HTTP(S) GET from hitlist or mimick TLS-based service
4 Transmit Relay Log
TLS server
[not operated by us]
TLS relay server
Client Log
========
2. Relayed TLS Handshake Transcript Verified Certificate Chain Relayed HTTP Content
3. Direct TLS Handshake Transcript Verified Certificate Chain Relayed HTTP Content

Figure 1: Architecture overview, source: Florian Wohlfart

Approach

The approach is to test multiple scenarios:

- Direct connection from client to a webserver (#1 in figure 1)
- Relayed connection via a relay server to a webserver (#2 and #3 in figure 1)
- Direct connection to our measurement server

For intercepted connections will be as much information about the proxy obtained as possible. This includes its address, allowed TLS versions and algorithms, the supported TLS extensions and support for SNI. Eventually all gathered information will be combined.

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 why 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.

Previous work

There exists an Android application created by Florian Wohlfart, which is considered a proof of concept. This application shows the feasibility to capture the raw socket data while doing the TLS handshake on top. The application will be used and extended such that the objectives stated above will be met.

As a reference for the implementation the ICSI Netalyzr Android application can be used. This application detects anomalies in the network connection and uploads the result to their server. The results then can be found by the user via internet.

References

[1] X. De Carnavalet *et al.*, “Killed by proxy: Analyzing client-end tls interception software,” *NDSS*, 2016. [Online]. Available: https://users.encs.concordia.ca/~mmannan/publications/ssl-interception-ndss2016.pdf

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

[3] 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