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

Thesis B.Sc. Thesis M.Sc. IDP

Mapping Network Flows to Local Processes Efficiently

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 knowing which program caused a packet. Such capabilities can help to find anomalous behaviors of processes, enhance IDS [1][2], or enable the creation of profiles that characterize applications. To overcome this issue, we developed a tool in Python that can match incoming and outgoing frames to PIDs. Due to Pythons implementation of multi-threading, our prototype has limitations with regards to its performance concerning network cards sending out lots of traffic.

Topic

In this thesis, the existing prototype for mapping network flows to PIDs should be reimplemented/refactored. The implementation should address the current limitation and enable the matching of frequently used network cards. Therefore, the current prototype needs to be analyzed and evaluated. Based on the analysis, the prototype should be reimplemented or refactored, depending on the chosen language. Further, to increase the accuracy of the prototype's matching, new methods for mapping network flows to PIDs should be explored and implemented. Finally, your implementation should be compared to the already existing implementation concerning their performance.

Your Task

- Analysis of interaction between the application and the network layer in Linux
- Analysis and evaluation of the current prototype
- Implementation of a high-performance application to map network flows to PIDs
- Development and implementation of new matching approaches to increase mapping accuracy
- Comparison of the existing and newly developed prototype

Requirements

- Basic network knowledge
- Ability to write maintainable and resource efficient 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