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

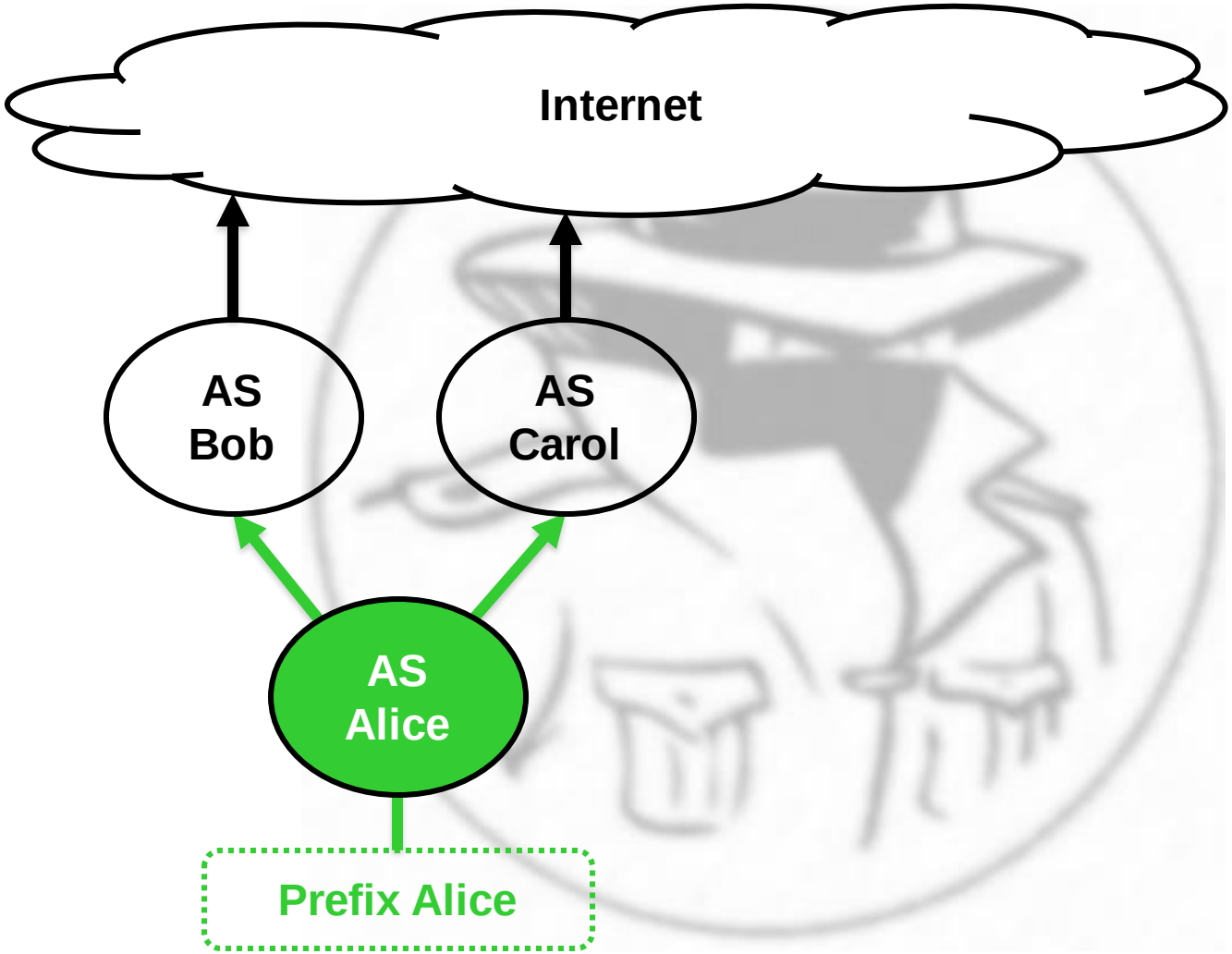
THE ABANDONED SIDE OF THE INTERNET: HIJACKING INTERNET RESOURCES WHEN DOMAIN NAMES EXPIRE

Johann Schlamp, Josef Gustafsson, Matthias Wählisch,
Thomas C. Schmidt, Georg Carle

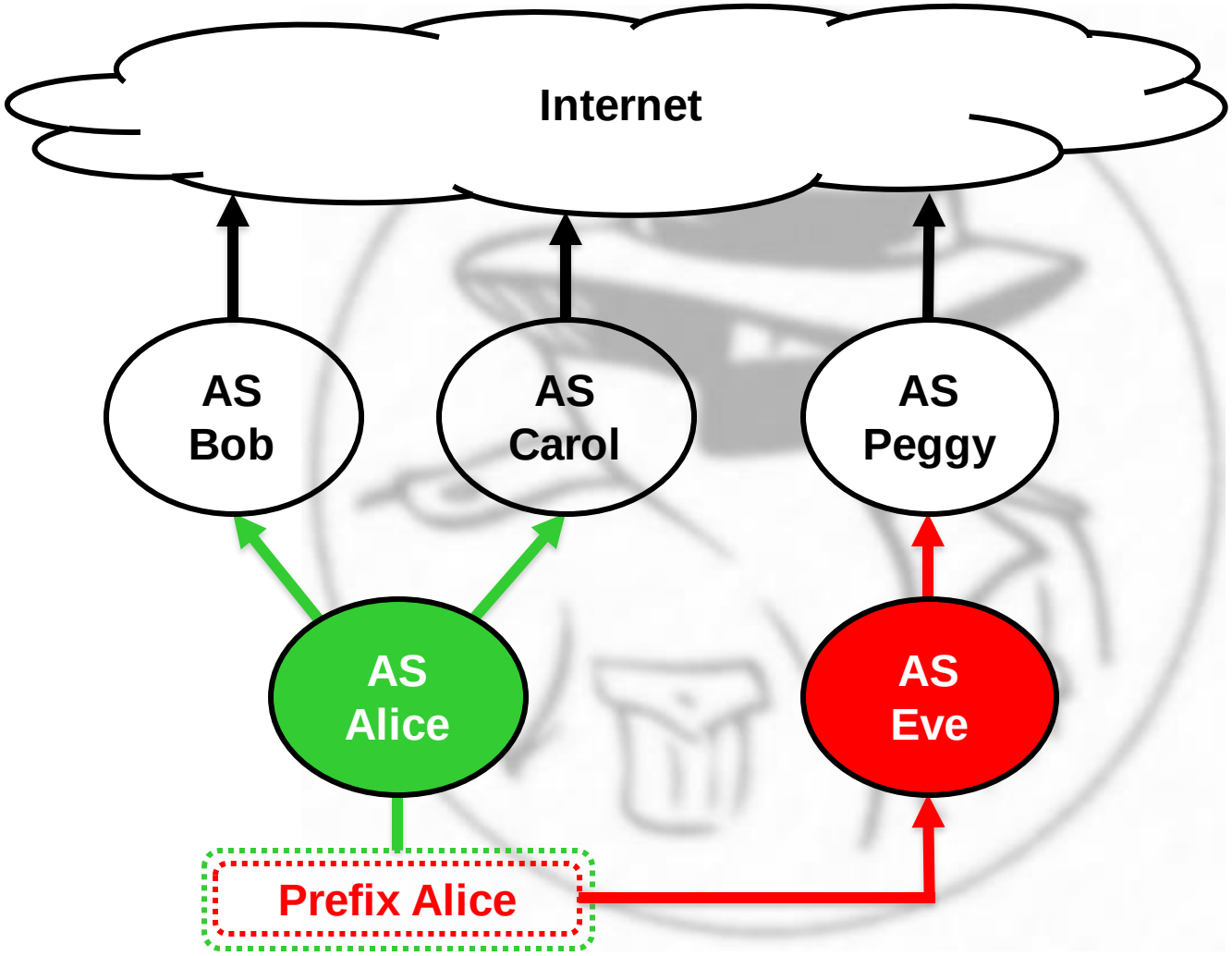
– 7th International Workshop on Traffic Monitoring and Analysis –
April 24, 2015

Motivation (I) – Long-Term Abuse of Prefixes

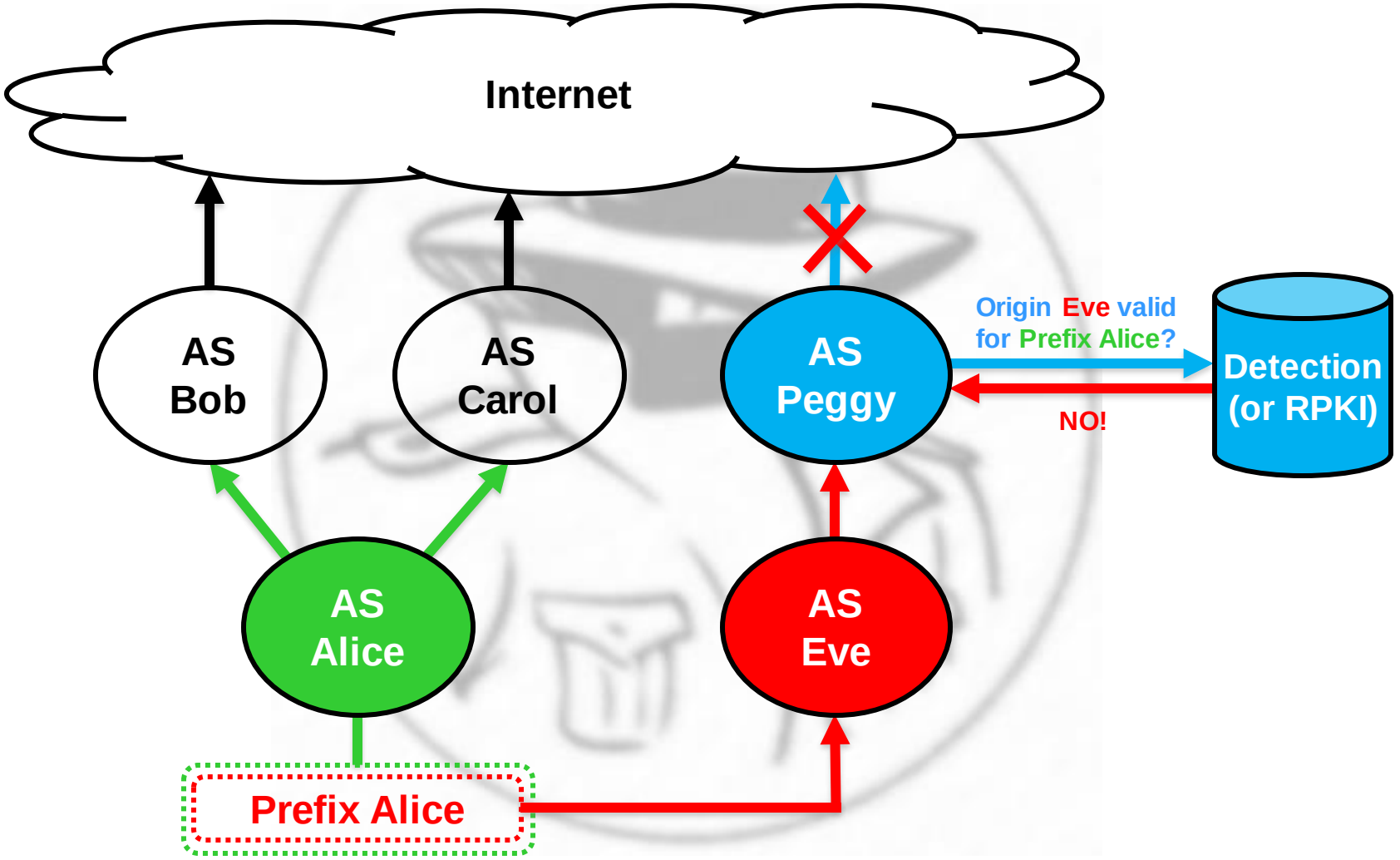
Regular Prefix Hijacking



Regular Prefix Hijacking



Regular Prefix Hijacking with RPKI

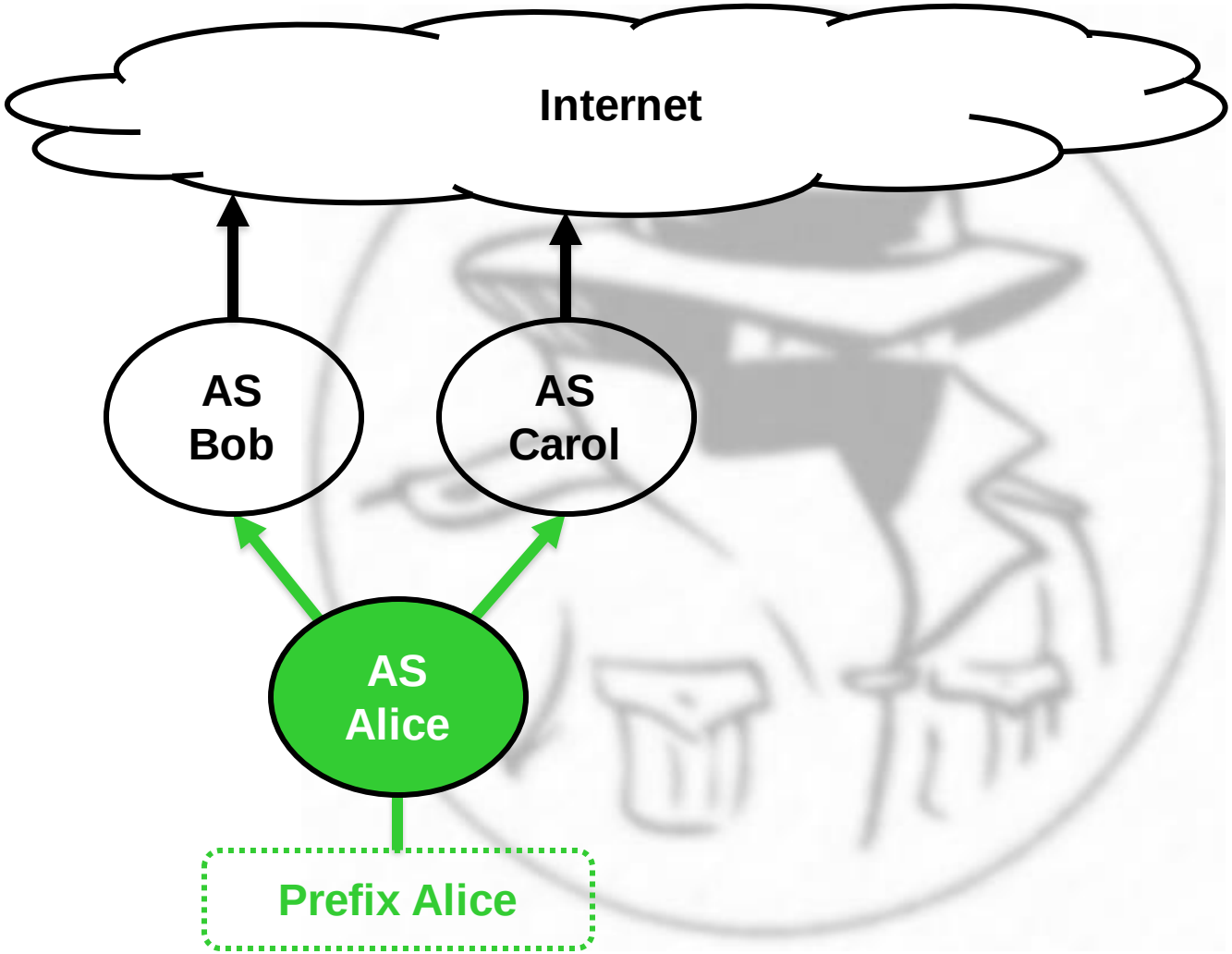


Motivation (II) – The LinkTel Incident

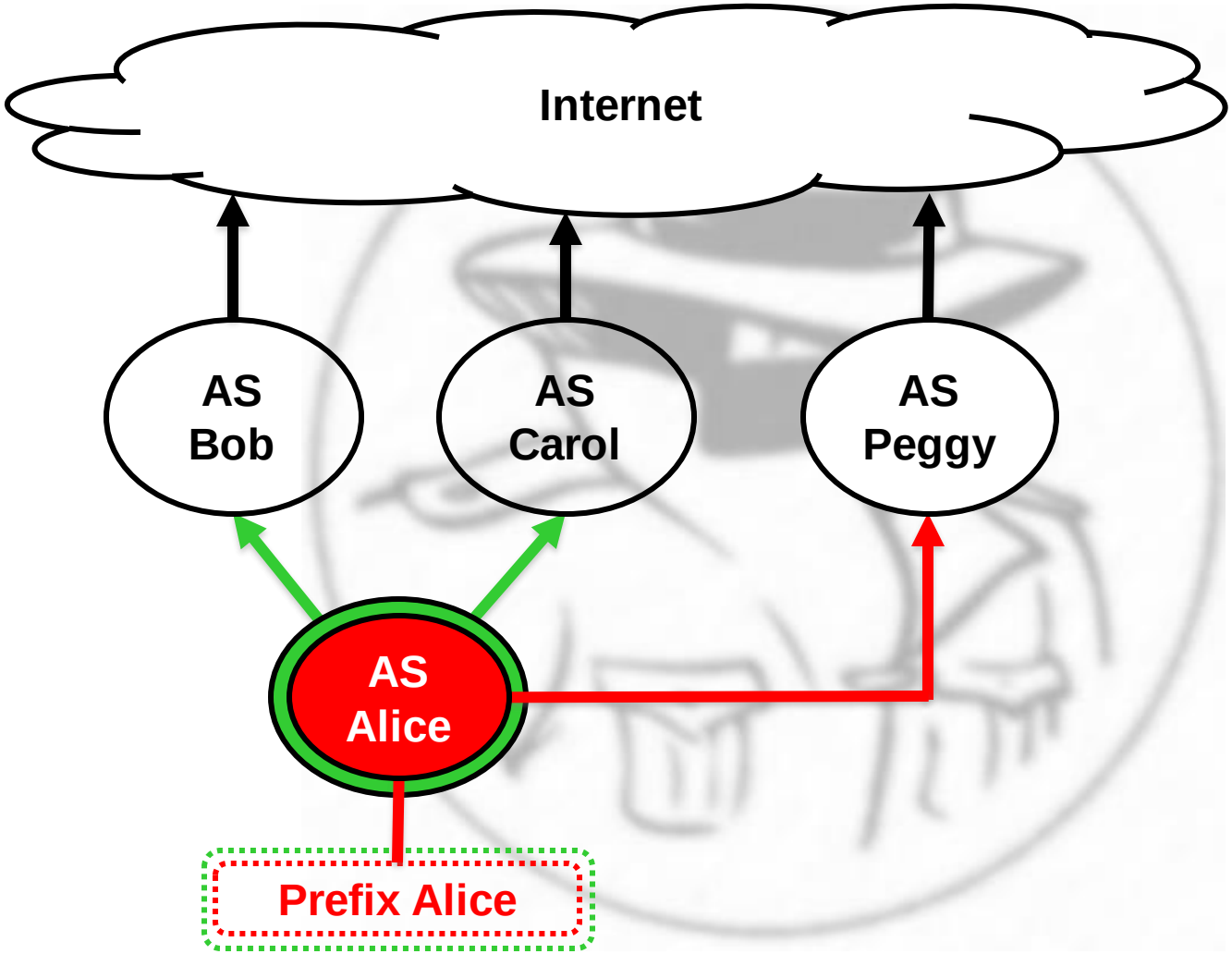
- A new hijacking attack [1]
  - SOS to NANOG from a Russian ISP under attack
  - Unnoticed for 6 months due to business struggles
  - Forensic analysis of the incident one year later
- Complex attack plan with a hand-picked target
  - The victim‘s DNS domain had expired, which enabled administrative take-over of its Internet resources
  - No BGP activity for the victim‘s IP prefixes, which enabled stealthy hijack of the prefixes and the AS

[1] J. Schlamp, G. Carle, and E. W. Biersack. A forensic case study on AS hijacking: the attacker‘s perspective. *ACM SIGCOMM CCR*, 43(2):5-12, 2013.

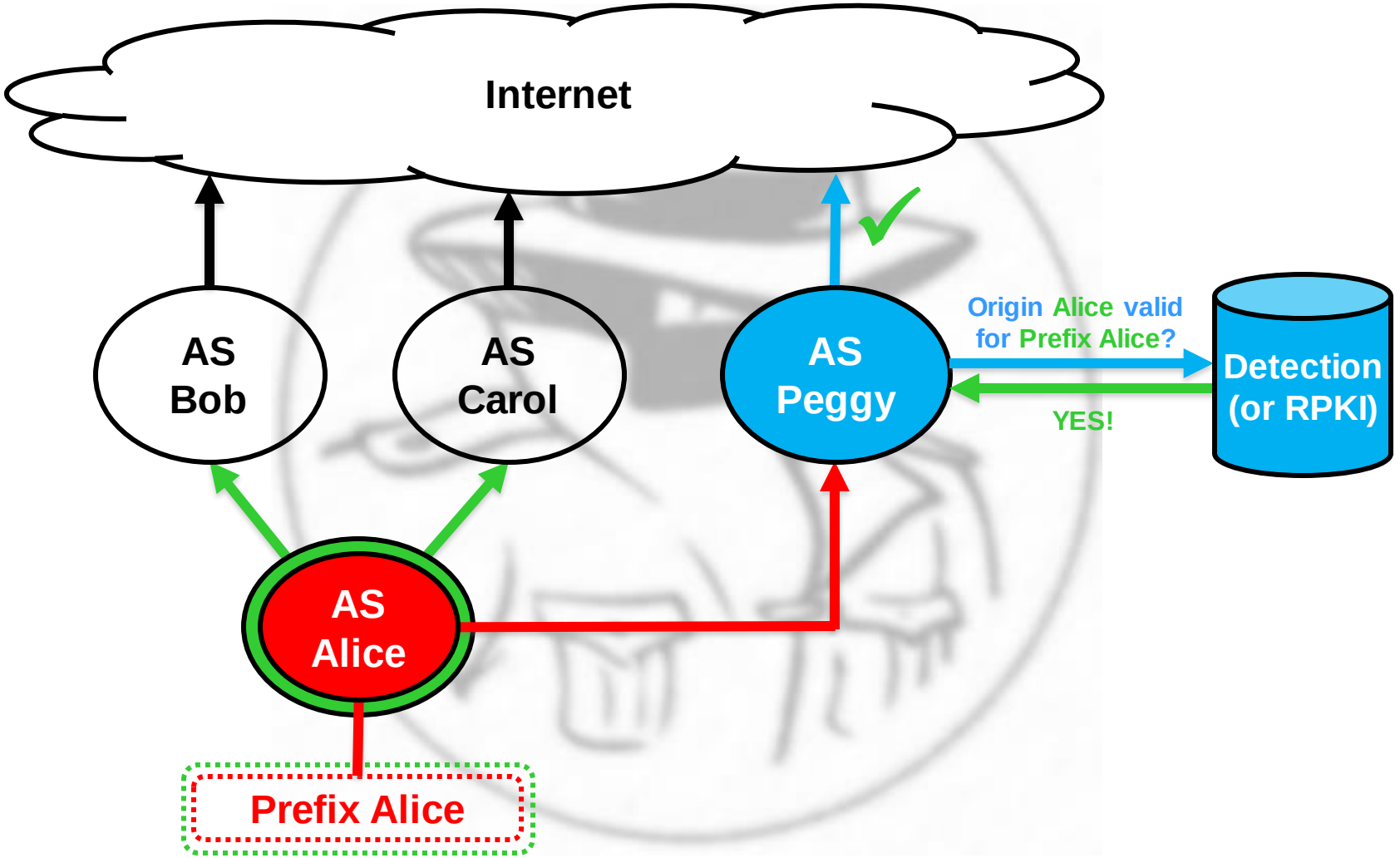
AS HIJACKING



AS HIJACKING



AS HIJACKING WITH RPKI



Identification of

Abandoned Internet Resources

Preconditions for Successful Attacks

- Today, origin validation is based on
  - ISP info in Internet Routing Registries (IRR)
  - Social exchange (email conversation)
  - IRR entries binding an AS to a prefix
- Imagine a company going (temporarily) out of business. Eventually, without cash flow…
  - Its DNS domain is going to expire
  - Its BGP activity terminates
  - Its IRR entries remain!

What we are looking for

- Given this knowledge, an attacker can easily impersonate a hand-picked victim by
  - Re-registration of the DNS domain
  - Claiming ownership and misleading any upstream ISP
- Our approach is similar
  - Find resource groups under same administration
  - Identify groups that reference expired domains only
  - Cross-check time of last IRR update
  - Take into account BGP history
  - Evaluate gain (e.g. number of abandoned prefixes)

Detailed

TECHNICAL APPROACH

The RIPE Database

- RIPE maintains an IRR database for the European service region
  - Daily snapshots are available (mostly anonymized)
  - We analyzed 2.5 years of archived snapshots (Feb 23, 2012 – July 9, 2014)
- Example data objects:

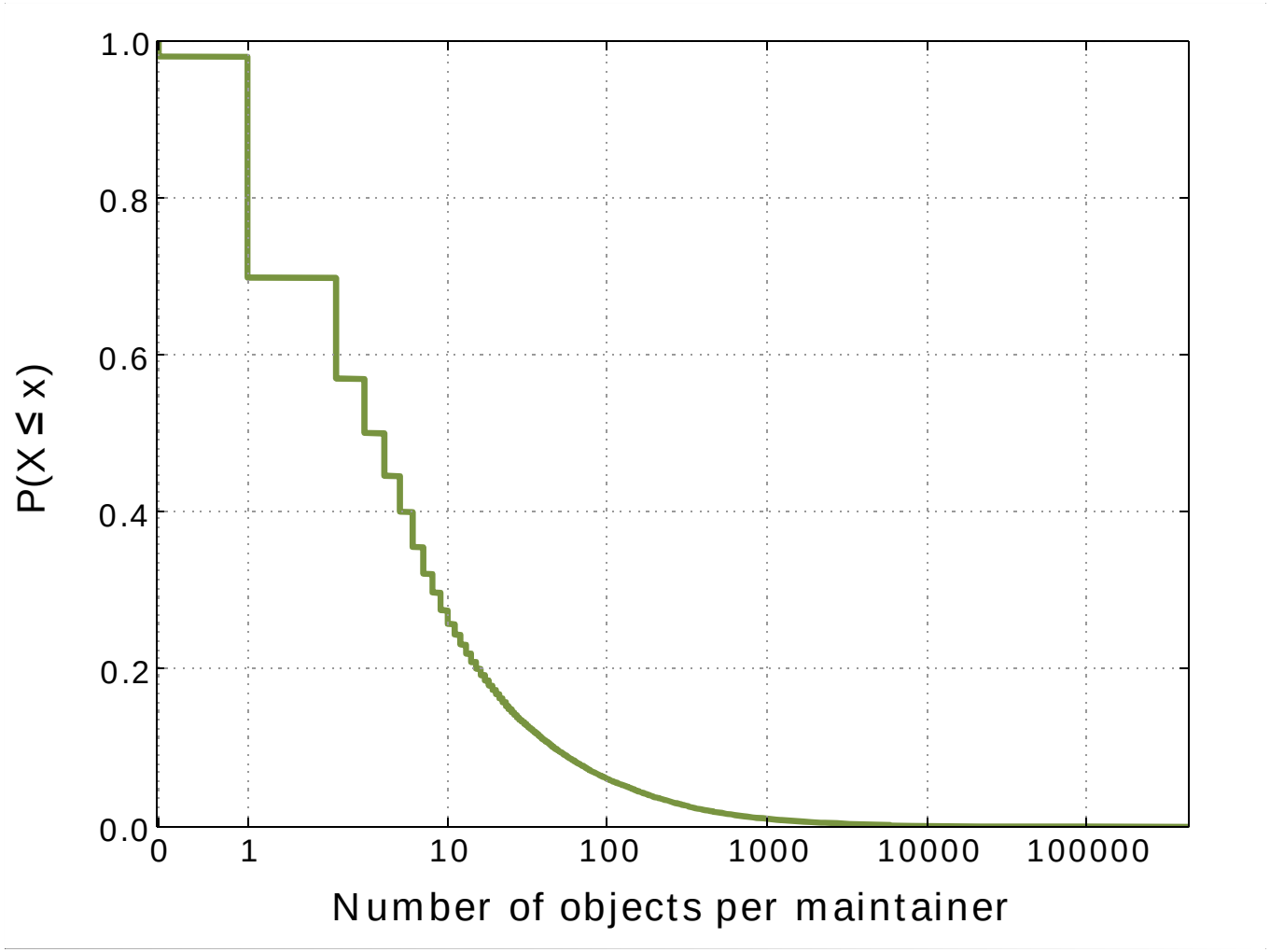
```
inetnum:    194.28.196.0 - 194.28.199.255
netname:    UA-VELES
descr:      LLC „Unlimited Telecom“
descr:      Kyiv
notify:     internet@veles-isp.com.ua
mnt-by:     VELES-MNT
```

```
aut-num:    AS51016
as-name:    VALES
descr:      LLC „Unlimited Telecom“
notify:     internet@veles-isp.com.ua
mnt-by:     VELES-MNT
```

Grouping Objects by Maintainer

- Maintainer groups
  - Group by unique mnt-by references of all objects
  - Yields 48,802 disjoint groups
- We disregard groups…
  - Of zero-size (unreferenced maintainers)
  - With multiple or without any DNS names
  - Without inetnum or aut-num objects
- We merge groups by identical DNS names, leading to a total of 7,907 remaining groups

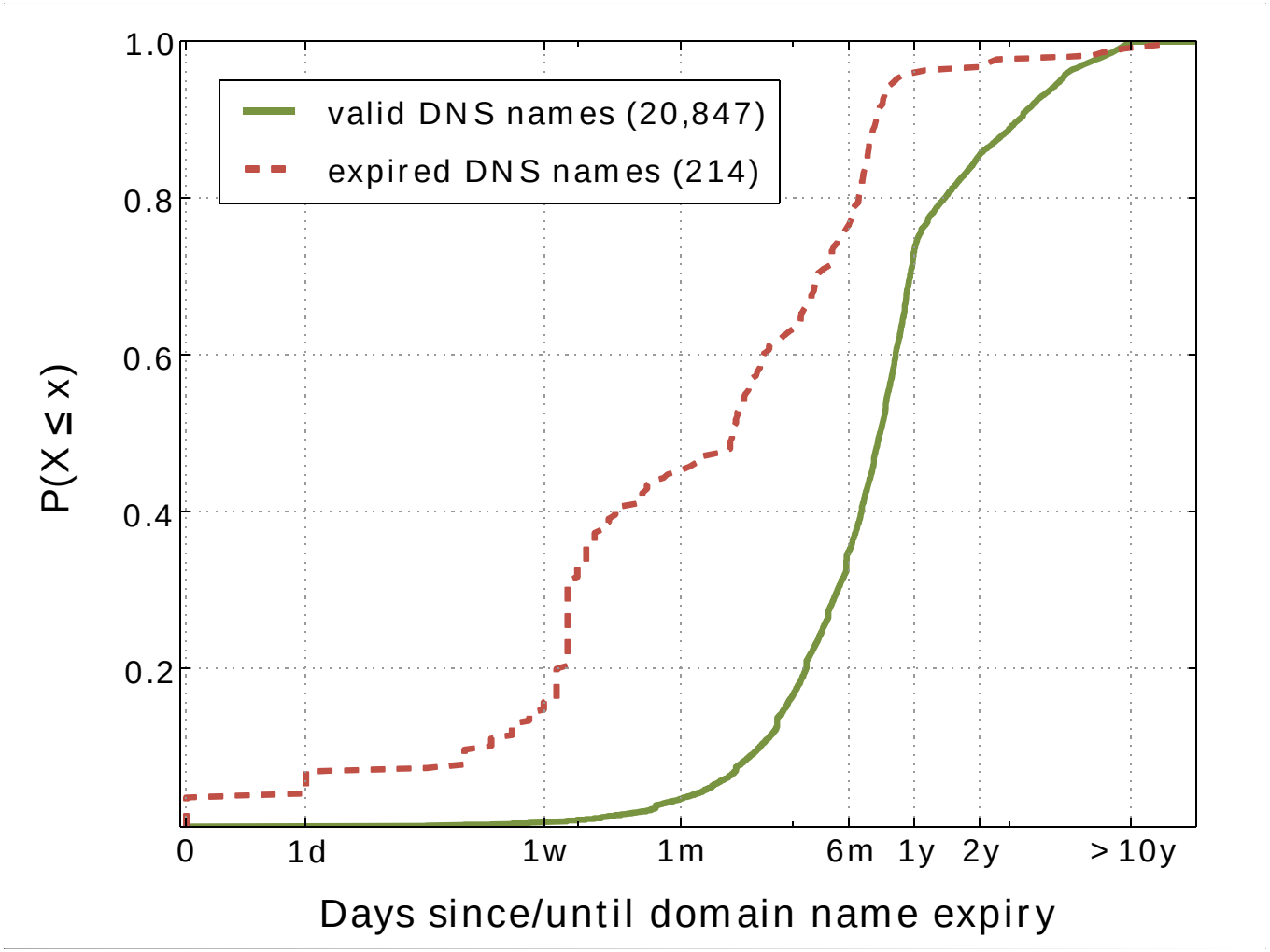
Size of Maintainer Groups



RIPE Database Objects

Object type	Frequency	DNS references	
inetnum	**3,876,883**	**1,350,537**	**(34.84%)**
domain	658,689	97,557	(14.81%)
route	237,370	50,300	(21.19%)
inet6num	231,355	8,717	(3.77%)
organisation	82,512	0	(0.00%)
mntner	48,802	0	(0.00%)
aut-num	**27,683**	**6,838**	**(24.70%)**
role	20,684	14,430	(69.76%)
as-set	13,655	2,500	(18.31%)
route6	9,660	723	(7.48%)
irt	321	162	(50.47%)
Total	**5,239,201**	**1,531,764**	**(29.24%)**

Lifetime of Domain Names



Extracted Domain Names

- More than 1.5 M references to DNS names, of which 21,061 are distinct
- Whois queries yield 214 expired DNS names

Top5 TLDs	
.com	27.9%
.ru	21.5%
.net	13.0%
.se	4.8%
.co.uk	3.5%

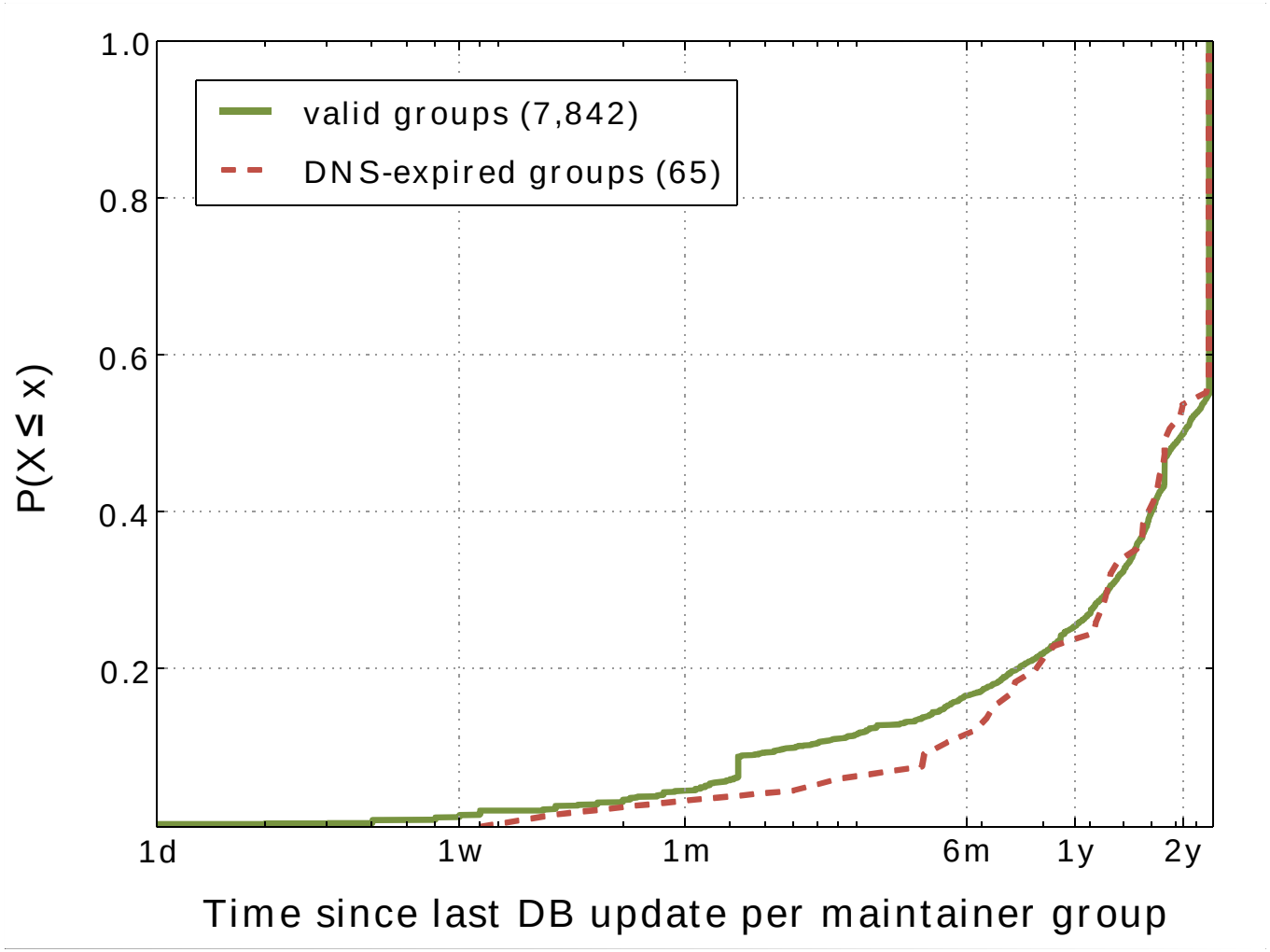
Top5 TLDs (expired)	
.ru	20.1%
.it	16.4%
.com	9.8%
.dk	9.8%
.net	7.0%

- 65 of 7,907 groups reference expired DNS names

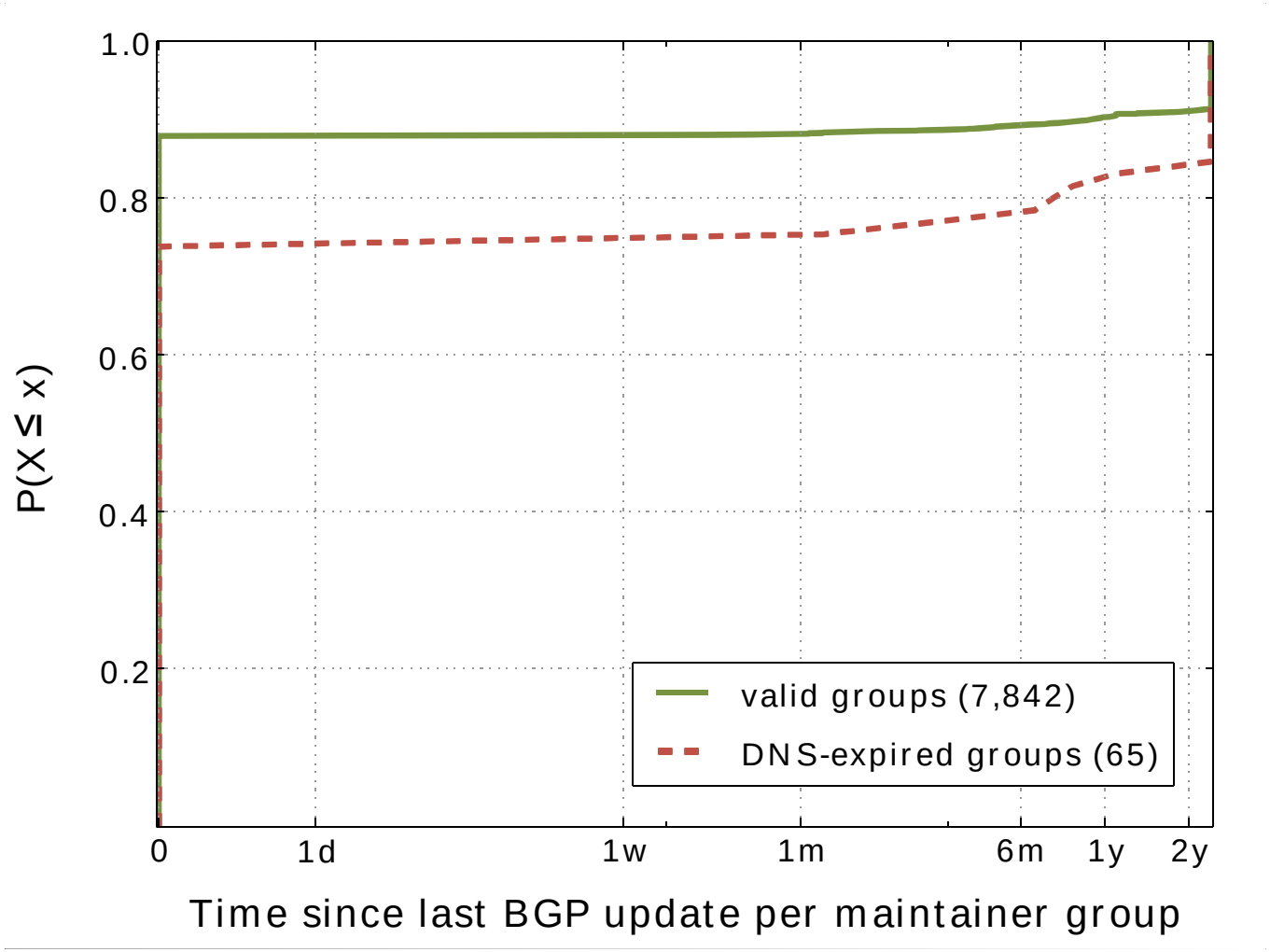
Refinement by Activity Measures

- The RIPE database could simply be outdated…
- Time since last database update
  - Top-10% of valid groups changed within 2 months
  - Top-10% of expired groups changed within 6 months
  - DNS expiry and update behavior correlate
- Time since last BGP update
  - Search for prefixes and ASes of the maintainer groups
  - Analysis of 2.5 years of archived BGP routing tables
  - Key findings: 90% of valid resources are active in BGP, in contrast to 75% of expired resources

TIME SINCE LAST DB UPDATE



TIME SINCE LAST BGP ACTIVITY



Our

FINDINGS

Abandoned Resources

- Expired DNS names
  - 65 disjoint resource groups reference expired domains
  - These groups hold 773 /24 networks and 54 ASes
- BGP activity for these resources
  - 75% are still in use (but impersonation is possible, i.e. a hijack would disrupt operational use)
  - 13 groups show no activity for more than 6 months
- Final result: we found 73 /24 networks and 7 ASes fully abandoned for more than 6 months

Conclusion

- Summary
  - Correlation of archived RIPE databases, BGP tables and DNS registration data over a period of 30 months
  - We found that in total, more than a /18 network is abandoned, waiting to be stealthily hijacked!
- Conservative results
  - Mostly anonymized data set (< 35% usable DNS data)
  - Analysis limited to the RIPE service region
- We need better ownership validation to secure unused resources!

THANK YOU!

Questions

The Abandoned Side of the Internet: Hijacking Internet Resources When Domain Names Expire

Johann Schlamp, Josef Gustafsson, Matthias Wählisch, Thomas C. Schmidt, Georg Carle