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

Thesis B.Sc.

Thesis M.Sc.

IDP

Network Flow Based Application Profiling and Detection

Motivation

Devices often run multiple programs that interact with hosts somewhere else in the network. When monitoring traffic at network interfaces administrators can only see a mixture of frames being sent without being capable of knowing which program caused a packet.
To overcome this issue, we developed a Python-based tool that matches incoming and outgoing frames to PIDs. This enables the creation of application profiles that characterize the ”normal” behavior of applications. These profiles can then be used to detect anomalous behavior or remotely identify applications on a host, enhancing the capabilities of administrators.

Topic

In this thesis, a new approach for profiling applications based on PID-network-flow mappings should be developed and implemented. Therefore, in the beginning, different methodologies for application profiling need to be analyzed and evaluated. Based on this analysis, characterizing properties of applications are to be identified and accumulated into a host/application profile. This profile should then be used to remotely detect applications on a host or detect anomalies in the behavior of a known application.

Your Task

- Analysis of interaction between the application and the network layer in Linux
- Analysis and evaluation of current application profiling techniques
- Implementation of an application profiling service based on PID-network-flow mappings
- Evaluation of the proposed approach to remotely detect applications running on a host OR detect anomalies in the behavior of applications running on a host

Requirements

- Basic network knowledge
- Ability to write maintainable code

Sources

- [1] Haas, Steffen, Robin Sommer, and Mathias Fischer. ”zeek-osquery: Host-Network Correlation for Advanced Monitoring and Intrusion Detection.” arXiv preprint arXiv:2002.04547 (2020).
- [2] Fink, Glenn A., Paul Muessig, and Chris North. ”Visual correlation of host processes and network traffic.” IEEE Workshop on Visualization for Computer Security, 2005.(VizSEC 05).. IEEE, 2005.

Contact

Lars Wüstrich wuestrich@net.in.tum.de
Sebastian Gallenmüller gallenmu@net.in.tum.de

http://go.tum.de/080755