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

Thesis M.Sc.

IDP, Guided Research

Analysis of Servers use of TLS Parameters

Motivation

Measuring for TLS parameters as well as analysing malicious webservers with TLS fingerprints is actively researched [1,2,3]. Currently passive approaches are used in order to find malicious or unwanted connections by analysing network traces. These approaches observe the TLS handshakes in the network and try to correlate specific parameter sets to OS versions and software.
In this thesis we want to actively scan TLS servers and observe their use of TLS cipher suits and extensions. Actively scannig the servers allows us to collect more information during the handshake process than by just using passive methods, e.g. to collect the server certificate in TLS 1.3.
The basic assumption is that similar type of servers (e.g. webserver and mail server) use similar parameter sets in the TLS handshake. According to Anderson et al. [2] also benign and malicious servers can be differentiated by such an analysis.

Your Task

- Create a pipeline from a list of IP addresses to evaluated TLS parameters
  - The list of IPs can be scanned with tools like zgrab2 [4]
  - Extend the scanner in order to support all necessary features
  - Create evaluation tools to extract and analyse the TLS parameters
- Create an evaluation of retrieved parameters
- Compare two different input lists of IPs
  - Based on the parameter evaluation find the most significant differences between two input lists
- Analyze different input lists and evaluate your results

Sources

- [1] Anderson et al., TLS Beyond the Browser: Combining End Host and Network Data to Understand Application Behavior, IMC' 19
- [2] Anderson et al., Deciphering malware's use of TLS (without decryption, Journal of Computer Virology and Hacking Techniques 2018
- [3] Kotzias et al., Coming of Age: A Longitudinal Study of TLS Deployment, IMC' 18
- [4] Zgrab 2.0, https://github.com/zmap/zgrab2

Contact

Patrick Sattler sattler@net.in.tum.de
Lars Wüstrich wuestrich@net.in.tum.de
Max Helm helm@net.in.tum.de

http://go.tum.de/003923