Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

In-network Anomaly Detection with Programmable Switches

Semester thesis proposal

Recent advances in network programmability enable both the control plane [5] and the data plane [4] to be reprogrammed on the fly. Among many advantages in manageability and policy management, this allows to provide certain services through the network devices (i.e. the switches) themselves instead of using distinct middleboxes.

The goal of this thesis is to develop an anomaly detection system that operates directly on the data plane of a network. For this, the network should monitor ongoing activities, distinguish between normal and suspicious activities and raise an alert if there is indication of malicious activity.

Bootstrapping questions

- How can we distinguish between normal and suspicious traffic? (e.g. with help of metadata such as source and destination, protocol, timing, size, ...)
- What kind of analysis can be performed in the dataplane (i.e. in P4-switches [3])?
- Implement the system in P4 [2] and evaluate it in a virtual environment [1] based on real network traces.

Contact

- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch
- Roland Meier, meierrol@ethz.ch

References

[1] Mininet. http://mininet.org/.

[2] P4 github repository. `https://github.com/p4lang`.

[3] P4 specification is p4_14. `http://p4.org/wp-content/uploads/2016/11/p4-spec-latest.pdf`.

[4] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker. P4: Programming protocol-independent packet processors. *SIGCOMM Comput. Commun. Rev.*, 44(3):87–95, July 2014.

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: Enabling innovation in campus networks. *SIGCOMM Comput. Commun. Rev.*, 38(2):69–74, Mar. 2008.