Decentralised Internet Infrastructure: Securing Inter-Domain Routing (DEMO)

Miquel Ferriol Galmés
Albert Cabellos-Aparicio
Universitat Politècnica de Catalunya
Barcelona, Spain
{mferriol, acabello}@ac.upc.edu

***Abstract*—The Border Gateway Protocol (BGP) is the inter-domain routing protocol that glues the Internet. BGP does not incorporate security and instead, it relies on careful configuration and manual filtering to offer some protection. As a consequence, the current inter-domain routing infrastructure is partially vulnerable to prefix and path hijacks as well as in misconfigurations that results in route leaks. There are many instances of these vulnerabilities being exploited by malicious actors on the Internet, resulting in disruption of services. To address this issue the IETF has designed RPKI, a centralised trust architecture that relies on Public Key Infrastructure. RPKI has slow adoption and its centralised nature is problematic: network administrators are required to trust CAs and do not have the ultimate control of their own critical Internet resources (e.g,. IP blocks, AS Numbers). In this context, we have built the Decentralised Internet Infrastructure (DII), a distributed ledger to securely store inter-domain routing information. The main advantages of DII are (i) it offers flexible trust models where the Internet community can define the rules of a consensus algorithm that properly reflects the power balance of its members and, (ii) offers protection against vulnerabilities (path hijack and route leaks) that goes well beyond what RPKI offers. We have deployed the prototype on the wild in a worldwide testbed including 7 ASes, we will use the testbed to demonstrate in a realistic scenario how allocation and delegation of Internet resources in DII work, and how this protects ASes against artificially produced path and prefix hijack as well as a route leak.**

I. Introduction

The Border Gateway Protocol (BGP) is the inter-domain routing protocol that *glues* the Internet. BGP provides reachability, path selection and policy to Autonomous Systems (AS). The security of BGP is critical to the correct operation of the Internet, this field is referred as Inter-Domain routing security. BGP was not designed with security in mind and instead it typically relies on careful configuration and manual filtering.

Inter-domain routing security is crucial to the correct operation of the Internet. An attacker can forge BGP announcements and hijack a prefix or an AS-Path, effectively diverting traffic to networks which should not receive it or render blocks of IP prefixes unavailable. Such attacks effectively bring Internet services down, the interested reader can find in the following references [2] a detailed lists of real-life examples of such attacks.

As a recent example of the severity of this issue, on June 24, 2019, several websites started to have performance issues, including AWS services. According to [3], on that day Allegheny Technologies Inc. incorrectly propagated prefixes received from one of its providers (DQE Communications) to another provider (AS701 - Verizon).

In order to address this issue the Internet Engineering Task Force (IETF) has designed solutions to provide cryptographic guarantees to BGP messages: RPKI (RFC6480) and BGP-SEC (RFC8205). RPKI is a Public Key Infrastucture (PKI) repository to contains certificate detailing the legitimate owners of IP prefixes, AS numbers and ROAs (Route Origin Authorization, a certificate to allow a router to announce an IP prefix). On the other side, BGP-SEC aims to provide strong cryptographic guarantees of the AS-Path by signing each BGP message.

Unfortunately, RPKI has not seen widespread adoption and -at the time of this writing, its deployment stands at roughly 25% of the total IPv4 prefixes [1]. The reasons for such slow adoption have been extensively studied and discussed in the literature [4]–[8]. (i) Centralization: participants are required to trust CAs, that hold ultimate control of the resources (e.g, IP blocks). Internet resources are crucial for the correct operation of networks and as such, network owners would prefer to have a high degree of control over them [9] and (ii), Exposure of business relationships through peering agreements in the RPKI [4].

Concerning BGP-SEC, it is not being deployed at the time of this writing. The main reasons are the lack of benefits to early adopters and high computational cost at the routers [6].

We have built the Decentralized Internet Infrastructure (DII) [10], a blockchain to store inter-domain routing information. In DII, ASes (ISPs, Enteprise, Universities) as well as Internet Registries (RIRs, NIRs) participate in the distributed ledger and store the relevant routing information, IP block and ASN holders, mappings between IP blocks and ASN, etc. As in the current Internet, participants can delegate their IP blocks, this is reflected in a transaction in the ledger. With DII, participating ASes can validate BGP messages, effectively protecting against prefix hijack, path hijack as well as route leaks. Assuming equal adoption of RPKI, RPKI + BGP-SEC and DII, DII offers protection against a wider range of threats.

The main benefit of using a blockchain to secure inter-domain routing information is that it offers a flexible trust model. While RPKI builds on top a fully centralized trust

model, the distributed ledger enables the Internet community to define the rules of a consensus algorithm that properly reflects the balance of power of its members. In addition and with blockchain, participants holding Internet resources have ultimate control over them by using the public-private key pair.

The interested reader can find more information about the Decentralised Internet Infrastructure initiative [10] as well as a video of the demo [11].

II. Decentralized Internet Infrastructure (DII)

Figure 1 shows an schematic representation of the Decentralized Internet Infrastructure (DII).

DII is based on Hyperledger Fabric (v1.4) and is participated by all ASes (ISPs, Enterprise, CDNs, etc) as well as relevant Internet government bodies (IANA, RIRs, NIRs, etc). Initially, all Internet resources (IPs, ASNs) are assigned to IANA in the Genesis block, then IANA delegates resources to RIRs/NIRs which in turn further delegate to ASes. This is reflected by transactions on the ledger. With this, ASes have control over their IP blocks and ASNs and can further delegate them if required. Finally, ASes can state their AS Adjacencies (ASes over which they are directly connected to) as well as their AS relationships (Peering, Customer-Provider). Since ASes they consider such information private, we take advantage of the privacy features available at HLF to enable ASes to control who has access to such information. This information is used to protect against path hijack and route leaks.

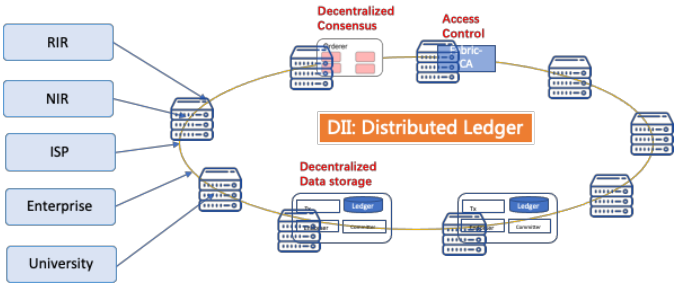

Fig. 1: Overview of the Blockchain Architecture.

Fig. 2: Decentralized Internet Infrastructure testbed.

We have built a prototype of DII using HLF 1.4, the code runs on a VM (Ubuntu 16.4) dockerized (18.09.7). Every peer node is both committer and endorsers, and for simplicity we only consider one HL organization. BGP speakers are implemented using software open-source routers (FRRouting [1]). We have deployed the testbed on the wild, figure 2 shows the worldwide deployment that includes 7 participants.

[1]https://frrouting.org/

III. Demo script

In the demo we use the testbed to show the DII capabilities, we have implemented a web-based GUI for this. The proposed script is as follows:

1) Context and Motivation: We first describe the main issues with inter-domain routing security, describe RPKI and BGP-SEC. Describe main security threats: prefix and path hijack, route leak. Describe how a distributed ledger can mitigate such attacks.
2) Internet resources allocation: We take advantage of the DII GUI to show a realistic chain of allocations and delegations of IP blocks and ASNs, from IANA to a set of ASes. This is showcased in the live worldwide testbed and demonstrated through log files.
3) Protection against relevant inter-domain security threads: Once the ledger has all the required information, we artificially produce three attacks (prefix hijack, path hijack and route leak) and showcase by means of log files (FRR and HLF) how the DII ledger protects the ASes.
4) Beyond Inter-domain routing security: To conclude, we discuss how the DII ledger can be used as a general layer to achieve decentralized trust for third party applications on the Internet.

References

[1] NIST RPKI Deployment Monitor https://rpki-monitor.antd.nist.gov/
[2] List of BGP hijack public incidents https://en.wikipedia.org/wiki/BGP$_hijacking$
[3] Aftab Siddiqui, "Route Leak Causes Major Google Outage", https://www.internetsociety.org/blog/2018/11/route-leakcaused-a-major-google-outage/
[4] M. Wahlisch, et al. RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem. Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV,2015
[5] W. George. Adventures in RPKI (non) deployment. Technical report, NANOG 62, 2014.
[6] S. Goldberg. Why is it taking so long to secure internet routing? Queue, 12(8): 20:20–20:33, August 2014. ISSN 1542-7730.
[7] X. Liu, et al. RPKI deployment: Risks and alternative solutions. In Advances in Intelligent Systems and Computing, volume 387, pages 299–310, 2016. ISBN 9783319232034.
[8] Y. Gilad, et al. Are we there yet? on rpki's deployment and security. IACR Cryptology ePrint Archive, 2016.
[9] D. Cooper, et al. On the risk of misbehaving rpki authorities. In Proceedings of the Twelfth ACM Workshop on Hot Topics in Networks, HotNets-XII,2013
[10] European Telecommunications Standards Institute (ETSI) PDL Decentralized Internet Infrastructure (DII) https://pdlwiki.etsi.org
[11] European Telecommunications Standards Institute (ETSI) Decentralized Internet Infrastructure (DII) Video Demo https://www.brighttalk.com/webcast/12761/433364