Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

Securing data-plane driven fast-reroute systems

Semester thesis proposal

Programmable switches have recently emerged and give researchers and operators a new way to operate, monitor and optimize their network [1]. Our group has designed a fast reroute system relying on these programmable switches which is capable of quickly rerouting traffic upon arbitrary Internet failures. Our system detects failures and recovers connectivity entirely in the data-plane. To do so, it relies on data-plane signals such as TCP retransmissions instead of the slow control-plane notifications (*e.g.*, BGP, which can take minutes to converge [2, 3]).

Unfortunately, as our system relies on data traffic, it is also vulnerable to malicious traffic manipulation. The main threat is that malicious users could manipulate our system by sending fake retransmissions for flows towards a victim destination. If multiple malicious flows start sending retransmissions at the same time, our system could consider this as a failure and as a result reroute the traffic towards the victim destination to another, less-preferred and possibly malicious, path. Such kind of attacks would not just be a threat for our system, but more generally for all data-plane driven systems.

Our system includes mechanisms to mitigate security risks. For example, our system reroutes traffic for a destination prefix if several flows experience retransmissions, and not just one. This would require an attacker to generate many flows in order to trick our system – a condition under which the attack would be quite visible, could be monitored and potentially mitigated at runtime. In addition, a flow is monitored by our system only during a short period of time, which gives to the attacker only a small amount of time to run the attack.

The first goal of this thesis is study the effectiveness of our current mechanisms used to mitigate security risks. For example, we would like to answer the following question: given a prefix and a number of flows destined to this prefix, how many malicious flows must be generated in order to trick our system for this prefix. The second goal is to propose additional mechanisms to protect our system against attacks. The proposed solutions should work for our system but we also envision to design more general mechanisms that would protect various types of data-plane driven systems.

Milestones

- Understand the related works, with a particular focus on our data-plane driven fast reroute system;
- Build a virtual network and show how our system can be attacked using simulations;
- Evaluate the effectiveness of the current mechanisms used to mitigate security risks;
- Improve the current mechanisms or propose new mechanisms to make data-plane driven systems more protected against attacks.

Prerequisites

- Being able to program in Python, some knowledge in P4 is a plus;
- Communication Networks (227-0120-00L), or equivalent.

Contact

- Thomas Holterbach, thomahol@ethz.ch
- Prof. Dr. Laurent Vanbever, lvanbever@ethz.ch

References

[1] 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.

[2] T. Holterbach, S. Vissicchio, A. Dainotti, and L. Vanbever. SWIFT: Predictive Fast Reroute. In *Proceedings of the Conference of the ACM Special Interest Group on Data Communication*, pages 460–473. ACM, 2017.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian. Delayed internet routing convergence. *ACM SIGCOMM CCR*, 2000.