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

Thesis B.Sc. Thesis M.Sc. IDP

Mapping Network Flows to Applications for Profile Creation

Motivation

Devices often run multiple programs that interact with hosts somewhere else in the network. In the network itself, only the network traces are visible. On the hosts which run the applications it is possible to map network flows to single processes which can help to find anomalous behavior and enhance IDS [1][2]. This information can also be beneficial to create profiles of applications running on a device.

Topic

In this thesis, networks flows observed at an interface should be mapped to applications running on a device. This mapping should then be used to create profiles of the running applications. In the beginning different methods for profiling applications should be explored. Then a module should be created which is capable of matching incoming and outgoing packets to processes. In the best case, this mapping is then used to create profiles of the applications running on a host.

Your Task

- Identification of characteristics to profile applications
- Analysis of interaction between application and the network layer in Linux
- Creation of a mapping between PID and network flows
- Creation of application profiles based on the previously created mapping.

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