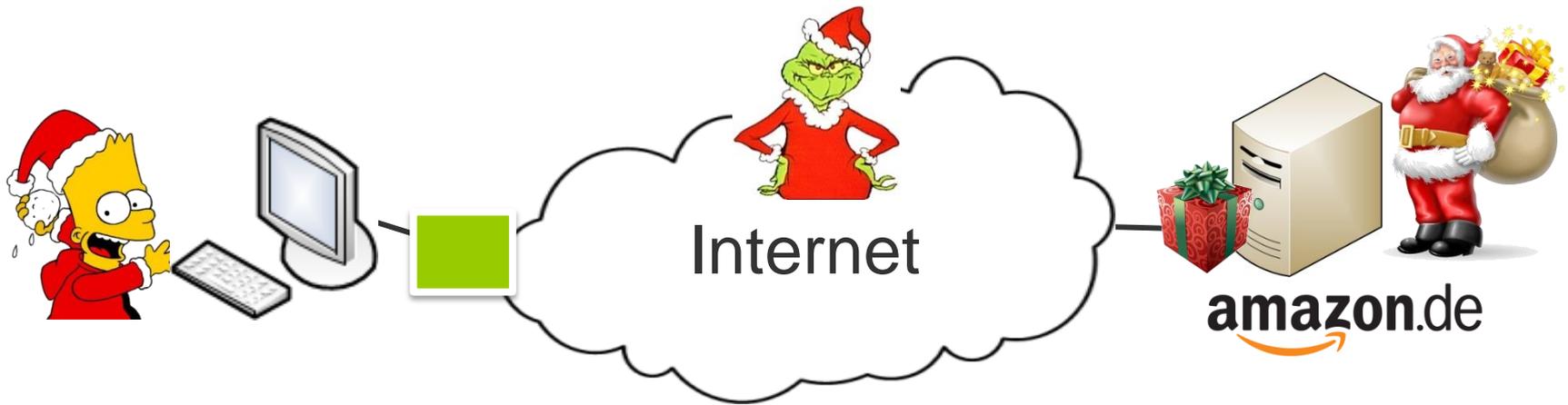


RiPKI: The Tragic Story of RPKI Deployment in the Web Ecosystem.

Or why Xmas online shopping might go wrong.

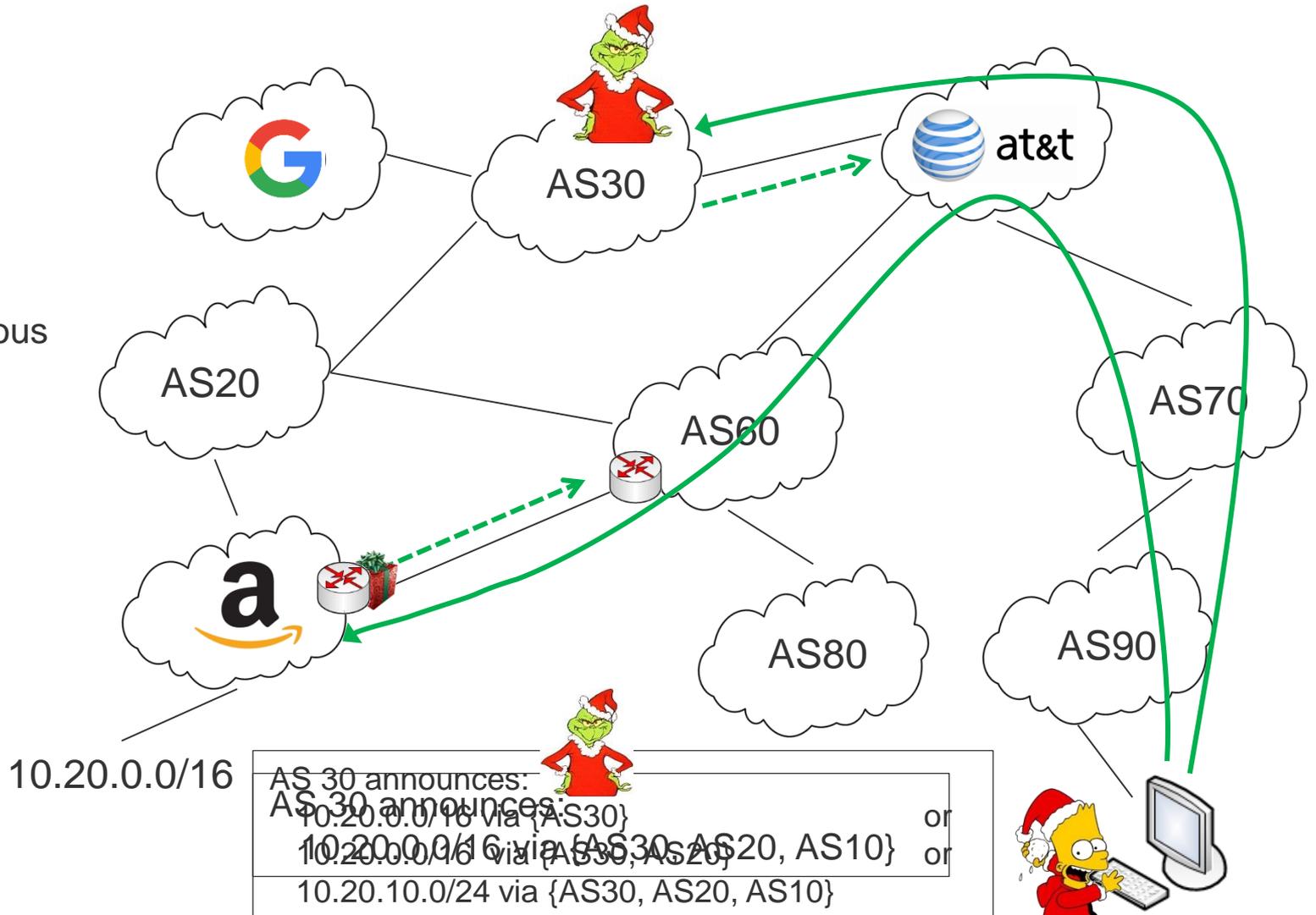
**Matthias Wählisch, Robert Schmidt, Thomas C.
Schmidt, Olaf Maennel, Steve Uhlig, Gareth Tyson**

Starting Point



Recap: Internet in a Nutshell & Attacks

Autonomous Systems (ASes)



What is This Talk About?

How can you prevent your network from prefix hijacking?

How can you perform prefix origin validation?

What is the state of deployment of current countermeasures?

Why does the current web ecosystem challenges network security?

Why would you not deploy current security mechanisms in the backbone?

Agenda

1. Problem space
2. Proposed IETF solutions
3. Tools: Monitoring RPKI deployment
4. RPKI and the web ecosystem

RPKI

Original Design Choice (RFC 4271)

- BGP is based on trust between peers

Implications

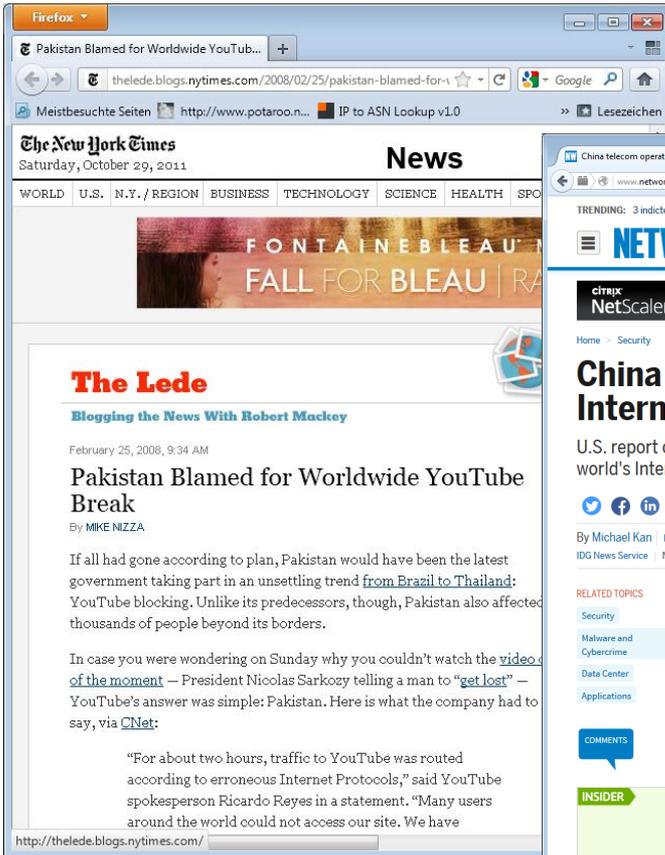
- Any BGP speaker can claim to own an IP prefix
- Any BGP speaker can modify the AS path
- Receiver of a BGP update cannot verify the correctness of the data

Compromise

- Filtering
 - Considering data of the Internet Routing Registry
- ⇒ This is not enough anymore!

Hijacks in the Real World?!

Prominent examples



The Lede
Blogging the News With Robert Mackey

February 25, 2008, 9:34 AM

Pakistan Blamed for Worldwide YouTube Break

By MIKE NIZZA

If all had gone according to plan, Pakistan would have been the latest government taking part in an unsettling trend from Brazil to Thailand: YouTube blocking. Unlike its predecessors, though, Pakistan also affected thousands of people beyond its borders.

In case you were wondering on Sunday why you couldn't watch the video of the moment – President Nicolas Sarkozy telling a man to “get lost” – YouTube's answer was simple: Pakistan. Here is what the company had to say, via CNet:

“For about two hours, traffic to YouTube was routed according to erroneous Internet Protocols,” said YouTube spokesperson Ricardo Reyes in a statement. “Many users around the world could not access our site. We have

<http://thelede.blogs.nytimes.com/>



China telecom operator denies hijacking Internet traffic

U.S. report claims China Telecom hijacked 15 percent of the world's Internet traffic for a short time in April

By Michael Kan

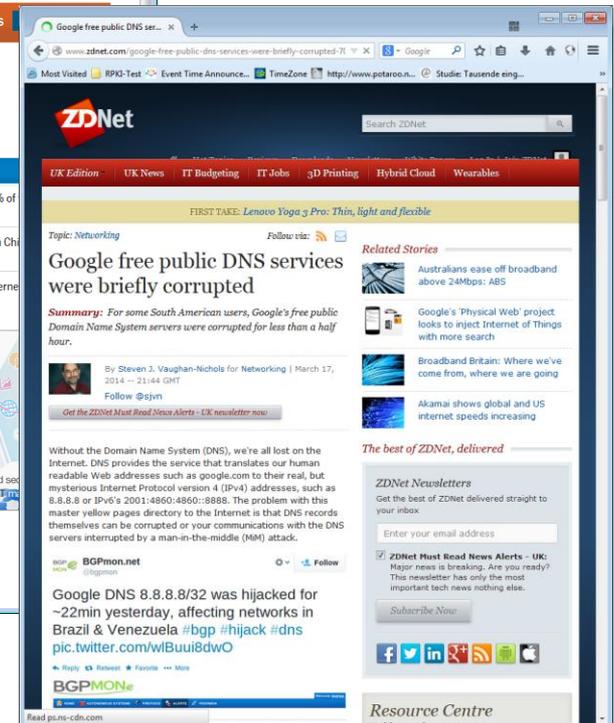
China's largest fixed-line phone carrier has denied it hijacked worldwide Internet traffic this past April following a U.S. government report that said the company had redirected network routes through Chinese servers.

Five ways to beat the Great Firewall of China

China Telecom rejected the claims in an email statement, but offered no further comment.

MORE ON NETWORK WORLD: 26 crazy and scary things the TSA has found on travelers

A report to the U.S. Congress published on Wednesday claims that for 18 minutes on April 8, China Telecom rerouted 15 percent of the Internet's traffic through Chinese servers. The traffic affected U.S. government and military websites, said the U.S.-China Economic and Security Review Commission in the report.



Google free public DNS services were briefly corrupted

Summary: For some South American users, Google's free public Domain Name System servers were corrupted for less than a half hour.

By Steven J. Vaughan-Nichols for Networking | March 17, 2014 - 21:44 GMT

Without the Domain Name System (DNS), we're lost on the Internet. DNS provides the service that translates our human readable Web addresses such as google.com to their real, but mysterious Internet Protocol version 4 (IPv4) addresses, such as 8.8.8.8 or IPv6's 2001:4860:4860::8888. The problem with this master yellow pages directory to the Internet is that DNS records themselves can be corrupted or your communications with the DNS servers interrupted by a man-in-the-middle (MIM) attack.

Google DNS 8.8.8.8/32 was hijacked for ~22min yesterday, affecting networks in Brazil & Venezuela #bgp #hijack #dns pic.twitter.com/wBui8dwO

Caveat: Reasons may also be misconfiguration ;-)

Protection Concepts

1. Prefix Origin Validation

- Mapping of IP prefixes and origin AS necessary
 - Including cryptographic proof
 - Prefix owner should be able to authenticate *Origin AS(es)*
- BGP router compares BGP update with mapping

2. Path Validation

- BGP path information are cryptographically secured
 - Paths will be signed

Challenges

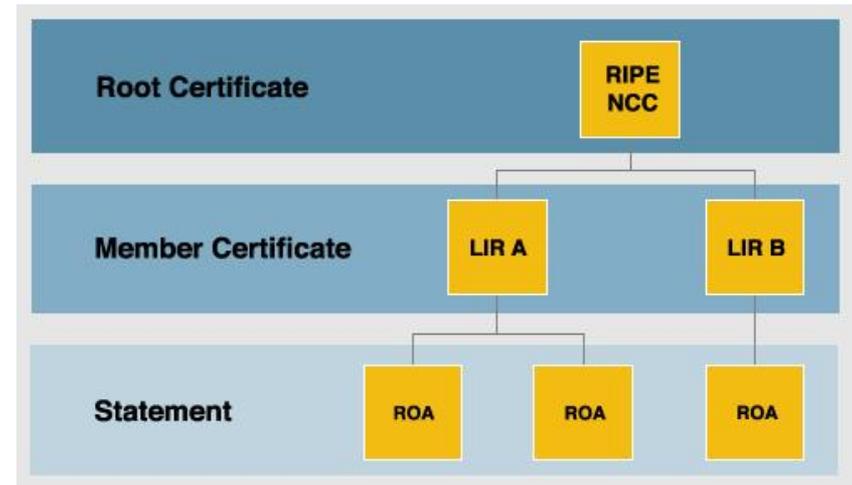
- Cryptographic operations are complex
- Minimal additional load at routers

In the following we concentrate on 1.

Proposed Solution in the IETF

Resource Public Key Infrastructure (RPKI)

- System that allows to attest the usage of IP addresses and ASNs (i.e., Internet resources)
- RPKI includes cryptographically provable certificates
- Certificate hierarchy reflects IP-/AS-allocation in the Internet
 - Currently, each RIR creates a self-signed root certificate



Source: RIPE

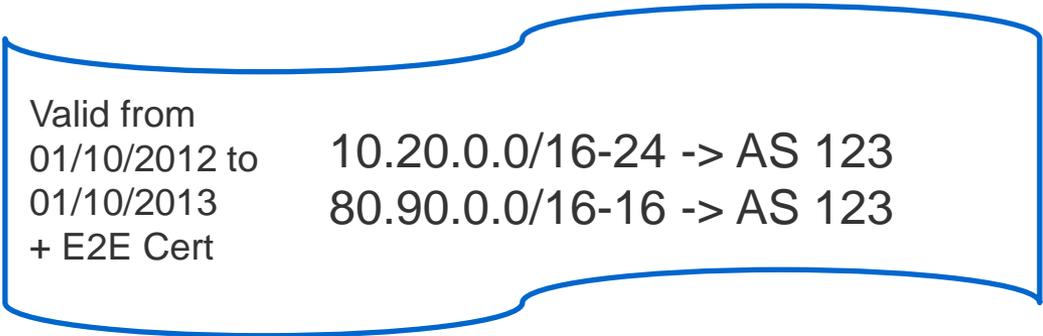
- Implementation of the RPKI started January 2011
- All RIRs participate

Routing Origination Authorization (ROA)

- Content of an ROA
 - Set of IP prefixes with minimal and maximal (optional) length
 - An AS number allowed to announce the prefixes
 - End-Entity-Certificate
- ROA will be signed with the certificate of the RPKI
- Note: Multiple ROAs per IP prefix possible

Example:

ROA



Valid from
01/10/2012 to 10.20.0.0/16-24 -> AS 123
01/10/2013 80.90.0.0/16-16 -> AS 123
+ E2E Cert

AS 123 is allowed to announce network range 10.20.0.0/16 to 10.20.0.0/24 and 80.90.0.0/16 from 1st Oct. 2012 until 1st Oct. 2013

Validation process consists of two steps

1. Validation of ROAs

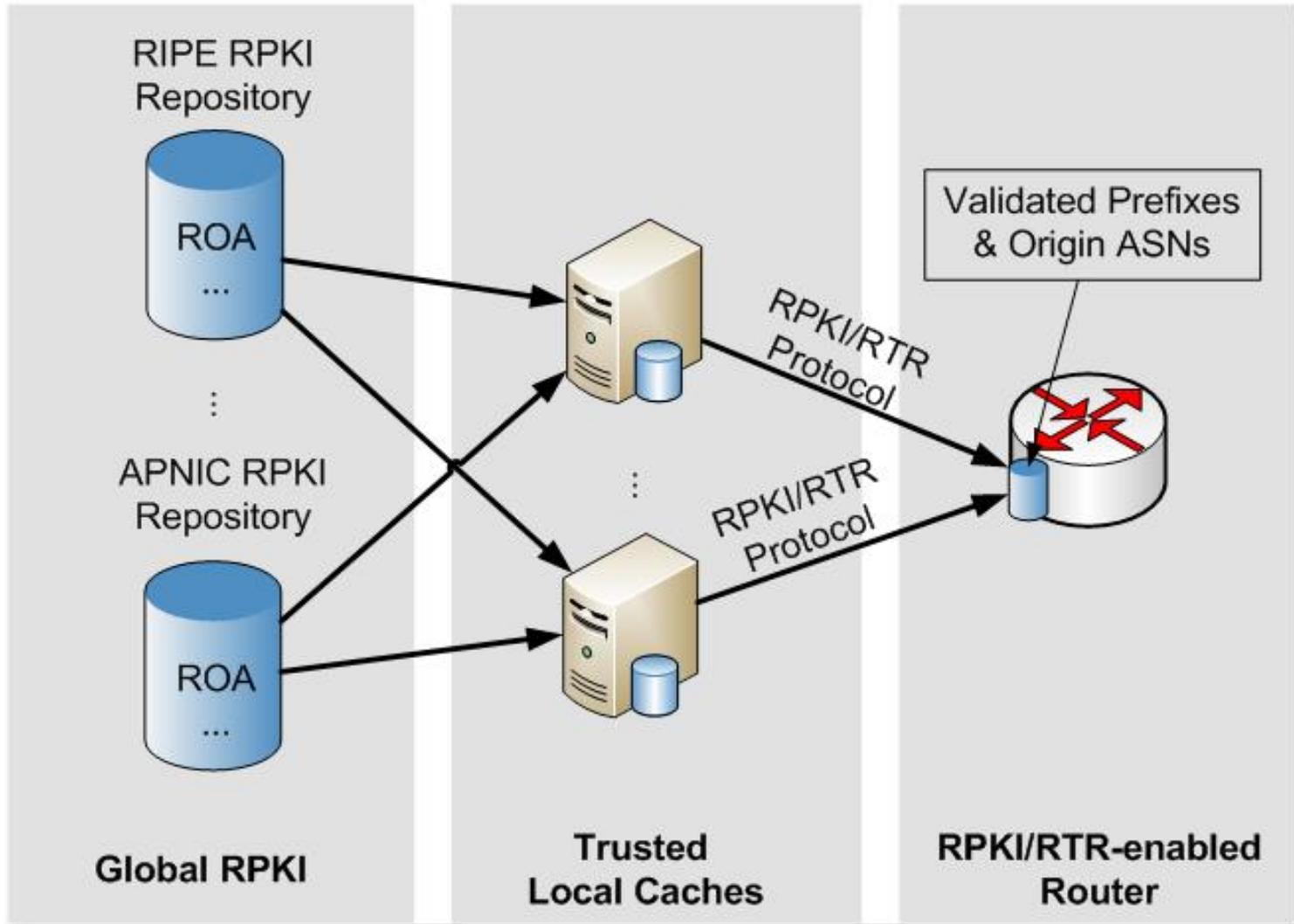
- Performed at external cache

2. Validation of BGP updates

- Performed at BGP router
- No additional cryptographic operations necessary

How does the RPKI data comes to the BGP router?

Architecture Overview



TOOLS

General objective

- Open source implementation of the RPKI-RTR client protocol in C

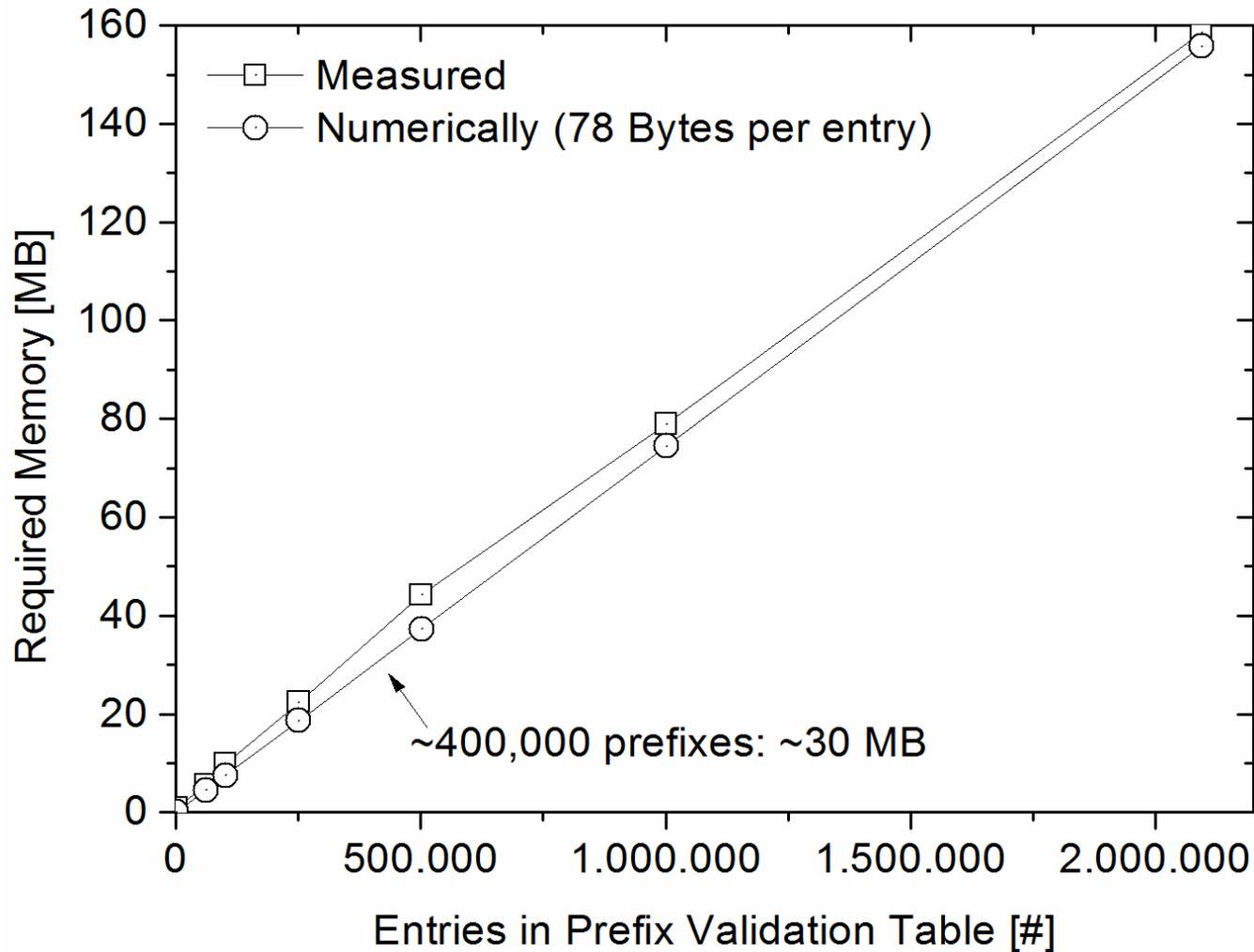
Details

- Fetch validated prefixes + origin ASes from RPKI cache
- Keep the routers validation database in sync
- Provide an interface between local database and routing daemon to access validated objects
- Allow also for validation of BGP updates
- Conforms to relevant IETF RFCs/drafts

Applications

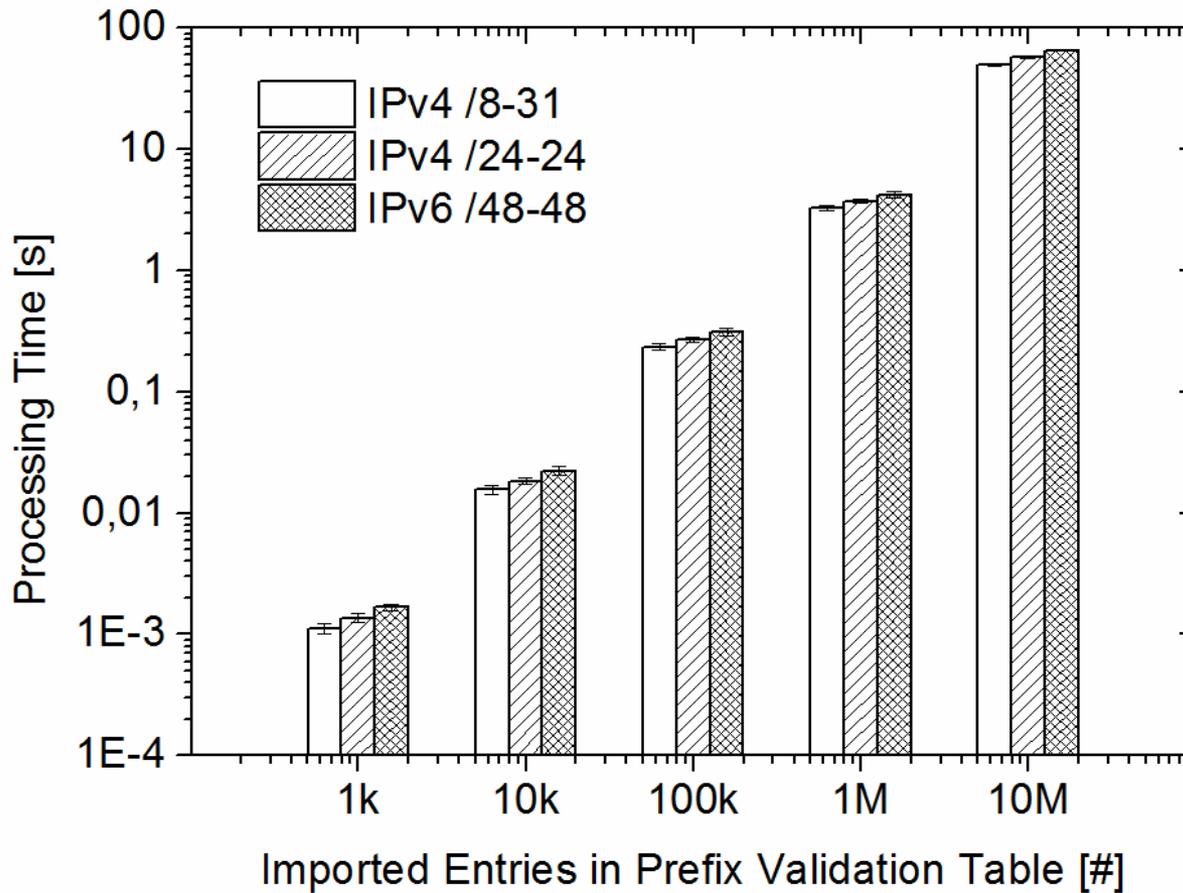
- Extending BGP daemons Quagga and BIRD
- Integration into CAIDA BGPstream
- +++

Memory Consumption



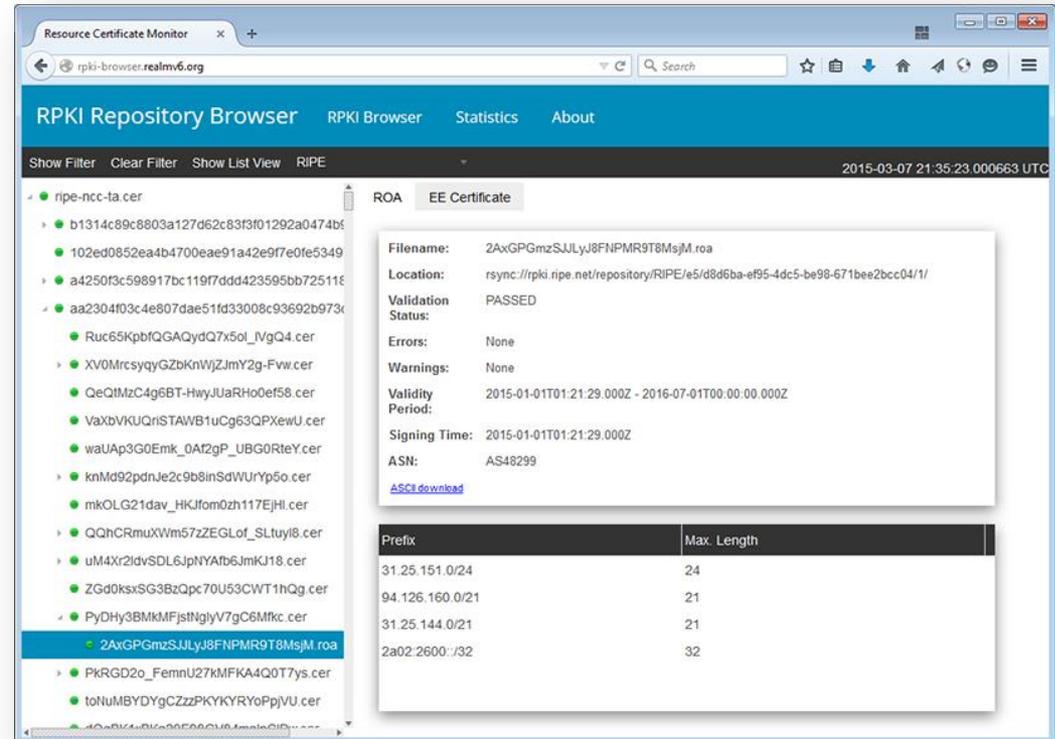
Delay While Loading ROA Data

Motivation: Router bootstrapping, Cache-Server-Reset



RPKI MIRO [Demo@SIGCOMM'15]

- Open source tool to monitor and explore RPKI repositories
- Modular architecture
 - Validator
 - Statistics
 - Browser
- Typical users
 - RIRs / CAs
 - Providers
 - Researchers
 - ...
- <https://github.com/rpki-miro>
- <http://rpki-browser.realmv6.org/>



The screenshot shows the RPKI Repository Browser interface. The left sidebar displays a tree view of certificates under the 'ripe-ncc-ta.cer' repository. The main content area shows the details for a selected ROA certificate: '2AxGPGmzSJLjy8FNPmR9T8MjM.roa'. The details include the filename, location, validation status (PASSED), errors (None), warnings (None), validity period (2015-01-01T01:21:29.000Z - 2016-07-01T00:00:00.000Z), signing time (2015-01-01T01:21:29.000Z), and ASN (AS48299). Below the details is a table showing the ROA prefixes and their maximum lengths.

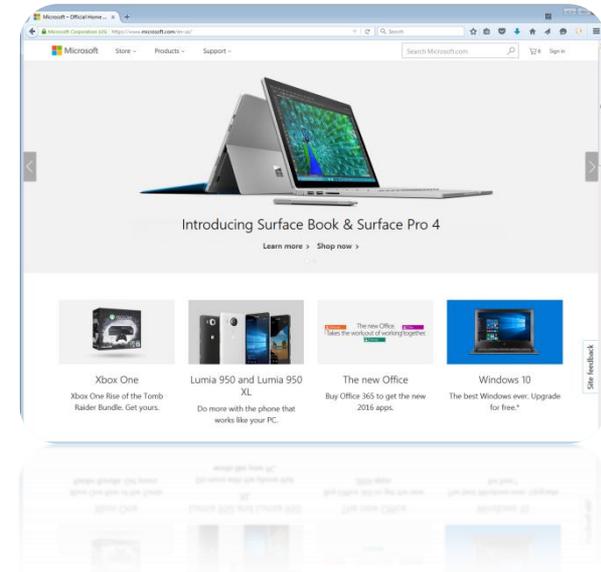
Prefix	Max. Length
31.25.151.0/24	24
94.126.160.0/21	21
31.25.144.0/21	21
2a02.2600./32	32

RiPKI: RPKI & THE WEB ECOSYSTEM [HOTNETS'15]

Motivation

Exclusive protection by TLS is insufficient!

1. Compromised trusted CAs
 - DANE rarely deployed
2. Forged certificates
 - DANE rarely deployed
 - Extended Validation rarely deployed [IMC'11]
 - Leveraged by prefix hijacking [Black Hat'15]
3. Blackholing
 - Implemented by prefix hijacking



Attacker Model (in the Web Ecosystem)

- Attacker is able to manipulate Internet routing
- Drop or forward redirected traffic to web server

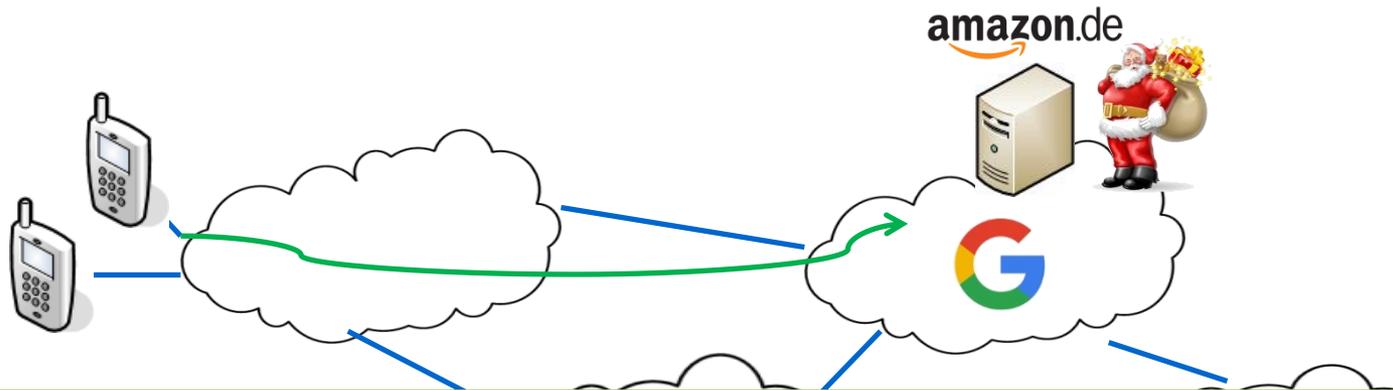
Advantages compared to common DDoS attacks in the web

- DDoS and data manipulation are possible
- Attack does not need to affect all clients
- Web server is not aware of attack

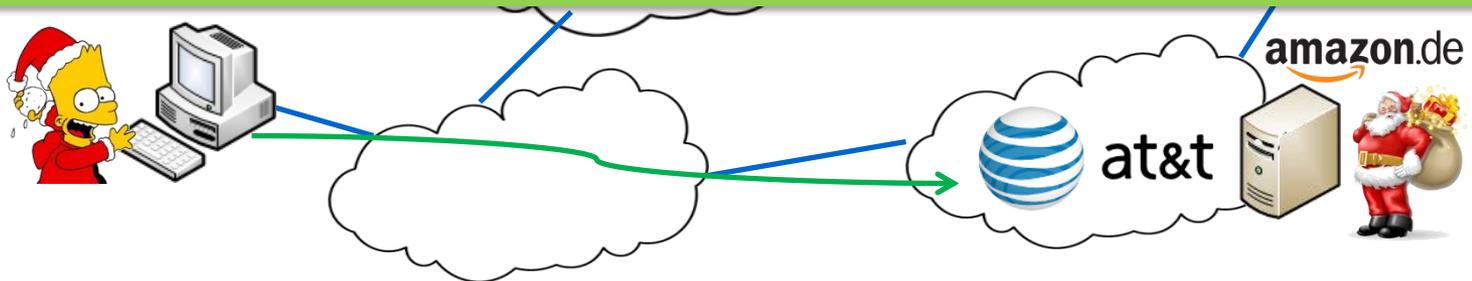
Empirically explore the relationship between web hosting infrastructure and RPKI deployment (ROA creation).

Which web servers are secured by the RPKI?

Web Ecosystem

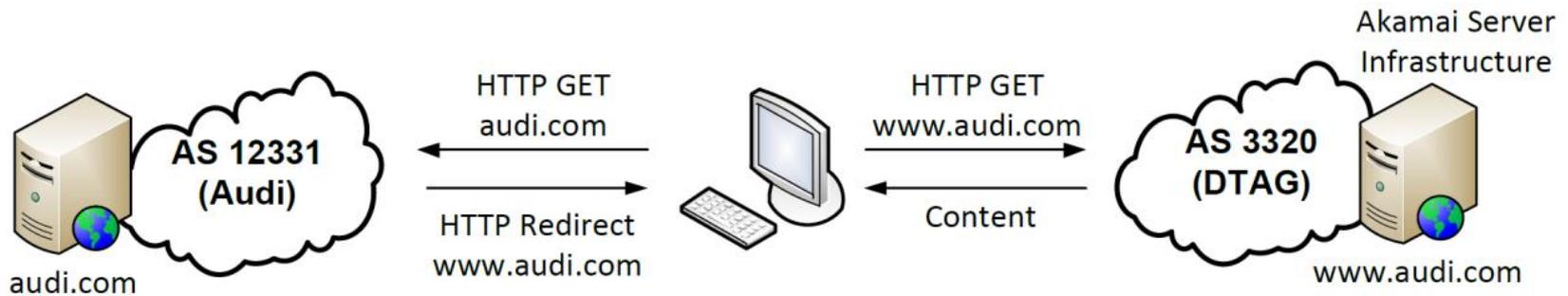


CDNs make web access faster.
But measurements and security more challenging.

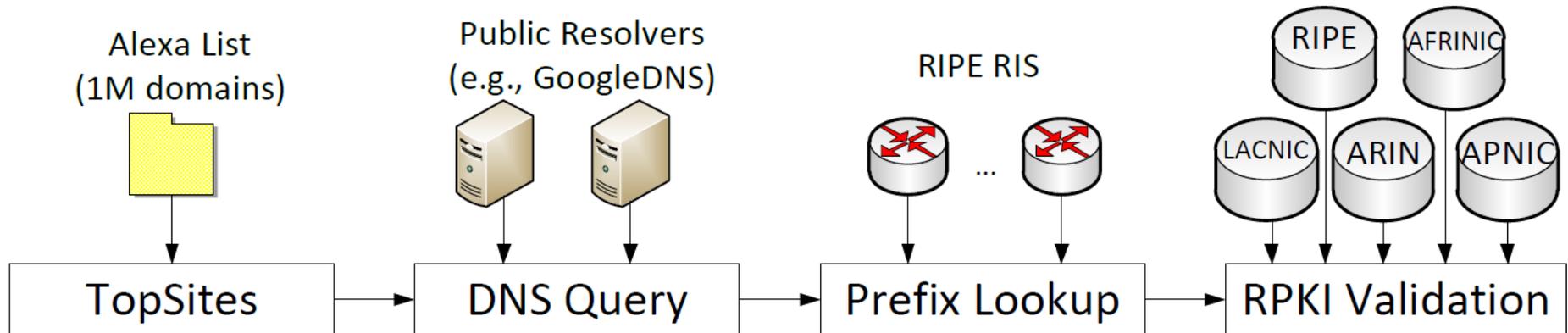


Challenges

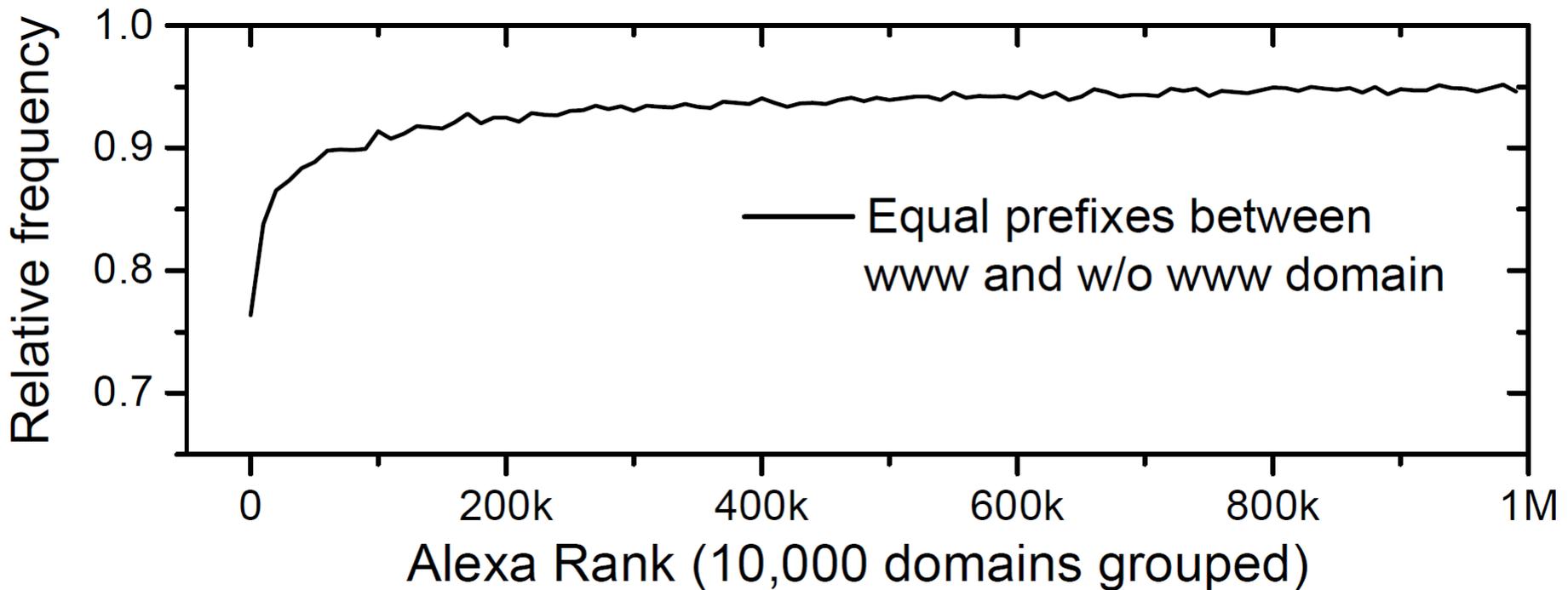
- DNS resolution results may depend on the location
- DNS resolution is time-consuming
- ⇒ We use stable, public ORDNS servers
- Embedded content
- ⇒ This study focuses on landing page
- Selecting domain names
- ⇒ Prefix www and w/o www



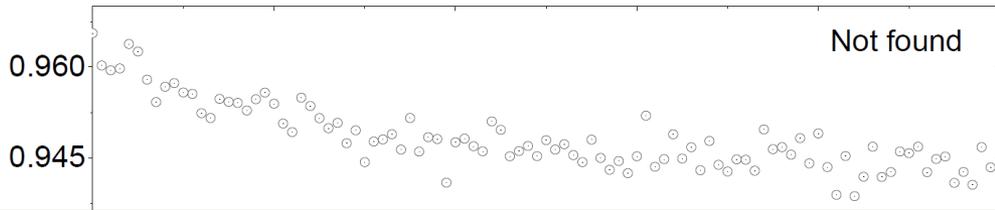
Overview: Measurement Methodology



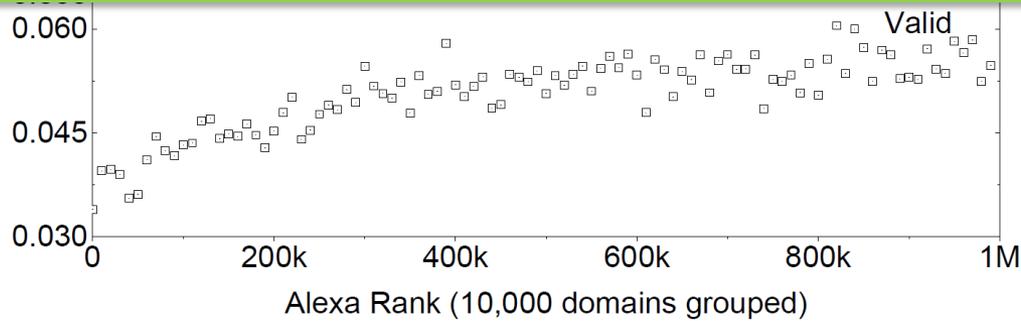
Side Result: Reducing Measurement Overhead?



RPKI Validation Outcome for 1M Web Sites

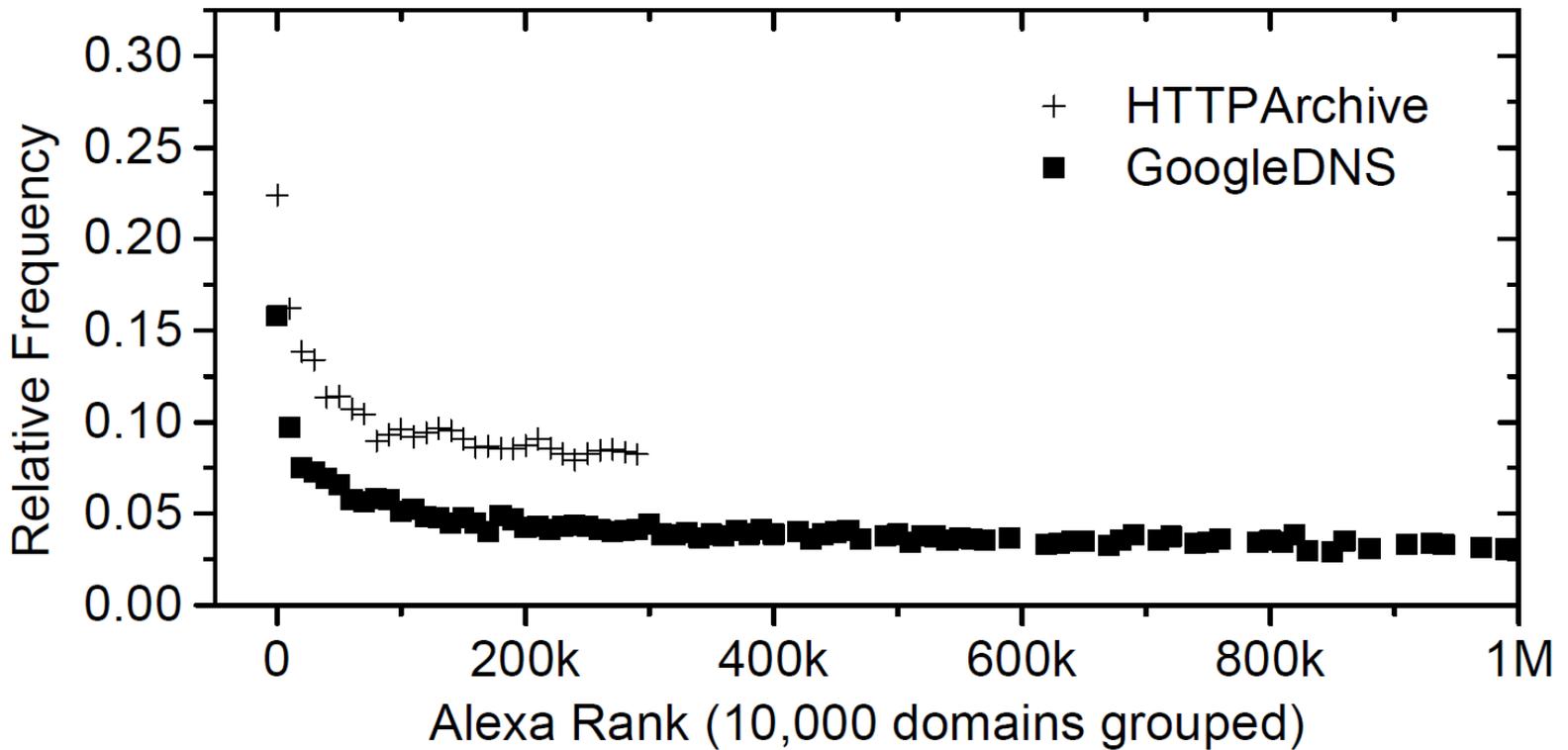


More popular sites are less secured!

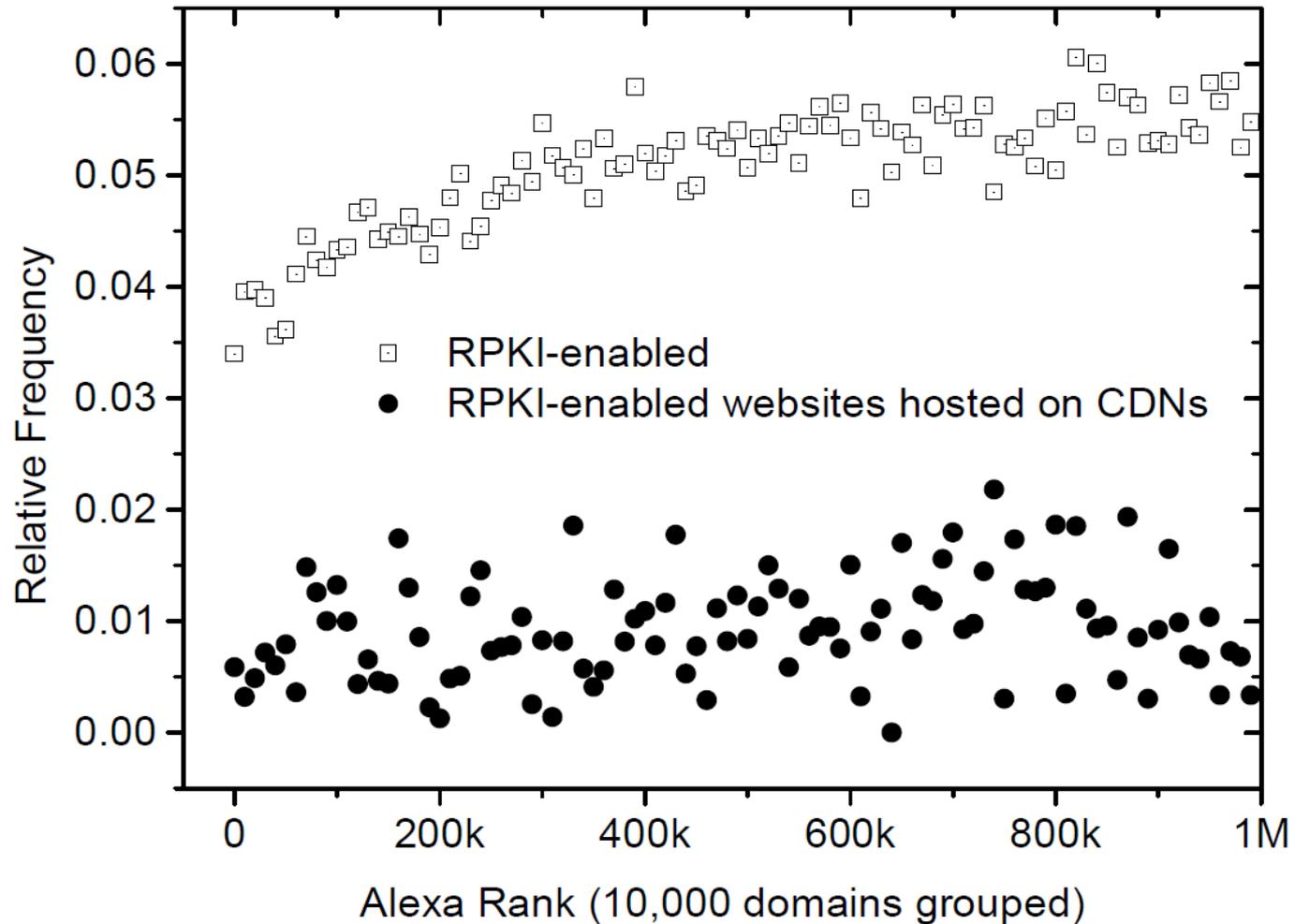


130 booking.com ✓ (4/4) ✓ (2/2)

Popularity of CDNs Across Ranks



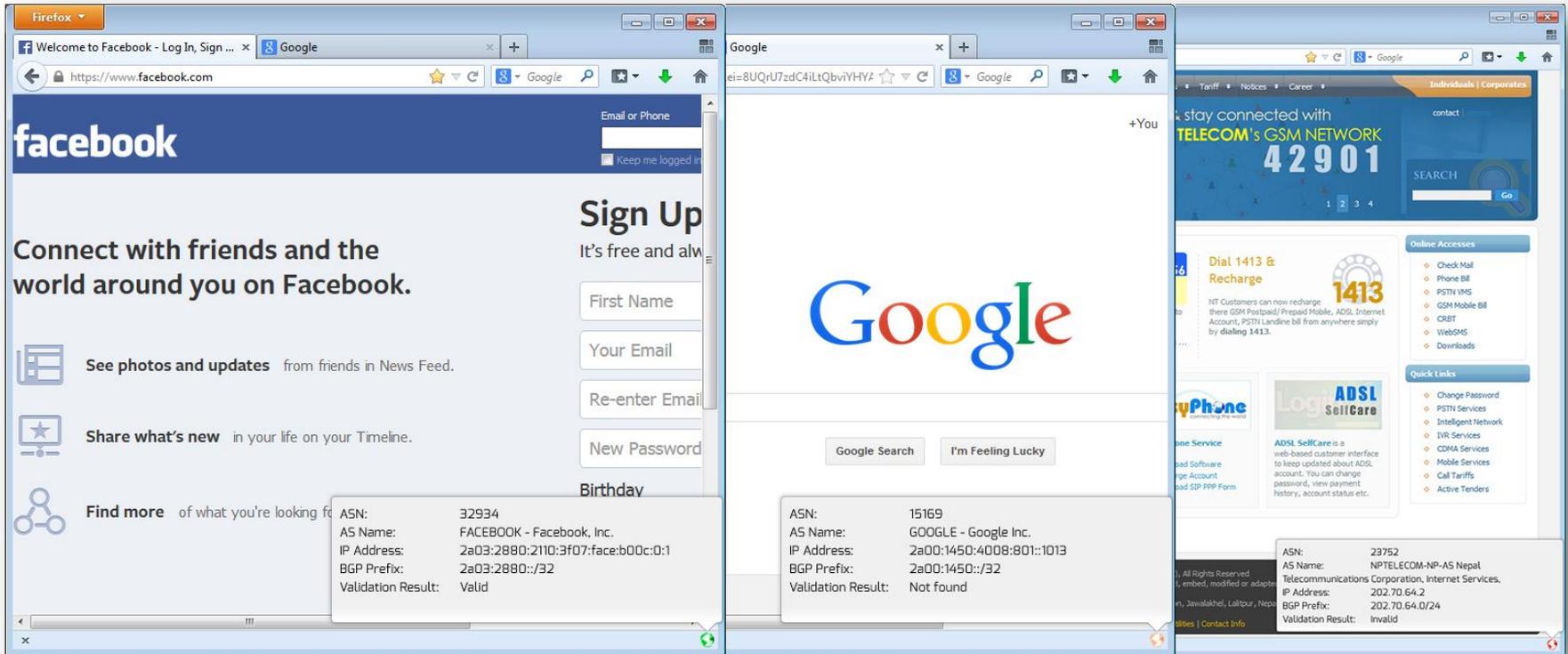
Do CDNs Push a Specific Rank?



Reasons for not Deploying RPKI

- Political reasons
 - RIR are trust anchors
 - Local law may instruct RIR to revoke certificates
 - ROAs become invalid
 - Out of control of the operator
- Business reasons
 - RPKI implements a positive attestation model
 - ISPs have to add prefix-AS relation in advance
 - Might conflict with business policies
- Cost and complexity reasons

First Steps Towards Improved Browsing Experience



- RPKI is one building block in securing e2e communication
- CDNs are hesitant in deploying RPKI, popular sites are less secure
- CDN content benefits from RPKI deployment in 3rd party networks

Future research topics

- Improve web measurement methodology
 - Accelerate DNS measurements ...
- Consider embedded content from external sites
- Improve securing web (content delivery) architecture
- Understand better *why* operators do not deploy security
 - Deployment comparison with DNSSEC