ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Prof. Laurent Vanbever
Networked Systems Group

# Implementing the RPKI infrastructure in a virtual mini-Internet

Semester thesis proposal

The routing project [9] is one of the key project in our communication networks lecture [2]. For this project, we build a virtual mini-Internet infrastructure composed of hundreds of routers and dozens of Autonomous Systems (ASes), and let the students configure their virtual devices and operate their AS. The students have to configure various routing protocols to enable Internet-wide connectivity. In particular, students have to use BGP to enable connectivity between the different ASes.

BGP is the de-facto inter-domain routing protocol, but was designed without considering security: an AS can advertise any IP prefix even if it does not own it/has not the rights to do so. These events are known as BGP hijacks. They either arise due to misconfigurations or as a result of malicious operations. A well-known example is the "Youtube incident" in 2008 where Pakistan Telecom started to advertise one of Youtube's prefixes, redirecting a lot of Youtube's traffic to the Pakistan Telecom network [6] (which collapsed under the additional load). Such BGP hijacks occur every day in the Internet [1], and regularly lead to traffic and revenue losses.

The Resource Public Key Infrastructure (RPKI) aims at (partially) solving these problems. RPKI started to be developed starting in 2008, with deployment beginning in 2011 [7]. Since then, it has been more and more deployed within the Internet [8, 10]. The networking community is actively training network operators on how to deploy RPKI Route Origin Validation within their network. All the software required is publicly available [4], and there are many tutorials and blogposts about it ( [3, 5]). Yet, there is still a large number of networks that have not deployed RPKI with Route Origin Validation, or have not properly configured it [8].

In this thesis, the goal is to implement the RPKI infrastructure within the mini-Internet we use at ETH Zurich for our Communication Networks course, to enable students to perform Route Origin Validation. We believe that learning about the RPKI infrastructure in a mini-Internet mimicking the real one is efficient: the effects of a misconfiguration will propagate network wide and the consequences will be directly visible, e.g. loss of connectivity or complaints from other users.

The student is expected to study how to implement the RPKI infrastructure within the mini-Internet, and uses state-of-the-art tools to do it. The implementation must be lightweight and should fit well in the current implementation of the mini-Internet. In addition, it must be possible to to do Route Origin Validation for IPv4 and IPv6 prefixes. The student is also expected develop a web-based visualization interface that can display the deployment status. Finally, the student is expected to evaluate the load added by the RPKI infrastructure and the Route Origin Validations on the server running the mini-Internet.

### Milestones

- Get familiar with the routing project and its implementation and understand the RPKI infrastructure, its different components and the tools required to use it;
- Implement the RPKI infrastructure in the mini-Internet such that students can create Route Origin Authorizations and routers can perform Route Origin Validations for IPv4 and IPv6 prefixes;
- Develop a web-based visualization interface that can display the deployment status;
- Measure the load added by the RPKI infrastructure and the Route Origin Validations on the server running the mini-Internet.

### Prerequisites

- Being able to program in Bash and Python, good knowledge in UNIX-like systems;
- Basic knowledge in cryptography and/or network security;
- Communication Networks (227-0120-00L).

### Contact

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

### References

[1] Bgpstream. https://www.rfc-editor.org/rfc/rfc7115.txt.

[2] Eth zurich, communication networks course, 2020. https://comm-net.ethz.ch/.

[3] How to: Creating rpki roas in myapnic. https://blog.apnic.net/2019/09/11/how-to-creating-rpki-roas-in-myapnic/.

[4] Resource public key infrastructure (rpki). https://www.ripe.net/manage-ips-and-asns/resource-management/certification.

[5] Secure routing. https://www.securerouting.net/.

[6] Youtube hijacking: A ripe ncc ris case study. https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

[7] R. Bush. Origin Validation Operation Based on the Resource Public Key Infrastructure (RPKI). RFC 7115, Jan. 2014.

[8] T. Chung, E. Aben, T. Bruijnzeels, B. Chandrasekaran, D. Choffnes, D. Levin, B. M. Maggs, A. Mislove, R. v. Rijswijk-Deij, J. Rula, and N. Sullivan. Rpki is coming of age: A longitudinal study of rpki deployment and invalid route origins. In *Proceedings of the Internet Measurement Conference*, IMC '19, page 406–419, New York, NY, USA, 2019. Association for Computing Machinery.

[9] T. Holterbach, T. Bühler, T. Rellstab, and L. Vanbever. An open platform to teach how the internet practically works. *ArXiv*, abs/1912.02031, 2019.

[10] D. Iamartino, C. Pelsser, and R. Bush. Measuring bgp route origin registration and validation. In *PAM*, 2015.