Network Architectures and Services
Faculty of Informatics
Technische Universität München, Germany

INVESTIGATING THE NATURE OF ROUTING ANOMALIES:
CLOSING IN ON SUBPREFIX HIJACKING ATTACKS

Johann Schlamp, Ralph Holz, Oliver Gasser, Andreas Korsten,
Quentin Jacquemart, Georg Carle, Ernst W. Biersack

– 7th International Workshop on Traffic Monitoring and Analysis –
April 24, 2015

MOTIVATION (I) – BLACKHOLING NETWORKS

Investigating the nature of routing anomalies

REGULAR PREFIX HIJACKING

REGULAR PREFIX HIJACKING

"Multi-Origin AS" (MOAS)

Investigating the nature of routing anomalies

"subMOAS"
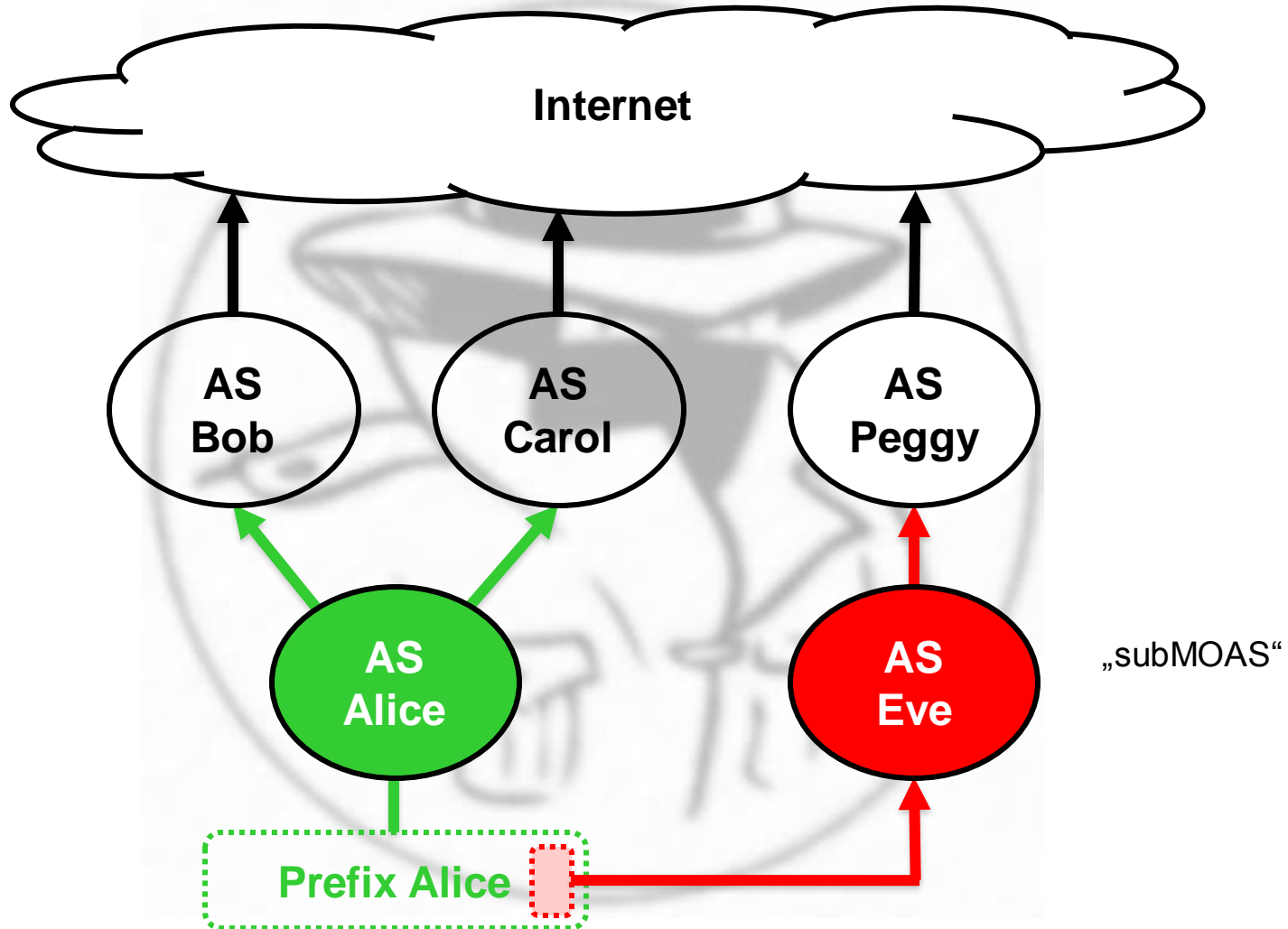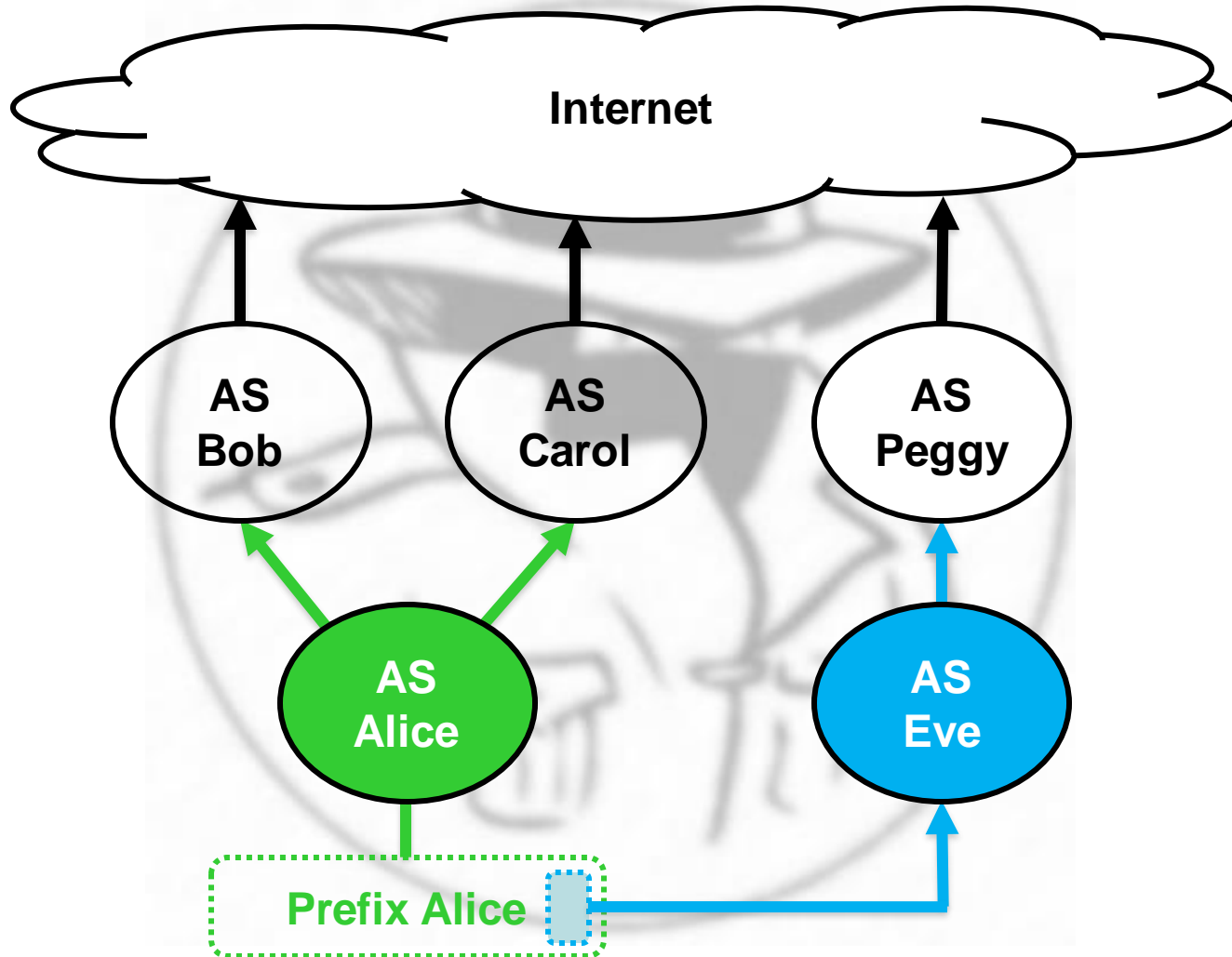
PROBLEM STATEMENT

- Detection of prefix hijacking is straightforward
  - Identify Multi-Origin ASes (MOAS), i.e. prefixes that are simultaneously announced by multiple ASes
  - Reduce false positives by drawing on orthogonal data

- What about subprefix hijacking?
  - On an ordinary day (June 1, 2014) we observed
    - → 511,118 announced prefixes (62.7% of IPv4)
    - → 76,121 subMOAS events (3.44% of IPv4)
  - We don't want to raise > 75k alarms every day!

- Let's investigate the nature of these „anomalies"

Measurement-based

OWNERSHIP VALIDATION

OUR APPROACH

- There is no ownership validation in BGP

- So let's built our own validation scheme to classify subMOAS events
  - Build a real-time framework to monitor BGP
  - Infer business relations and ownership info from publicly accessible Internet Routing Registries (IRR)
  - Utilize topology reasoning algorithms
  - Provide cryptographic assurance with SSL/TLS measurements

- We focus on finding legitimate subMOAS causes

□ We utilize daily RIPE database snapshots to extract legitimizing relations for any subMOAS

□ Our simplified database model (we use neo4j)
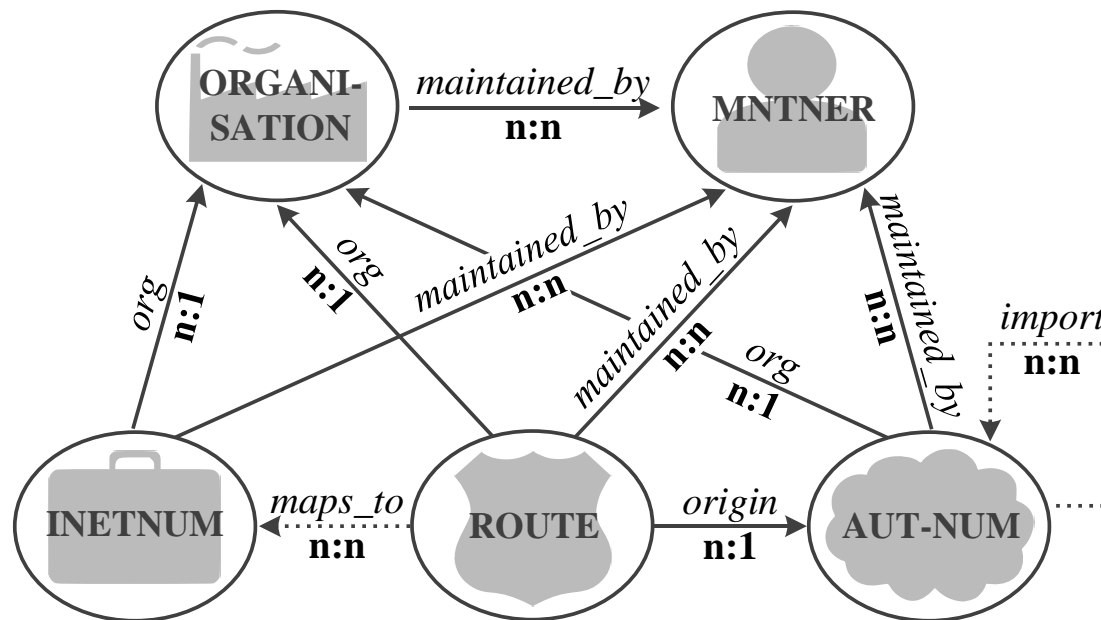
LEGITIMATE AS-TO-AS RELATION

❑ Legitimizing RIPE relations between two ASes

- Documented routing policy (import statements)
- Common maintainer
- Same organization

❑ Evidence for valid business relationships
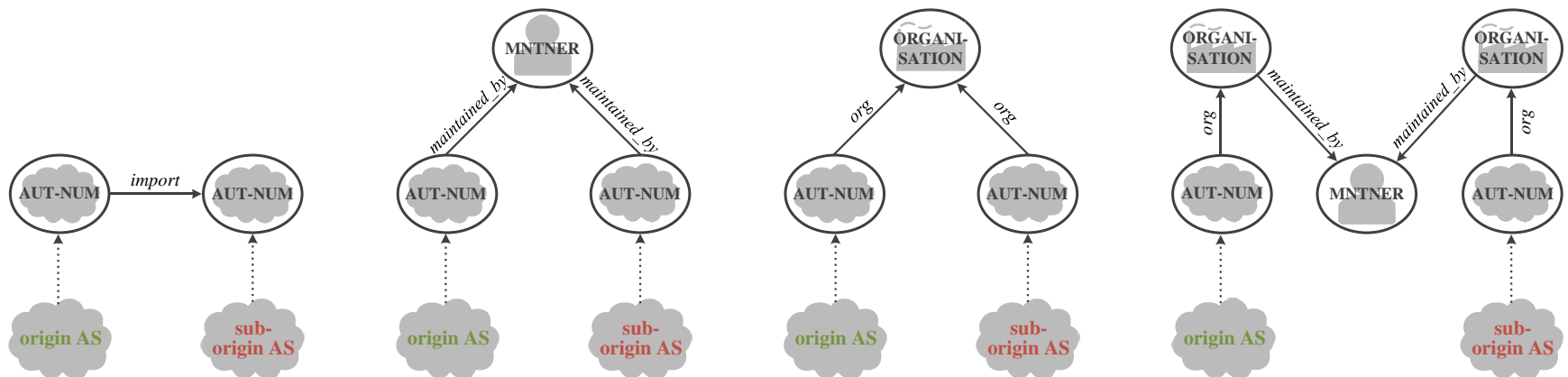
- Legitimizing RIPE relations for an AS and prefix
  - Route objects for the subprefix with valid AS origin
  - Same maintainer of the inetnum and sub-origin AS
  - Same organization of the inetnum and sub-origin AS

- Evidence for legitimate resource ownership

TOPOLOGY REASONING
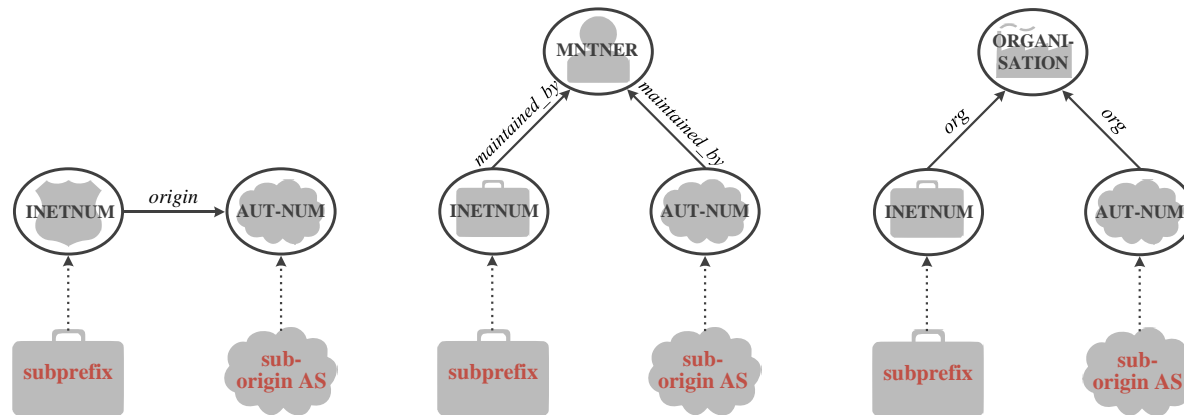
- Build a directed topology graph from all AS paths leading to affected subprefixes

- An attacker has little interest in hijacking his upstream ISP, since
  - The victim could easily filter out the attacker's malicious route updates
  - The victim could easily cut off the attacker completely

- If we observe the victim in an attacker's upstream path forwarding a subMOAS update, it can be safely considered legitimate

SSL/TLS MEASUREMENTS

☐ Basic idea

- We scan the entire Internet for active SSL/TLS hosts
- During a subMOAS event, we rescan affected hosts
- If the presented certificates are the same, it cannot be an attack (since we assume the attacker has no access to the victim's private keys)

☐ Ground truth has to be gathered in advance

| April 07, 2014 | **#1 SSL/TLS scan** all hosts IPv4-wide | April 24, 2014 | May 07, 2014 | **#2 SSL/TLS scan** active hosts from #1 | May 24, 2014 |

every 15 minutes

#3 subMOAS discard affected scans

A note on

SSL/TLS VALIDATION PERFORMANCE

SSL/TLS PERFORMANCE (I)

- ❒ Availability of SSL/TLS enabled hosts
  - ▪ For >75% of all events, we found more than one host
  - ▪ If at least one cryptographic key remains unchanged during an event, we can rule out an attack
  - ▪ For 25% of all events, we have more than ten hosts available, which increases robustness of our scans

- ❒ Obtaining a ground truth is intrusive
  - ▪ We scan „polite", i.e. slowly over a period of two weeks
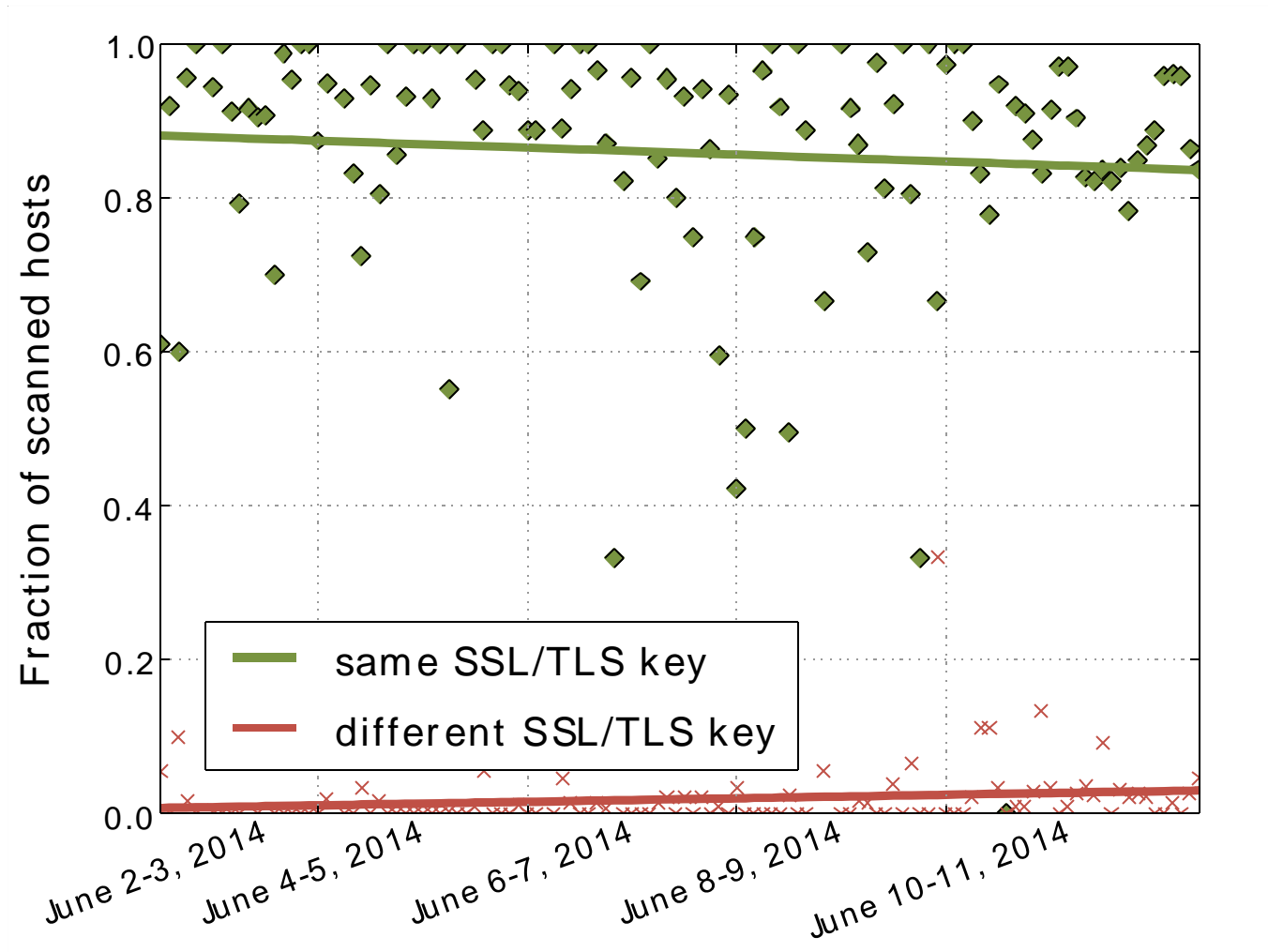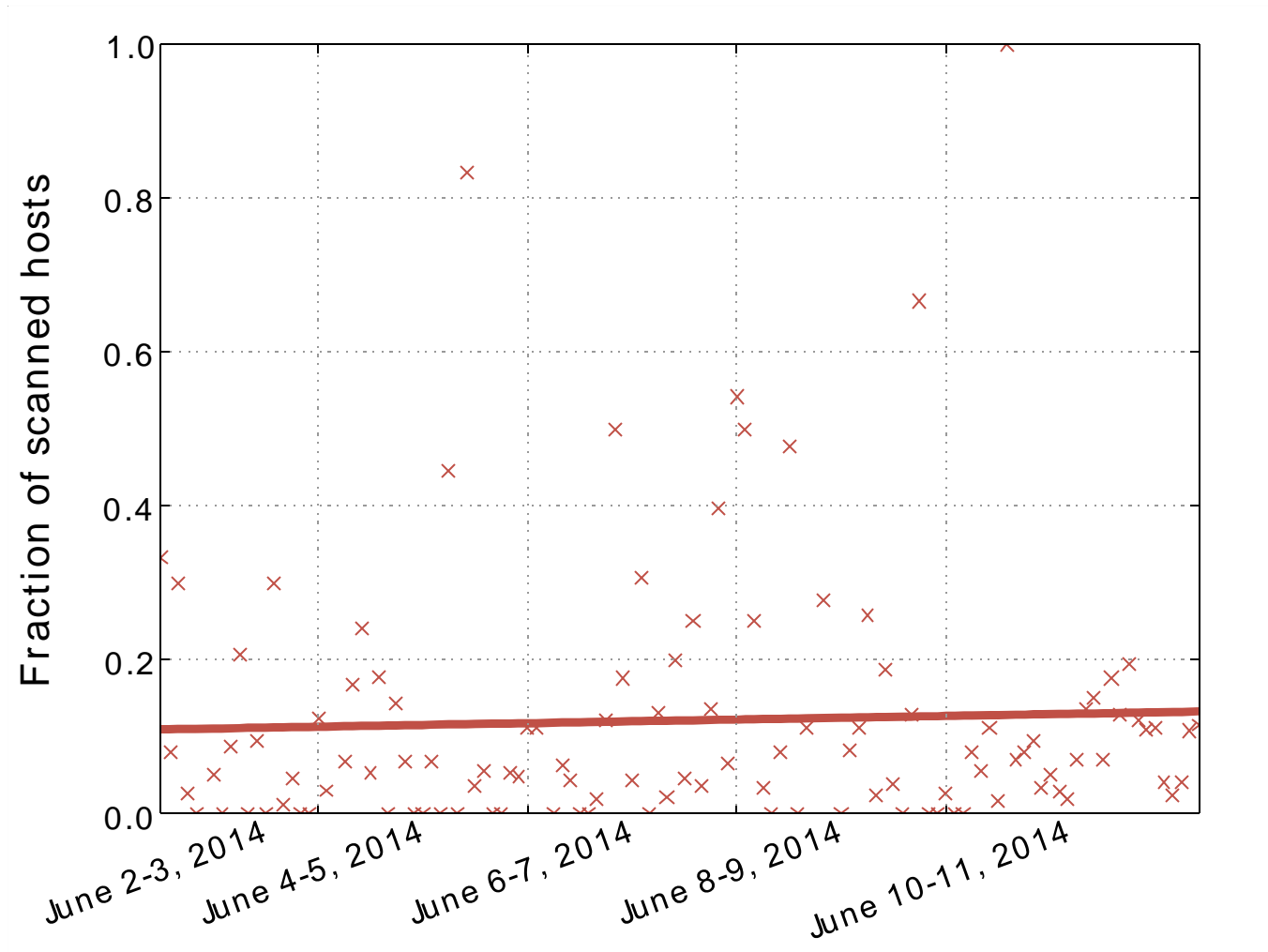 - ▪ The ground truth does not expire quickly (we can use it for months)
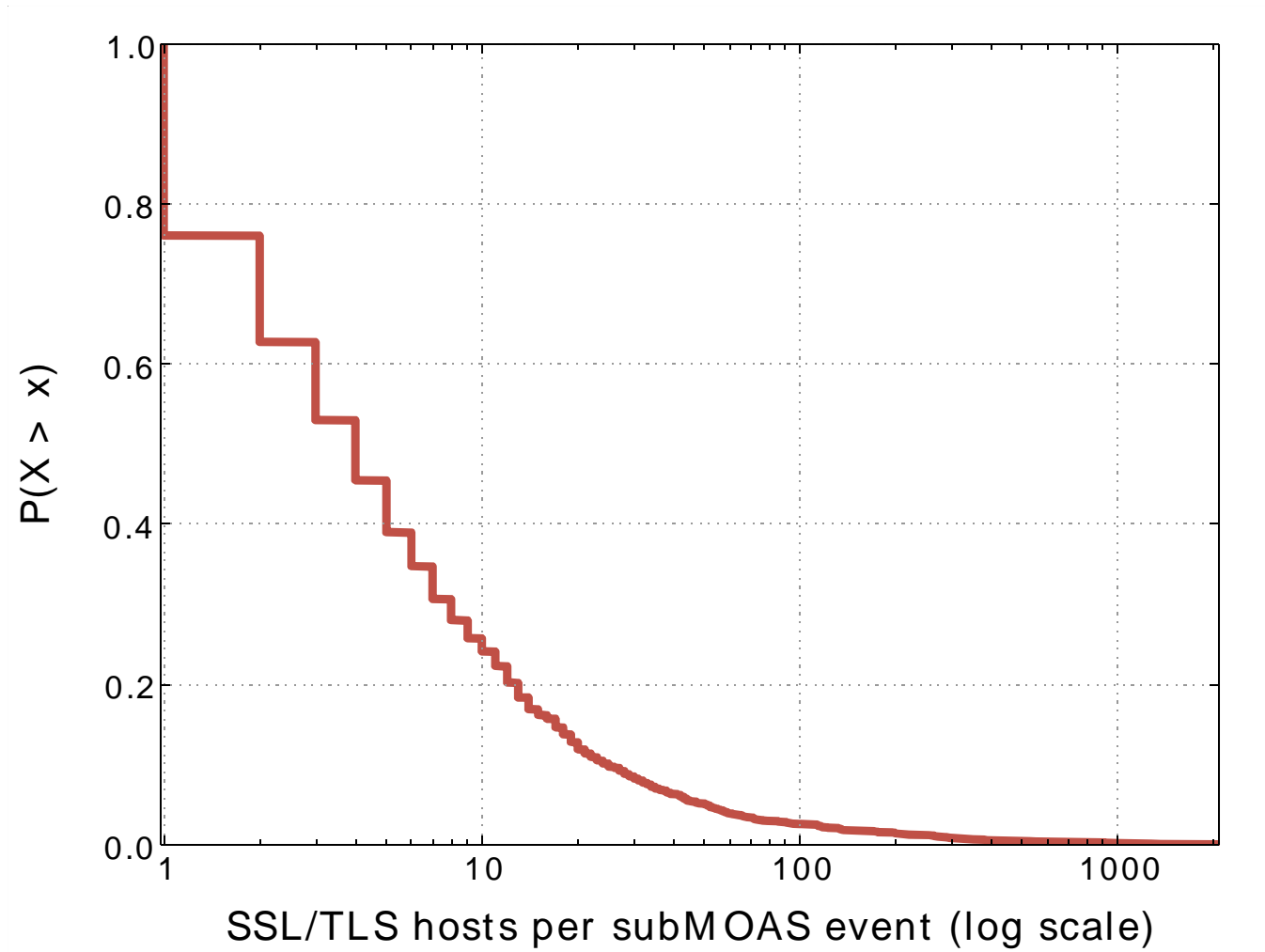
Investigating the nature of routing anomalies

UNRESPONSIVE SSL/TLS HOSTS OVER TIME

Investigating the nature of routing anomalies

Legitimized

SUBMOAS EVENTS

EVALUATION

❒ General observations

- Analysis period: June 2-12, 2014
- We only consider most specific subprefixes (since these are decisive for routing)
- This yields 74 subMOAS events per hour on average
- We investigated a total of 8,071 unique events

❒ Our data sources cover 60% of these events

- No inherent limitation of our approach
- Can be improved by adding further IRR sources (e.g. ARIN) and other scanned protocols (e.g. SSH, IMAPS)
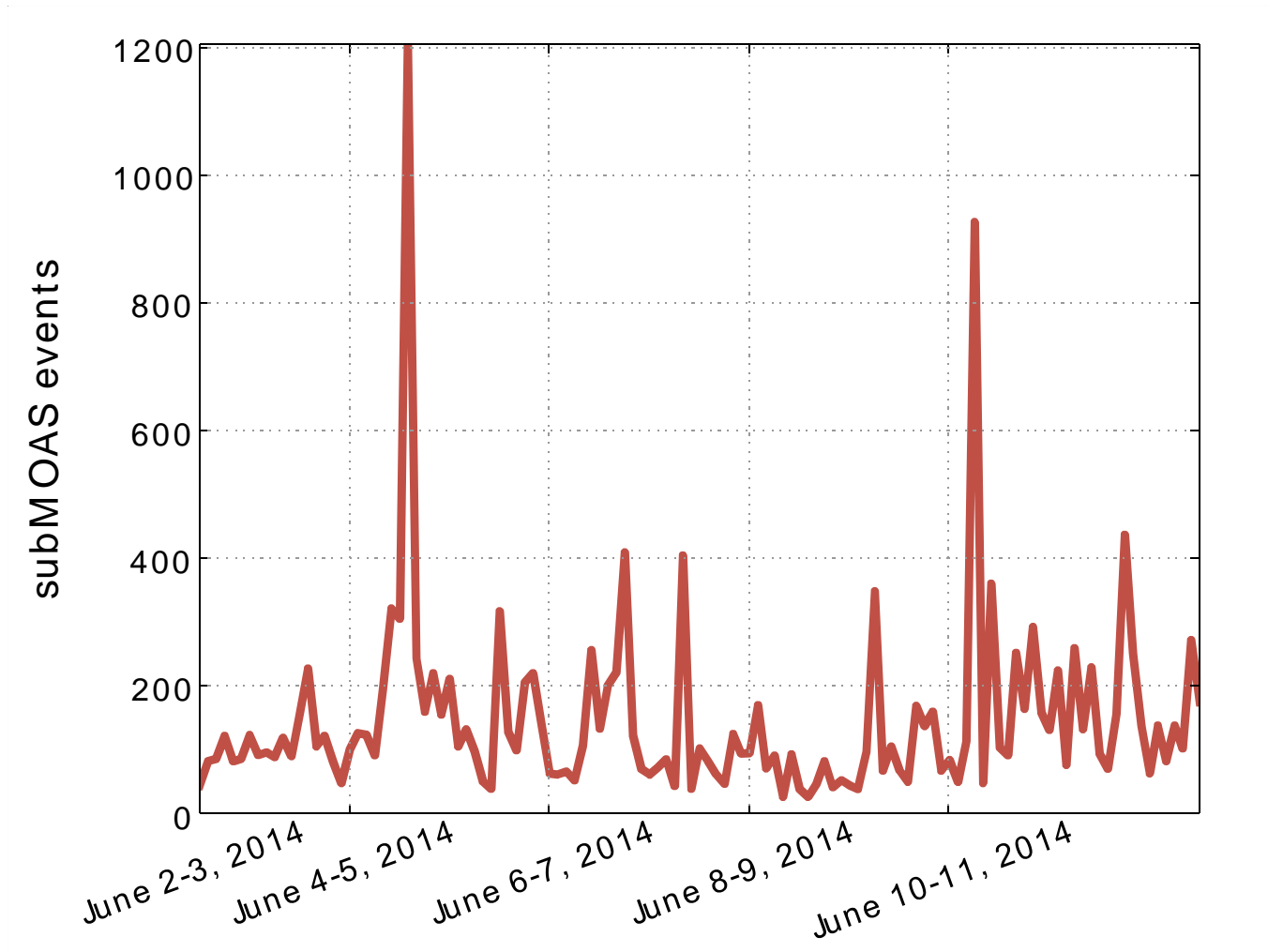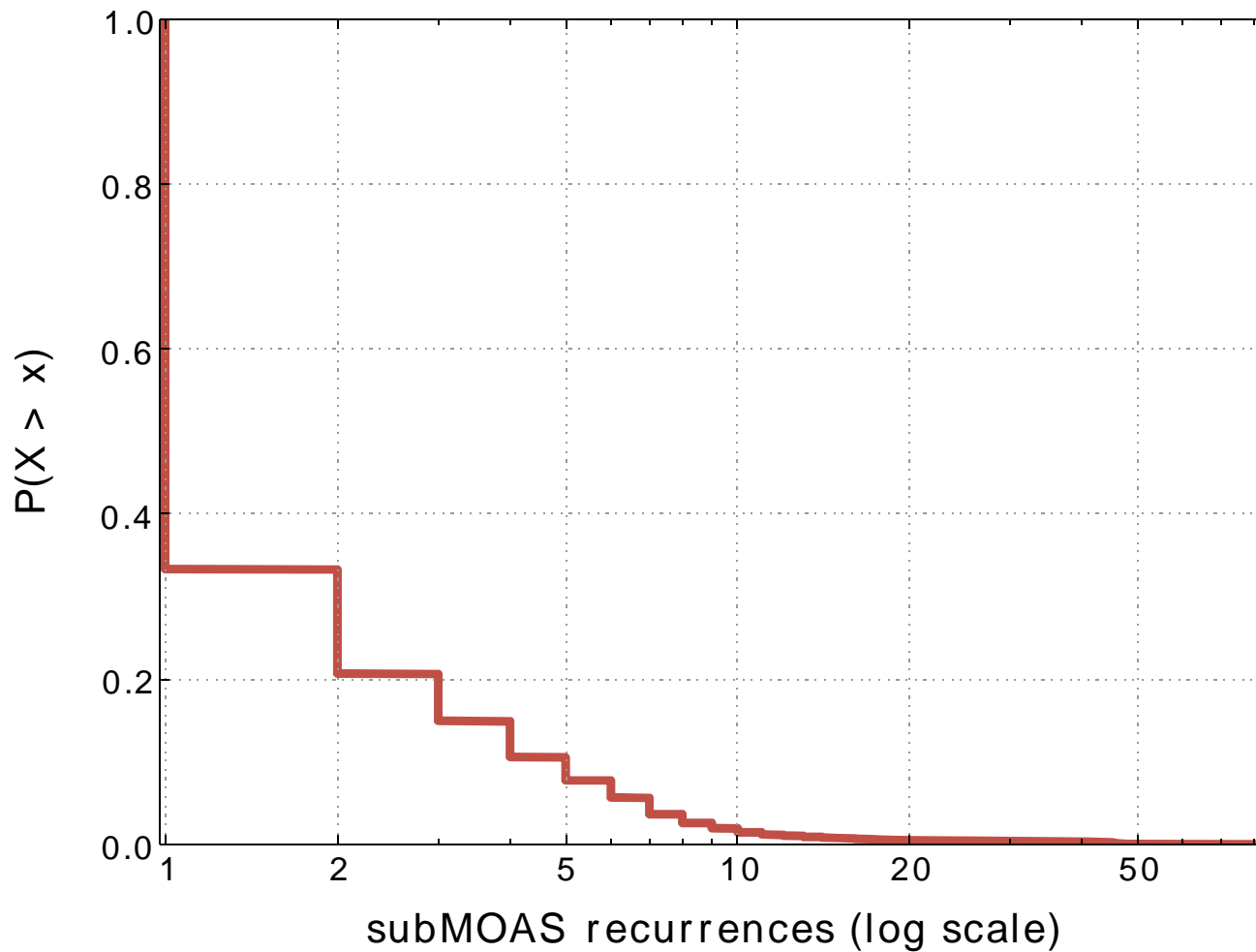
FINAL RESULTS

- We legitimized about 46% of all subMOAS events (while covering 60% with our data sources)

- Every legitimization step is relevant
  - Small overlap of results
  - Adding additional steps is reasonable

	total	percentage
All subMOAS events	**8,071**	**100.00%**
IRR analysis	870	10.78%
Topology reasoning	2,560	31.72%
SSL/TLS scans	1,851	22.93%
Legitimate events (cum.)	**3,755**	**46.53%**

CONCLUSION

- ❑ IRR databases are a valuable data source
  - ▪ Although possibly outdated, conclusive results can be obtained nevertheless
  - ▪ We plan to include other databases to increase the legitimization capabilities

- ❑ SSL/TLS scans can provide cryptographic insurance of network ownership

- ❑ We have developed a first step to narrow down the search space for subprefix hijacking attacks

THANK YOU!

Questions

Investigating the Nature of Routing Anomalies: Closing in on Subprefix Hijacking Attacks

Johann Schlamp, Ralph Holz, Oliver Gasser, Andreas Korsten, Quentin Jacquemart, Georg Carle, Ernst W. Biersack