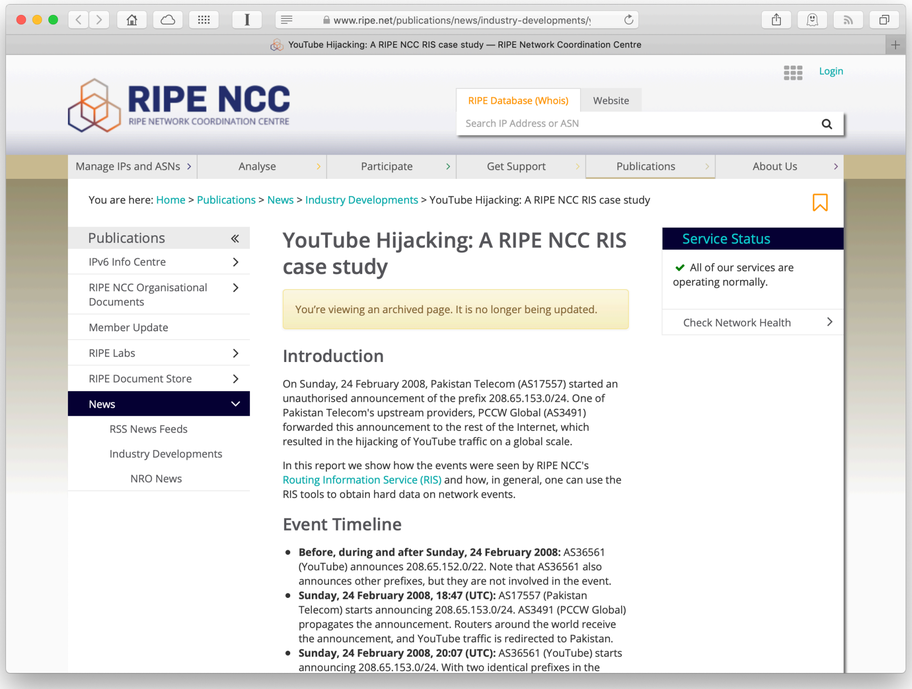
Routing Security

- Internet Routing Security
- RPKI
- MANRS

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Internet Routing is not Secure

- Any AS participating in BGP routing can announce any address prefix – whether or not they own it
  - Sometimes this is accidental
  - Sometimes this is malicious
- Result is that traffic is misdirected: **BGP hijacking**
  - Security risk if traffic can be misdirected
  - Accidental hijacking is a serious stability problem for the network



https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Resource Public Key Infrastructure (RPKI)

- RPKI is an attempt to secure Internet routing
- Lets an AS make a signed **Route Origin Authorisation** (ROA) – a digital signature, announced via BGP, proving the AS is authorised to announce a IP address prefix
  - Hierarchical delegation: RIR → provider AS → customer AS
  - Allows a router to validate whether a prefix announcement is authorised – hijacked prefixes will not have a valid signature
  - Becomes part of BGP policy: prefer signed prefixes
- As of 2019, about ~12% of IPv4 addresses are covered by prefixes with valid digital signatures, but growing rapidly
- More information:
  - https://blog.cloudflare.com/rpki-2020-fall-update/
  - https://isbgpsafeyet.com/



RPKI is Coming of Age

A Longitudinal Study of RPKI Deployment and Invalid Route Origins

Taejoong Chung
Rochester Institute of Technology

Emile Aben
RIPE NCC

Tim Bruijnzeels
NLNetLabs

Balakrishnan Chandrasekaran
Max Planck Institute for Informatics

David Choffnes
Northeastern University

Dave Levin
University of Maryland

Bruce M. Maggs
Duke University and
Akamai Technologies

Alan Mislove
Northeastern University

Roland van Rijswijk-Deij
University of Twente and
NLNetLabs

John Rula
Akamai Technologies

Nick Sullivan
Cloudflare

ABSTRACT

Despite its critical role in Internet connectivity, the Border Gateway Protocol (BGP) remains highly vulnerable to attacks such as prefix hijacking, where an Autonomous System (AS) announces routes for IP space it does not control. To address this issue, the Resource Public Key Infrastructure (RPKI) was developed starting in 2008, with deployment beginning in 2011. This paper performs the first comprehensive, longitudinal study of the deployment, coverage, and quality of RPKI.

We use a unique dataset containing *all* RPKI Route Origin Authorizations (ROAs) from the moment RPKI was first deployed, more than 8 years ago. We combine this dataset with BGP announcements from more than 3,300 BGP collectors worldwide. Our analysis shows the after a gradual start, RPKI has seen a rapid increase in adoption over the past two years. We also show that although misconfigurations were rampant when RPKI was first deployed (causing many announcements to appear as invalid) they are quite rare today. We develop a taxonomy of invalid RPKI announcements, then quantify their prevalence. We further identify suspicious announcements indicative of prefix hijacking and present case studies of likely hijacks.

Overall, we conclude that while misconfigurations still do occur, RPKI is "ready for the big screen," and routing security can be increased by dropping invalid announcements. To foster reproducibility and further studies, we release all RPKI data and the tools we used to analyze it into the public domain.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

IMC '19, October 21–23, 2019, Amsterdam, Netherlands

© 2019 Association for Computing Machinery.

ACM ISBN 978-1-4503-6948-0/19/10…$15.00
https://doi.org/10.1145/3355369.3355596

1 INTRODUCTION

The Border Gateway Protocol (BGP) is *the* mechanism that allows routers to construct routing tables across the Internet. Unfortunately, the original BGP protocol lacked many security features (e.g., authorization of IP prefix announcements), making BGP vulnerable to attacks such as prefix hijacking [3, 5, 7, 14] and route leaks [5]. To defend against these threats, the Resource Public Key Infrastructure (RPKI) was developed in April 2008 as part of the IETF in the SIDR Working Group [54]. Beta deployments followed in the years after, until all Regional Internet Registries (RIRs) started production deployment of RPKI in January 2011.

At its core, RPKI is a hierarchical Public Key Infrastructure (PKI) that binds Internet Number Resources (INRs) such as Autonomous System Numbers (ASNs) and IP addresses to public keys via certificates. The corresponding private keys can be used by certificate holders to make attestations about these INRs—most importantly, Route Origin Authorization (ROA) objects. ROAs allow a certificate holder to authorize an ASN to announce certain IP prefixes, and are signed using the private key of a certificate covering the IP space.

Each of the five RIRs operate their own RPKI *trust anchor* (equivalent to a root certificate in other PKIs), the private key of which is used to sign such certificates. The RIRs also offer hosted services to their members, enabling them to obtain RPKI certificates and generate ROAs.

RPKI objects including certificates, ROAs, and supporting structures such as manifests and certificate revocation lists (CRLs) are published in so-called RPKI *repositories*. RPKI validation software—called Relying Party (RP) software—retrieves objects from these repositories and performs cryptographic validation of the content, ultimately producing a set of valid ROAs. A *validating router* can then use this set to verify incoming BGP announcements. If the router finds a BGP announcement to be in conflict with the set of valid ROAs, it should reject the announcement as (by definition) the origin AS is not authorized to announce the IP prefix(es).

While RPKI sounds straightforward, in practice it can be complex, creating many opportunities for mistakes. For example, an AS may sub-allocate an IP prefix to a customer AS without updating its ROAs or mistakenly include the wrong range of IP prefixes in a

406

Taejoong Chung, *et al.*, "RPKI is coming of age: A longitudinal study of RPKI deployment and invalid route origins", ACM Internet Measurement Conference, Amsterdam, October 2019.https://dx.doi.org/10.1145/3355369.3355596

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Mutually Agreed Norms for Routing Security (MANRS)





- **Mutually Agreed Norms for Routing Security (MANRS)** project aims to improve routing security (https://www.manrs.org)
  - Filtering
  - Anti-spoofing
  - Coordination
  - Global validation via RKPI
  - Combination of signed route advertisements via RKPI to catch malicious attacks, with best practises for route filtering, anti-spoofing, and coordination between ISPs to protect against misconfigurations

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow

Routing Security

- Internet Routing Security
- RPKI
- MANRS

Colin Perkins | https://csperkins.org/ | Copyright © 2020 University of Glasgow