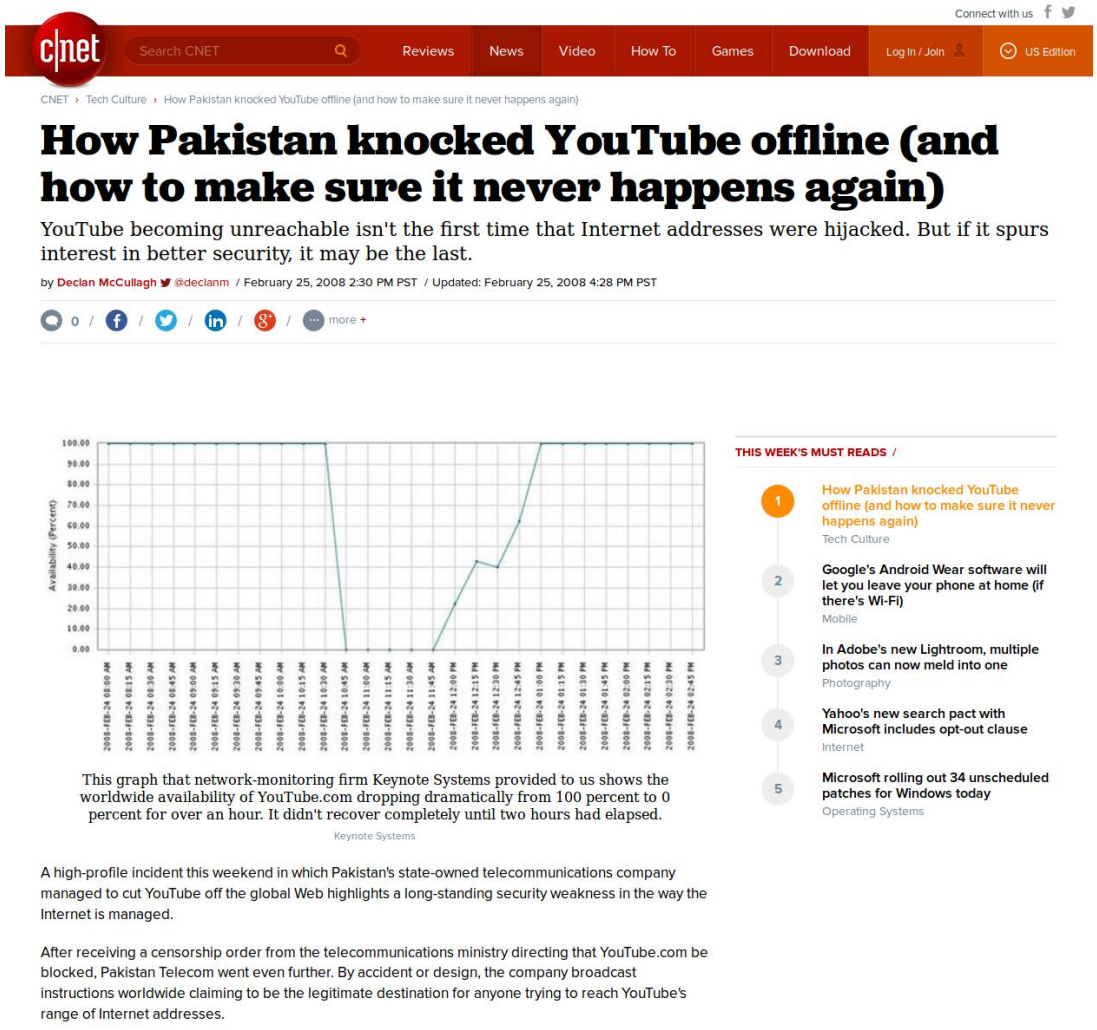
Network Architectures and Services
Faculty of Informatics
Technische Universität München, Germany

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



Connect with us

c|net Search CNET Reviews News Video How To Games Download Log In / Join US Edition

CNET › Tech Culture › How Pakistan knocked YouTube offline (and how to make sure it never happens again)

How Pakistan knocked YouTube offline (and how to make sure it never happens again)

YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.

by Declan McCullagh @declanm / February 25, 2008 2:30 PM PST / Updated: February 25, 2008 4:28 PM PST

0 / / / / / more +

This graph that network-monitoring firm Keynote Systems provided to us shows the worldwide availability of YouTube.com dropping dramatically from 100 percent to 0 percent for over an hour. It didn't recover completely until two hours had elapsed.

Keynote Systems

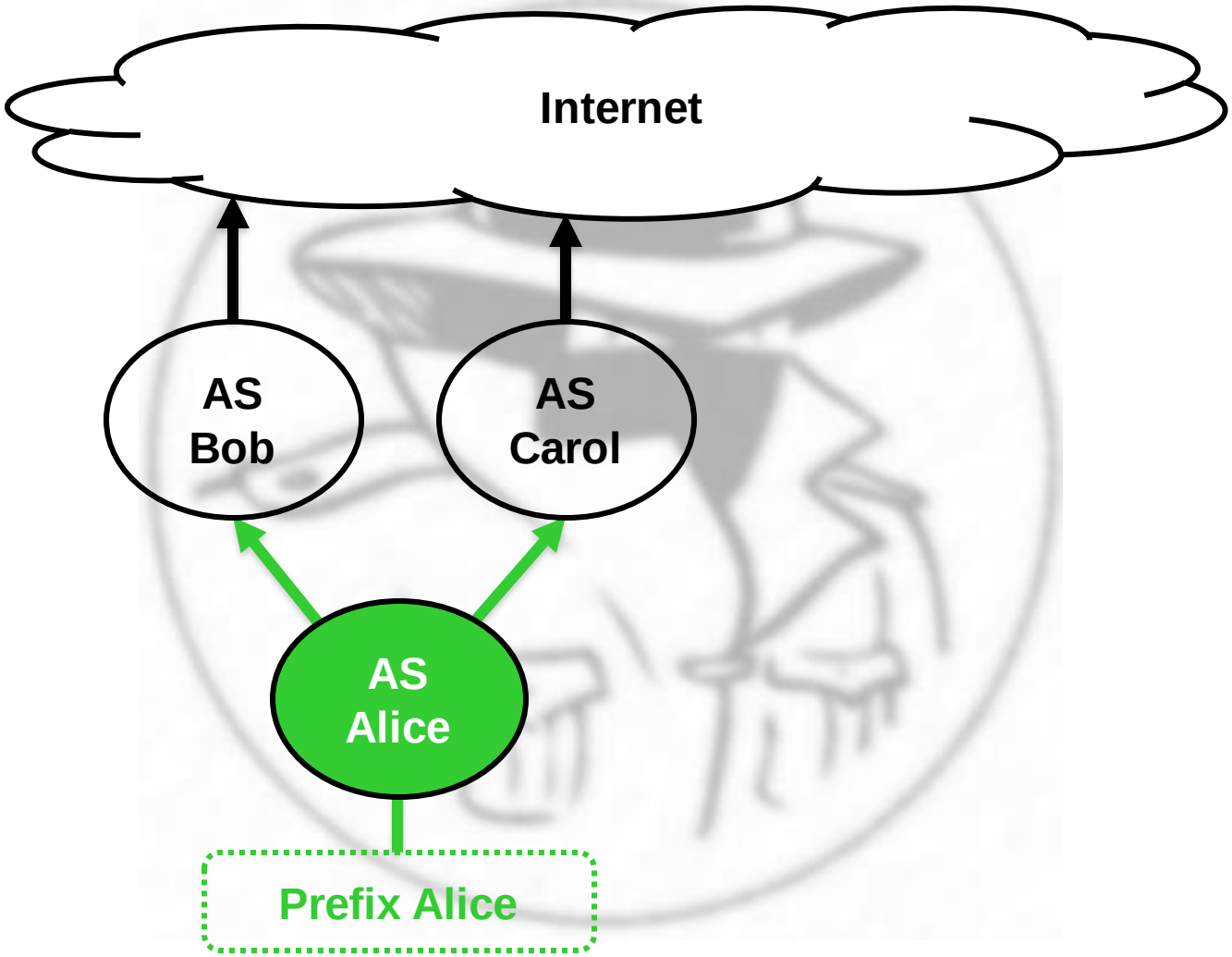
A high-profile incident this weekend in which Pakistan's state-owned telecommunications company managed to cut YouTube off the global Web highlights a long-standing security weakness in the way the Internet is managed.

After receiving a censorship order from the telecommunications ministry directing that YouTube.com be blocked, Pakistan Telecom went even further. By accident or design, the company broadcast instructions worldwide claiming to be the legitimate destination for anyone trying to reach YouTube's range of Internet addresses.

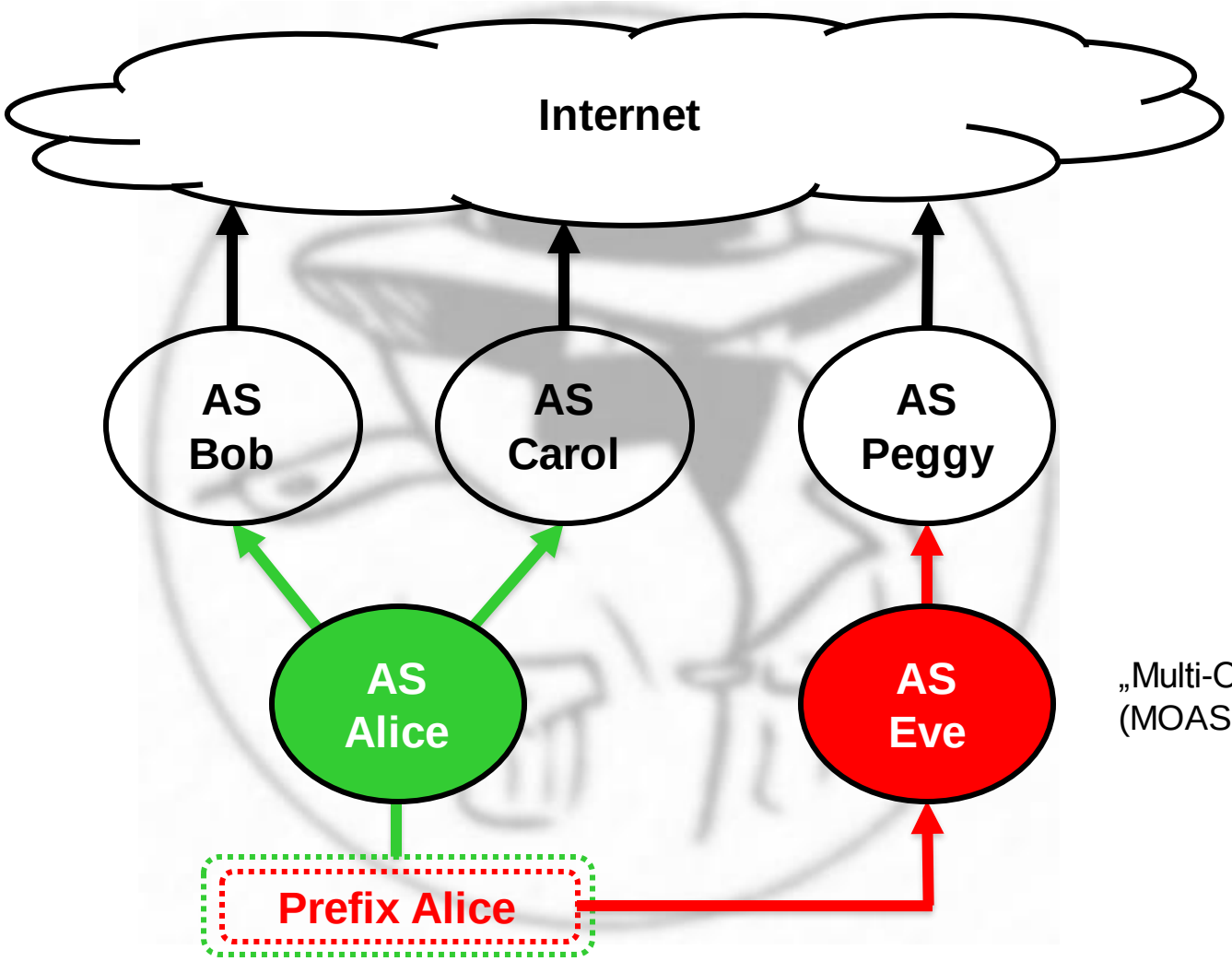
THIS WEEK'S MUST READS /

1. How Pakistan knocked YouTube offline (and how to make sure it never happens again) — Tech Culture
2. Google's Android Wear software will let you leave your phone at home (if there's Wi-Fi) — Mobile
3. In Adobe's new Lightroom, multiple photos can now meld into one — Photography
4. Yahoo's new search pact with Microsoft includes opt-out clause — Internet
5. Microsoft rolling out 34 unscheduled patches for Windows today — Operating Systems

Regular Prefix Hijacking

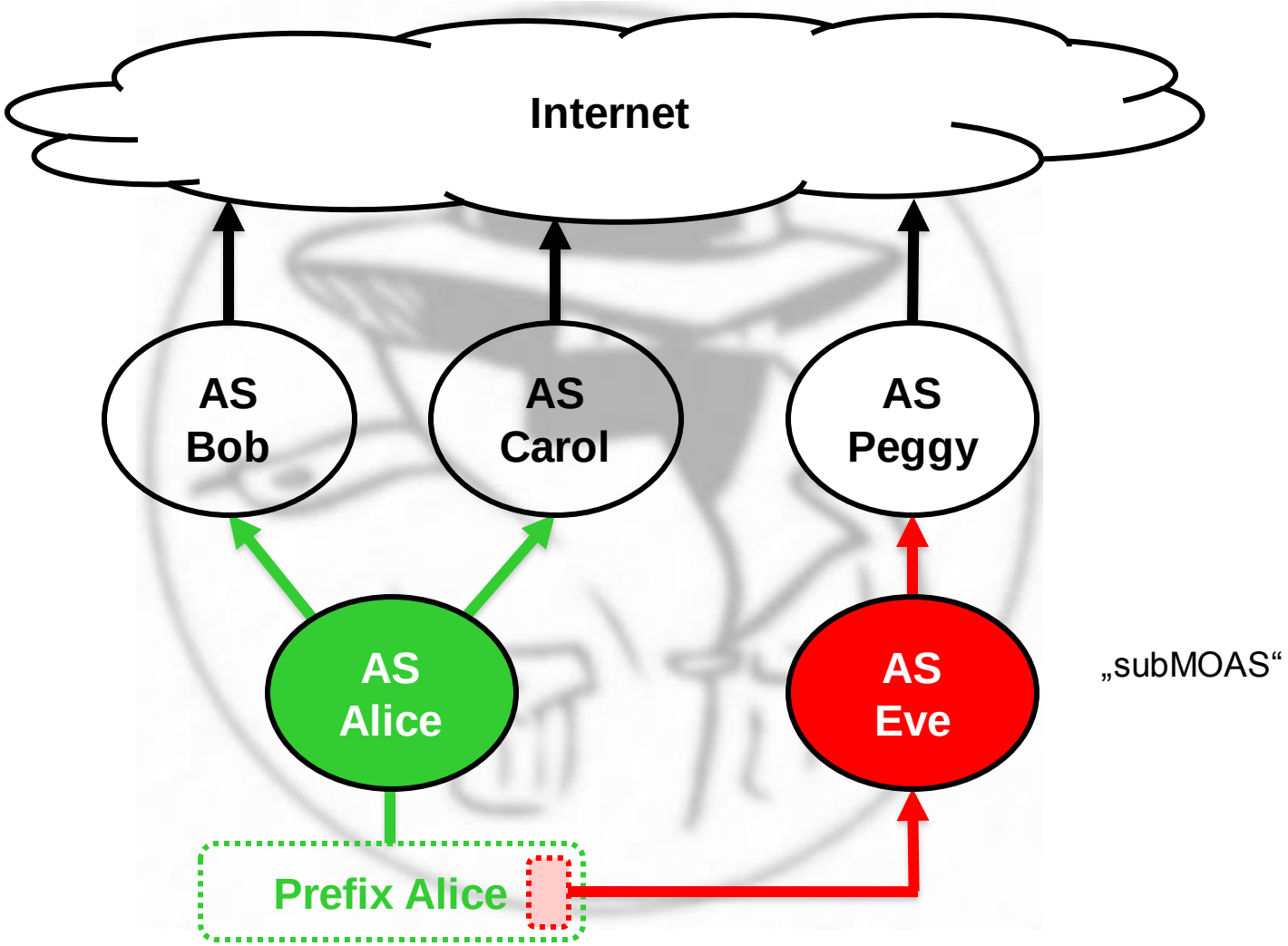


Regular Prefix Hijacking

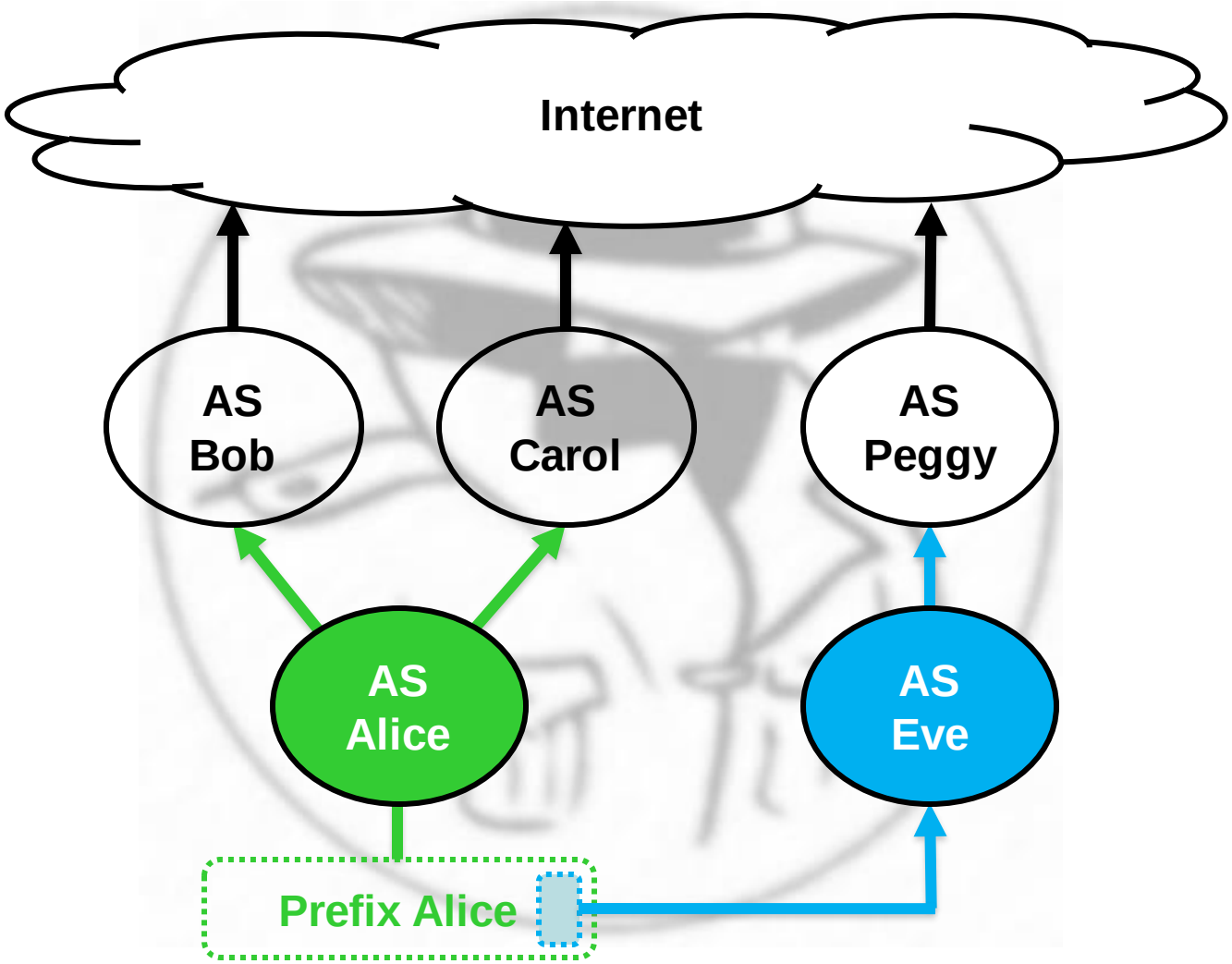


„Multi-Origin AS“ (MOAS)

SUBPREFIX HIJACKING



Regular ISP Business



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

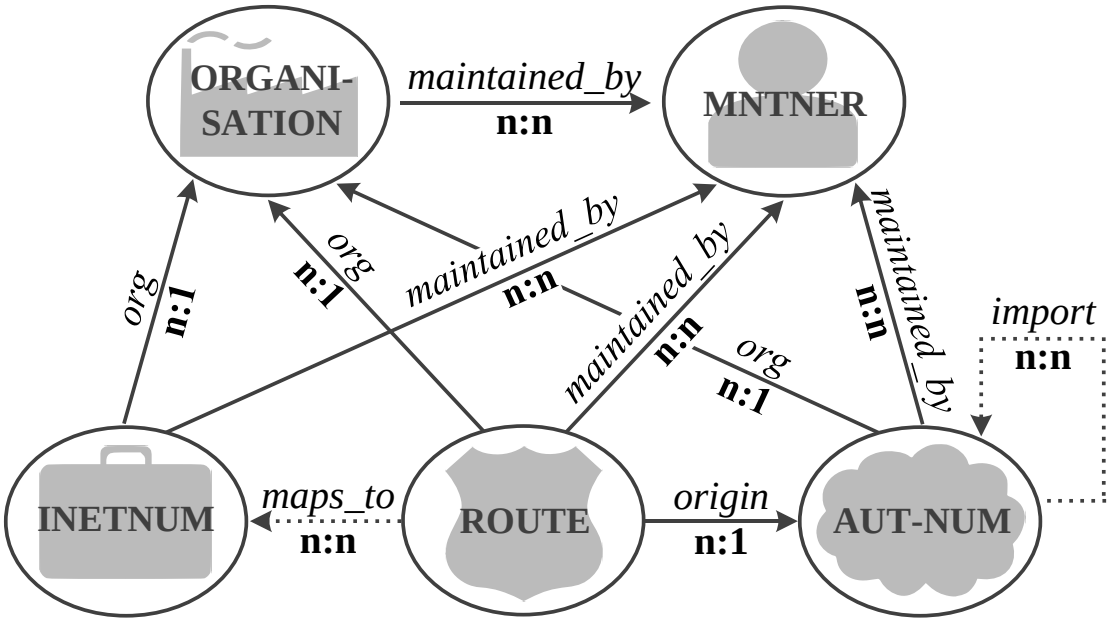
OWNERSHIP VALIDATION

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

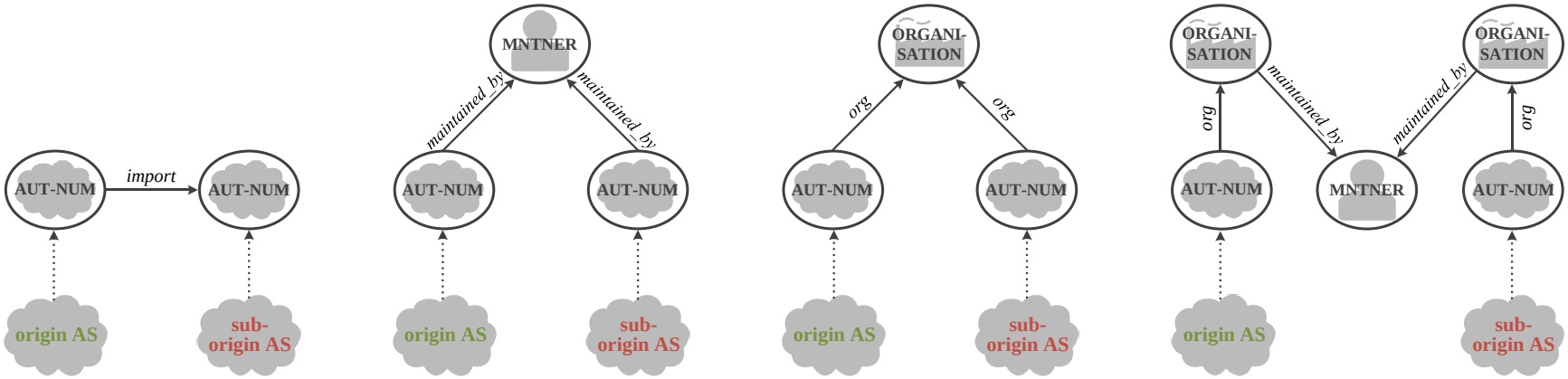
IRR Analysis

- We utilize daily RIPE database snapshots to extract legitimizing relations for any subMOAS
- Our simplified database model (we use neo4j)



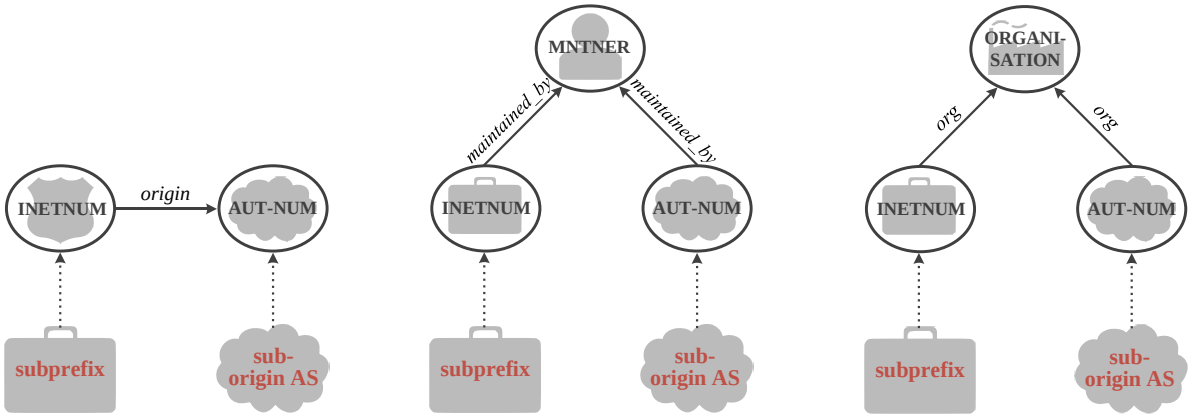
LEGITIMATE AS-TO-AS RELATION

- Legitimizing RIPE relations between two ASes
  - Documented routing policy (import statements)
  - Common maintainer
  - Same organization
- Evidence for valid business relationships



LEGITIMATE SUBPREFIX OWNERSHIP

- 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

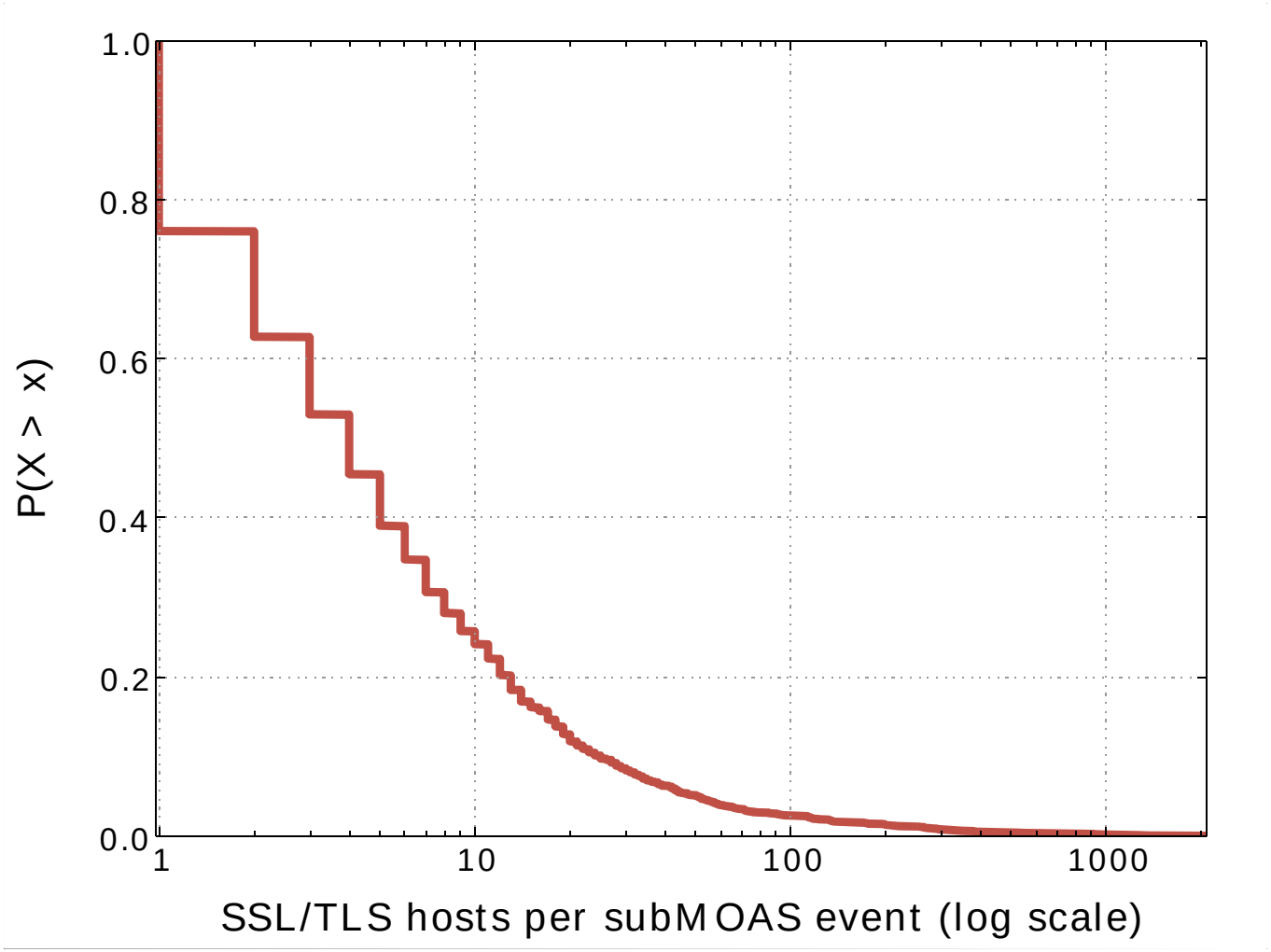
A note on

SSL/TLS Validation Performance

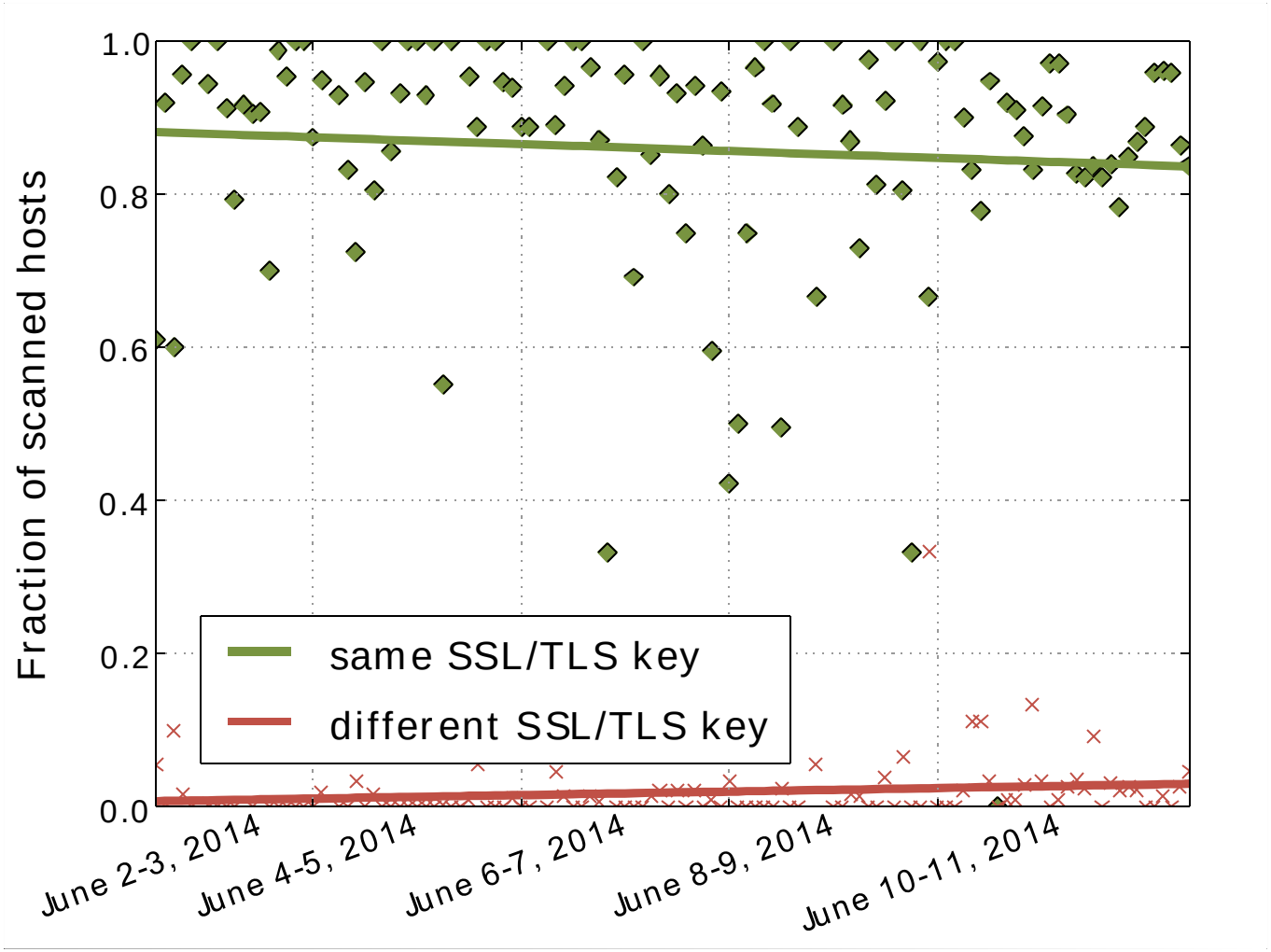
SSL/TLS Performance (I)

- 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)

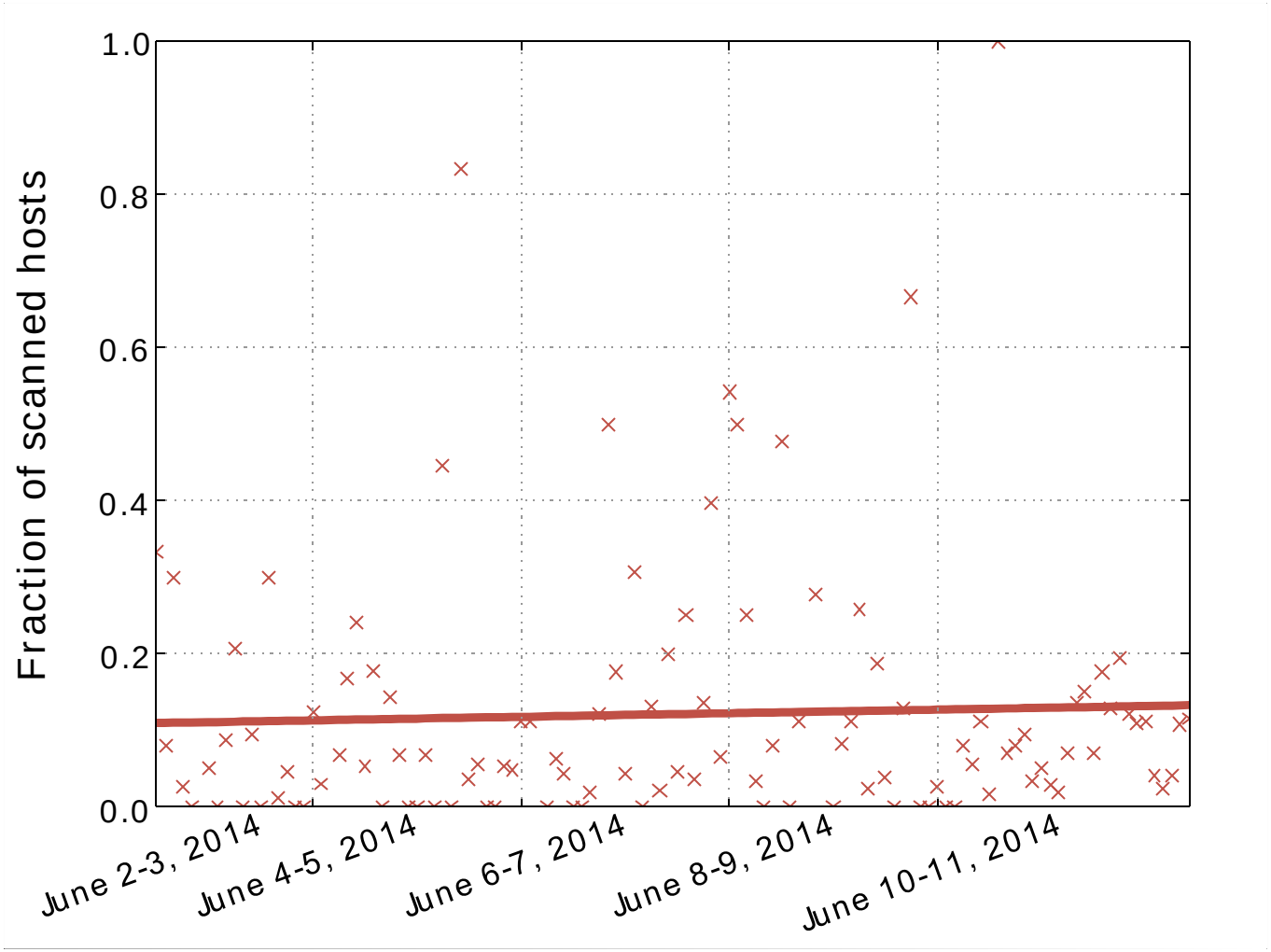
Number of Available SSL/TLS Hosts per Event



Natural Change of SSL/TLS Keys



Unresponsive SSL/TLS Hosts over Time



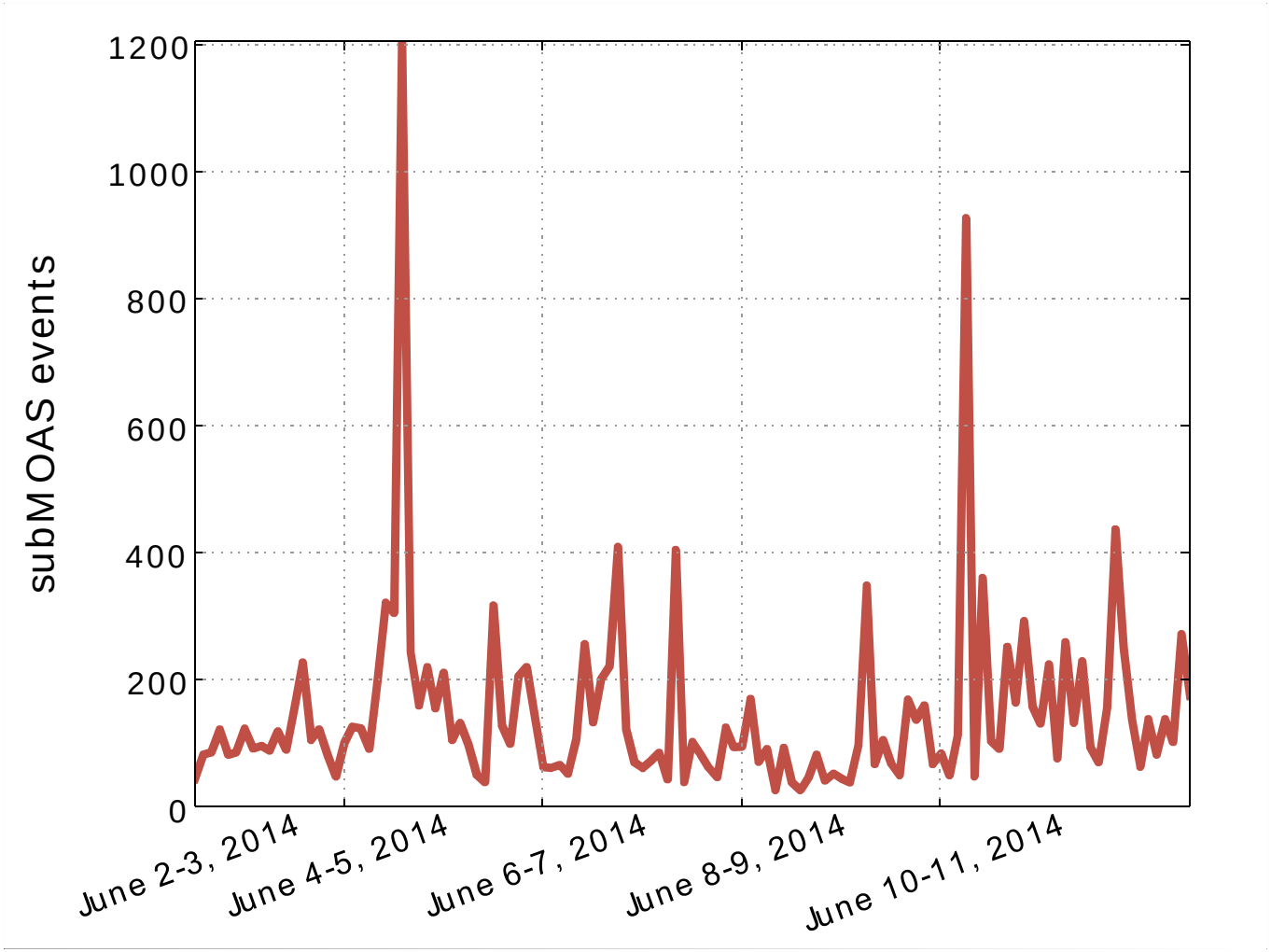
Legitimized

SubMOAS Events

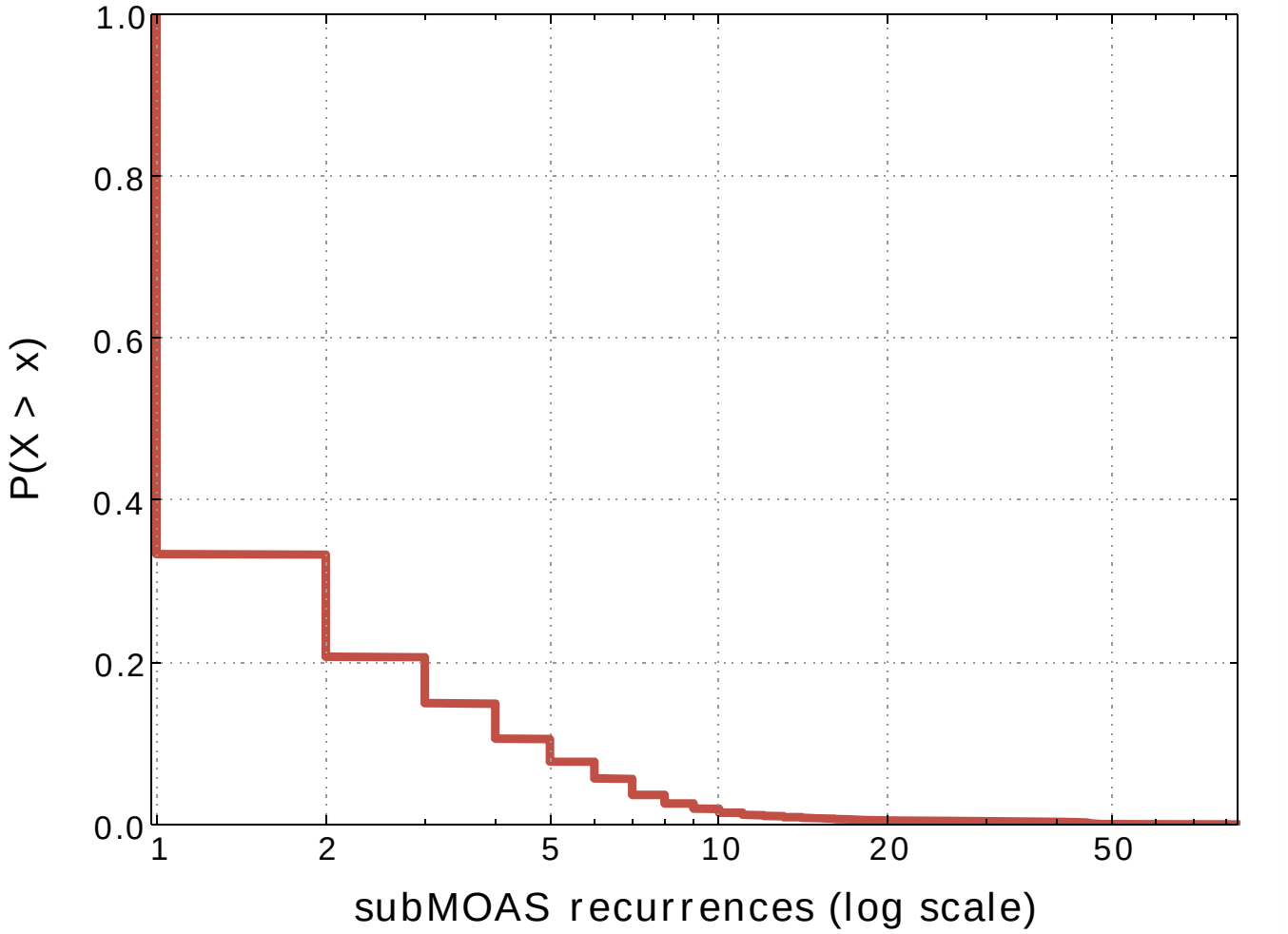
EVALUATION

- 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)

OBSERVED SUBMOAS



RECURRING SUBMOASES



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