Phased Deployment of Distributed RPKI

Kris Shrishak[1], Haya Shulman[2]
[1]TU Darmstadt [2]Fraunhofer SIT

In this work we aim to mitigate one of the major obstacles toward deployment of Resource Public Key Infrastructure (RPKI): exposure to prefix takedowns. RPKI was designed to prevent prefix and subprefix hijacks by enabling Autonomous Systems (ASes) to perform Route Origin Validation (ROV) to filter BGP announcements from bogus sources. However, the security benefits which come with RPKI are coupled with a new attack vector: RPKI introduces an easy way for taking down prefixes. To take down a prefix of some victim AS, a Regional Internet Registry (RIR) can manipulate the certificate information for that AS, e.g., modify a Route Origin Authorization (ROA) so that it conflicts with the BGP announcement for that AS. Networks enforcing ROV will then filter the conflicting announcements, rendering the victim AS unreachable to the rest of the Internet.

The new threat vector to take down prefixes can be exploited by law enforcement agencies. When an RIR receives a takedown request from a law enforcement agency against one of its customers, it complies with the request and revokes the signed objects. The network goes down and the result is a significant financial damage. A legal defence can take years and damage cannot be reversed. Prefix take-downs have been observed: RIPE NCC mistakenly deleted 2669 ROAs [RIP20] and, similarly, due to a mistake ARIN issued a conflicting ROA [HCRG14]. The result is that legitimate announcements were invalidated causing the networks to become disconnected. Such prefix take-downs were not possible without RPKI, since taking down a prefix not in RPKI would require carrying out a *hijack attack*, which the courts do not authorise.

In [SS20, SS21] we proposed a technological solution to this security threat introduced by RPKI. Our mechanism uses a threshold signature scheme to prevent an individual RIR from taking down IP-prefixes unilaterally and requires cooperation among the RIRs. Our mechanism not only resolves the benign errors, but also ensures that to take down a prefix in our mechanism a government or a cyber criminal would need to work across different jurisdictions where the RIRs are based. We extensively evaluated our mechanism in the lab to understand the performance and the communication overhead that it introduces.

In this talk we will discuss the steps for resolving the practical challenges towards Internet wide adoption of our proposed solution. These include evaluation in the wild, test setup at RIRs and production deployment at RIRs. First, we will set up and operate our mechanism on five distinct ASes, each instance under a different RIR, to evaluate the performance of our proposal on the existing dataset of ROAs. Second, we will set up a test environment starting with one RIR and then extending to at least three RIRs. Each participating RIR will maintain a threshold signature module. We will explore technological and inter-RIR policy challenges by communicating with the three RIRs to understand the hurdles related to policy development processes, member structures, the combined legal barriers of the RIRs. Finally, After collecting sufficient practical experience with real ASes and RIRs we will move to production deployment. Our approach utilises an incrementally deployable system that leverages instances at multiple RIRs to mitigate prefix takedowns.

References

[HCRG14] Ethan Heilman, Danny Cooper, Leonid Reyzin, and Sharon Goldberg. From the consent of the routed: improving the transparency of the RPKI. In *SIGCOMM*, pages 51–62. ACM, 2014.

[RIP20] RIPE NCC. Accidental ROA Deletion, 2020. `https://www.ripe.net/support/service-announcements/accidental-roa-deletion`.

[SS20] Kris Shrishak and Haya Shulman. Limiting the power of RPKI authorities. In *ANRW '20: Applied Networking Research Workshop, Virtual Event, Spain, July 27-30, 2020*, pages 12–18. ACM, 2020.

[SS21] Kris Shrishak and Haya Shulman. Privacy preserving and resilient RPKI. In *40th IEEE Conference on Computer Communications, INFOCOM 2021*. IEEE, 2021.

crypto day matters 32 (2021)
Beiträge vom 32. Kryptotag, 15.01.2021, online.
doi:10.18420/cdm-2021-32-13