T3: Reliable measurements with BGP and RPKI

Part II - RPKI

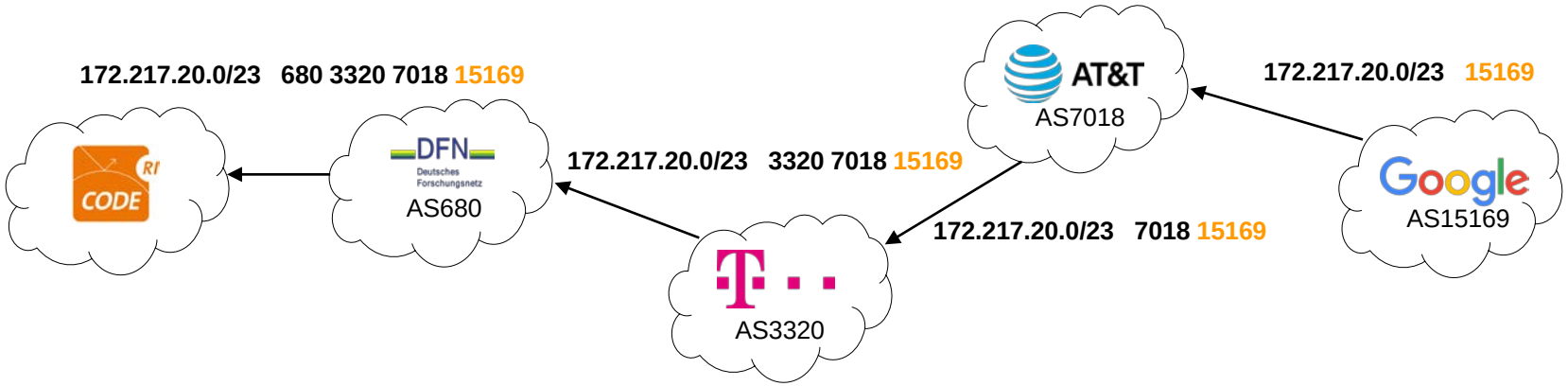
Mattijs Jonker, m.jonker@utwente.nl
Nils Rodday, nils.rodday@unibw.de

Timeline

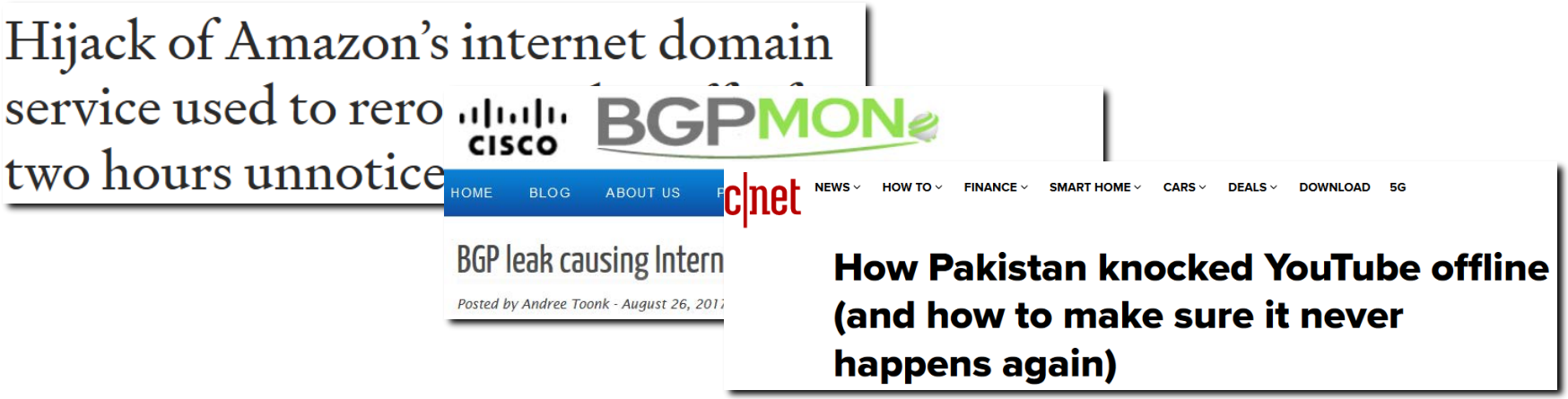
1. Introduction to RPKI (20min)
2. Which address space is covered by RPKI?
   - Exercise 1 – Hands On (15min)
   - Exercise 1 – Solution (5min)
3. Controlled vs. uncontrolled experiments (15min)
4. Which Autonomous Systems are performing ROV?
   - Exercise 2 – Hands On (20min)
   - Exercise 2 – Solution (5min)
5. Wrap-Up (10min)

Introduction to RPKI – BGP Routing

Regular scenario:



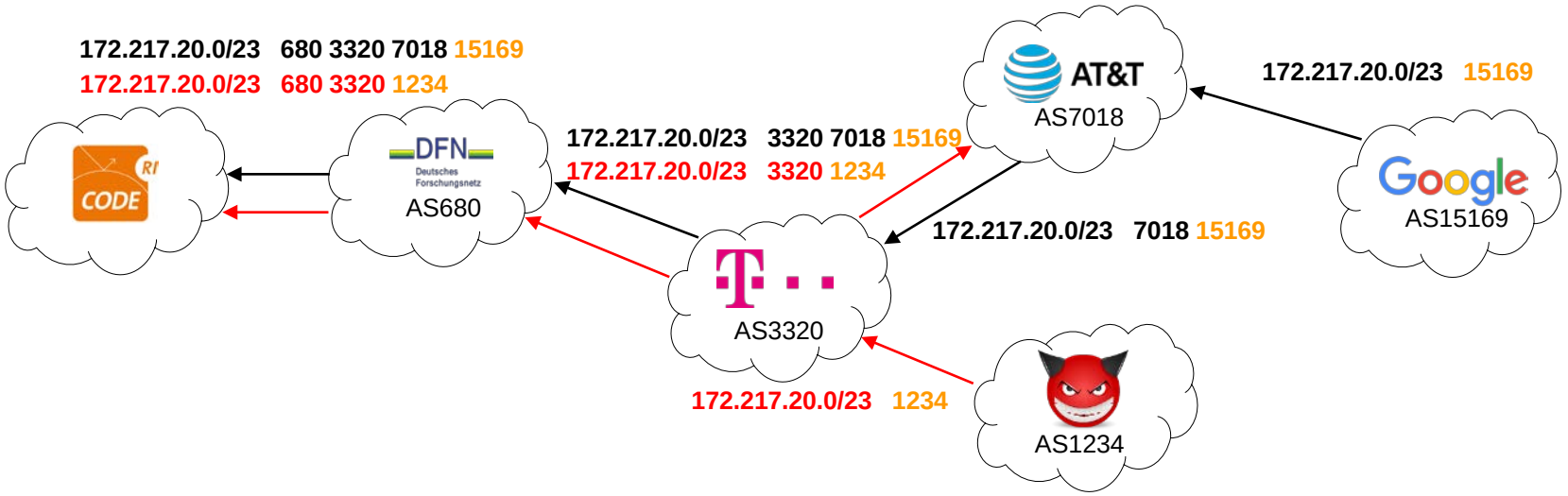
Introduction to RPKI – The Problem



BGP Hijacking

Introduction to RPKI – The Problem

Exact Prefix Hijack:

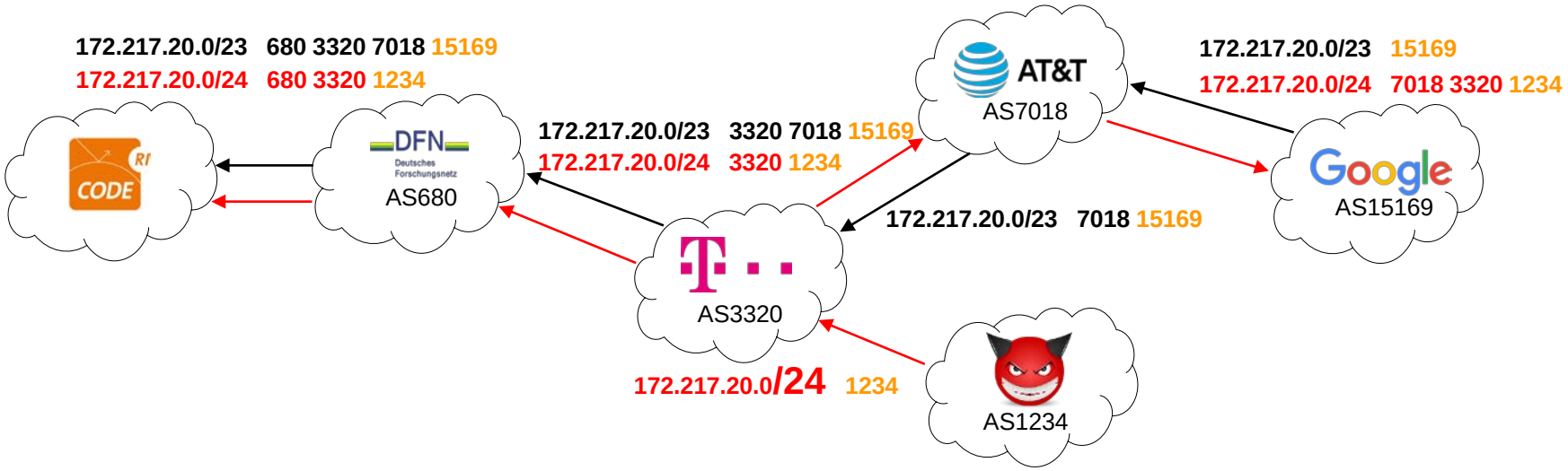


would choose the hijacked route as it is shorter towards the destination.

AT&T would still choose the correct route as it is shorter towards the destination.

Introduction to RPKI – The Problem

More-Specific Prefix Hijack:



Everyone chooses the hijacked route as it is more specific (/24 instead of /23)!

Introduction to RPKI – Origin Validation

Problem: No proof of address ownership

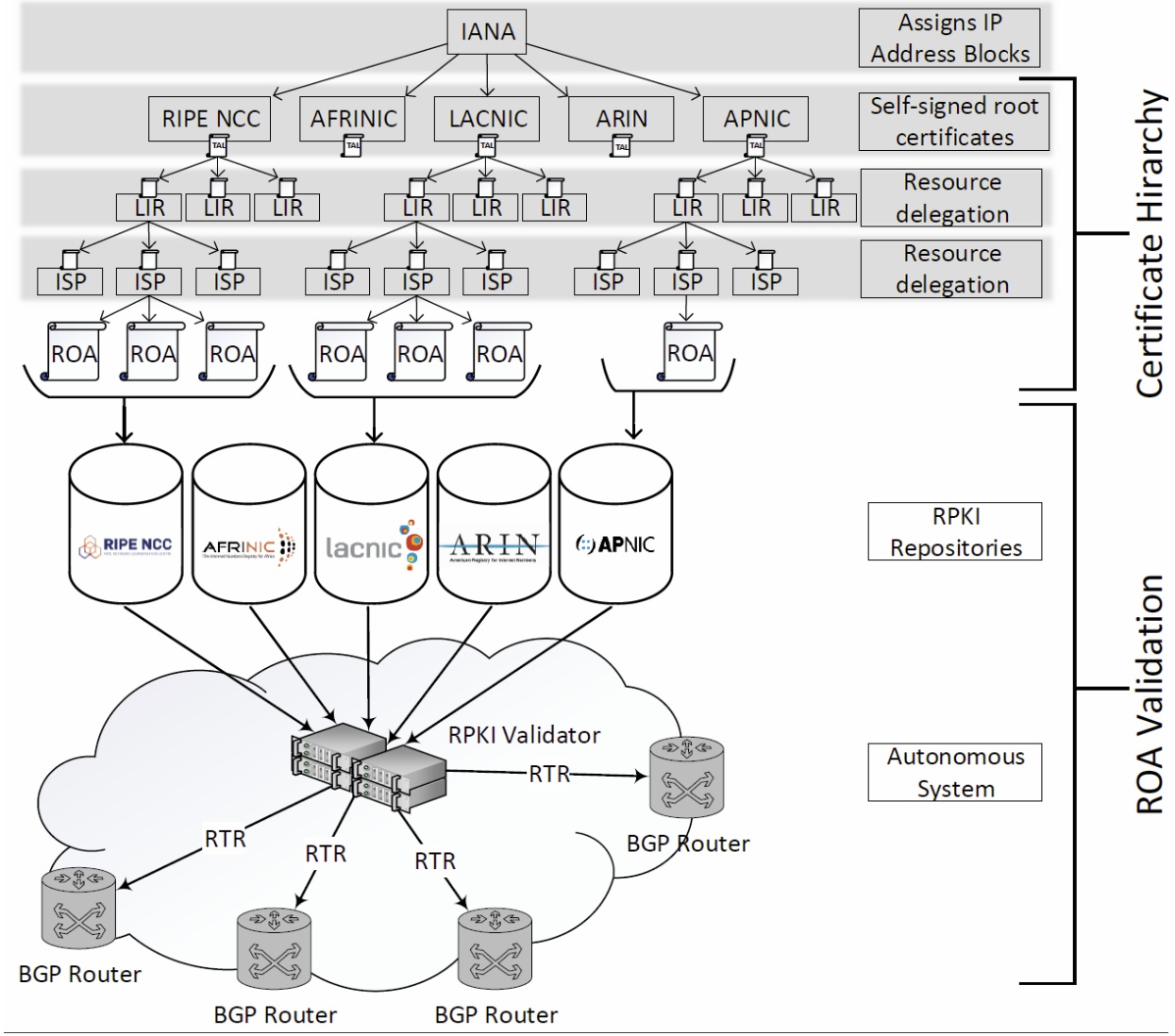
Solution: **R**esource **P**ublic **K**ey **I**nfrastructure

→ Each owner of an address space holds an end-entity certificate from the RIR (e.g. RIPE NCC). This will be used to sign **R**oute **O**rigin **A**uthorization objects. ROAs will be used by ASes to validate announcements.

The RPKI has two sides:

1) ROAs need to be created by resource owners
   → Exercise 1
2) ASes on the Internet need to perform Origin Validation and filter invalid announcements
   → Exercise 2

Introduction to RPKI – Origin Validation



RPKI – Resource Public Key Infrastructure

The Resource Public Key Infrastructure (RPKI) describes an approach to build a formally verifiable database of IP addresses and AS numbers as resources. [RFC6811]

The RPKI allows an AS to prove whether the origin AS of that announcement is indeed allowed to announce this prefix.

Introduction to RPKI – Route Origin Authorization

What is a ROA?

A ROA is an attestation that the holder of a set of prefixes has authorized an autonomous system to originate routes for those prefixes [RFC6480]. According to RFC6482, it contains:

1) Prefix
2) Max-Length
3) ASN

ROA | EE Cert

General Information	
Filename	eQh1l8EPvypzxzpyzU7ShUOtv1I.roa
ASN	31463
Signing Time	Mon, 24 Feb 2020 16:50:32 GMT
Location	rsync://rpki.ripe.net/repository/DEFAULT/28/5d5cc5-9d98-415a-ab0e-aa1481f0c13a/1/
Validity Period Start	Mon, 24 Feb 2020 16:50:32 GMT
Validity Period End	Thu, 01 Jul 2021 00:00:00 GMT
Validation Status	PASSED
Validation Errors	None
Validation Warnings	None

Prefixes	
Prefix	Max. Length
195.246.200.0/22	24
2a0d:12c0::/32	48

http://rpki-browser2.realmv6.org/

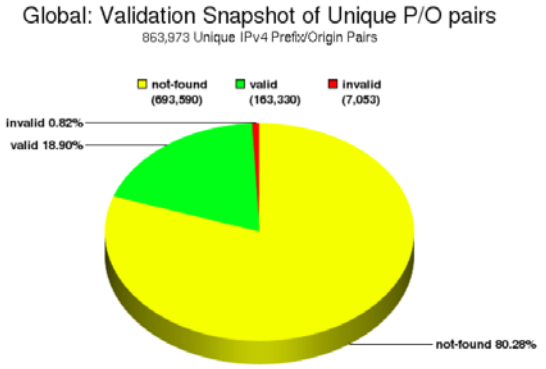
Nice tutorial to play around: https://www.securerouting.net/tutorial/

Introduction to RPKI – Exercise 1

How much of the address space is covered by RPKI?

Input:
- BGP Collector dump from 14th April
- Validated ROAs from 14th April 2020

Output:
- Distribution of valid / invalid / not found BGP announcements:



https://rpki-monitor.antd.nist.gov/

Methodology:
- Correlate the BGP data with the RPKI data to observe how many of the BGP announcements are protected. Simplification: Only look for exact prefix/ROA matches (do not look for covering ROAs)

Time: 15min

Introduction to RPKI – Exercise 1 – 15min

15:00

Questions: WebEx chat

Introduction to RPKI – ROV-enforcing ASes

- The first part was about identifying which share of address space is covered by RPKI.
- The second part will be about how many ASes actually use the information to drop invalid announcements.

Experiment types:

Uncontrolled
(passive)

- Uses preexisting data
- No control over ROAs
- No control over BGP announcements

→ Draw conclusions from observations that might change due to limited control

Controlled
(active)

- Generates data
- Controlling own ROAs
- Advertising own address space in BGP

→ Draw conclusions from observations we can influence

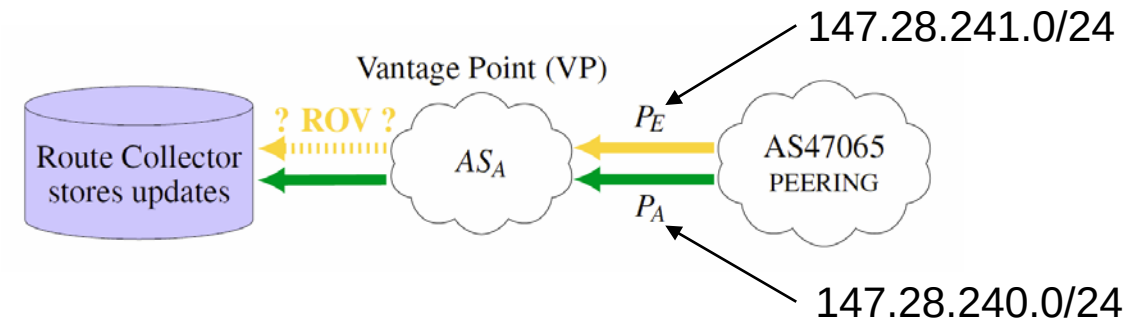
Introduction to RPKI – Controlled Experiments

BGP	RPKI
Announce prefixes P_A (Anchor) and P_E (Experiment)	**Issue ROAs for both prefixes**
✓ **Same RIR DB route object** ✓ **Same prefix length** ✓ **Announced at the same time** ✓ **Announced to same peers** ✓ **Announced from same origin AS**	**P_A announcement is always *valid*.** **Periodically change ROA for P_E :** ➢ **Flips announcement from *valid* to *invalid* to *valid* daily.**

Credit for slide content: Matthias Wählisch

Reuter, A., Bush, R., Cunha, I., Katz-Bassett, E., Schmidt, T.C. and Wählisch, M., 2018. Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering. *ACM SIGCOMM Computer Communication Review*, *48*(1), pp.19-27.

Introduction to RPKI – Controlled Experiments



Requirements:

1) Connectivity requirement: Each tested AS must be directly peering with PEERING*.
2) Visibility requirement: Each tested AS must be a Vantage Point (VP), e.g. export routes to RIS/Routeviews**.

Observation:

(O1) VP has the same route for both prefixes P_A and P_E → no ROV.
(O2) VP has a different route for prefix P_E → ROV @ AS on path.
(O3) VP has no route to P_E → ROV @ VP.

* https://peering.ee.columbia.edu/peers/

** http://routeviews.org/

Reuter, A., Bush, R., Cunha, I., Katz-Bassett, E., Schmidt, T.C. and Wählisch, M., 2018. Towards a rigorous methodology for measuring adoption of RPKI route validation and filtering. *ACM SIGCOMM Computer Communication Review*, *48*(1), pp.19-27.

Introduction to RPKI – Exercise 2

Which ASes perform Route-Origin-Validation?

Input:
- BGP Collector dump from 14th April (filtered for P_A + P_E)
- Knowledge that the ROA for P_E is swapped while for P_A it is not

Output:
- List of Route-Origin-Validation enforcing Ases:

```
('2020-04-14', '34224', '94.156.252.18', '147.28.240.0/24', '147.28.241.0/24')
('2020-04-14', '31019', '91.228.151.1', '147.28.240.0/24', '147.28.241.0/24')
('2020-04-14', '37100', '105.16.0.247', '147.28.240.0/24', '147.28.241.0/24')
('2020-04-14', '8492', '85.114.0.217', '147.28.240.0/24', '147.28.241.0/24')
('2020-04-14', '6939', '64.71.137.241', '147.28.240.0/24', '147.28.241.0/24')
```

Methodology:
- Work through the dataset and determine when a Vantage Point
  (1) while P_A was present and had a direct route
  (2) had a different route (or none at all) for P_E

Time: 20min

Introduction to RPKI – Exercise 2 – 20min

20:00

Questions: WebEx chat

Reliable measurements with BGP and RPKI – RECAP

- Introduction to BGP
  - What BGP is
  - How the protocol works
- Working with BGP data
  - What can you do with control plane data?
  - How can you collect data
  - Where to get readily available data
  - Data types
  - How to process and analyze data
- Introduction to RPKI
  - Origin Validation
  - RPKI aims at solving BGP Hijacking
  - RPKI hierarchy + ROA creation
- Measurements with RPKI data
  - How much prefix space is covered by RPKI?
  - Controlled vs. Uncontrolled Measurements
  - How many ASes are using the RPKI?

Mattijs Jonker, m.jonker@utwente.nl
Nils Rodday, nils.rodday@unibw.de