



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

The Abandoned Side of the Internet



The screenshot shows an eBay auction page. At the top left is the eBay logo. To its right are navigation links: home, my eBay, site map, and sign in/out. Below these are buttons for Browse, Sell, Services, Search, Help, and Community. A sub-button for 'item view' is under 'Browse'. A message says 'See this item in eBay's new look for this page.' The main title of the auction is '/16 CLASS B - 65534 IP's GRANDFATHERED !!!!' with item number 3029809556. The category is 'Electronics & Computers: Networking & Telecom: Other' and 'Electronics & Computers: Wholesale Lots: Networking & Telecom'. The current bid is US \$6,800.00 (reserve not yet met), starting at US \$0.01. There is 1 quantity, 8 days left, and 29 bids. The location is Houston, United States. The auction started on Jun-09-03 and ends on Jun-19-03. The seller is csutter2002 with a 170 feedback rating and 100% positive reviews. The page is marked as a 'Featured Auction'.

home | my eBay | site map | sign in/out

Browse Sell Services Search Help Community

item view

See this item in eBay's new look for this page.

/16 CLASS B - 65534 IP's GRANDFATHERED !!!!

Item # 3029809556

[Electronics & Computers: Networking & Telecom: Other](#)
[Electronics & Computers: Wholesale Lots: Networking & Telecom](#)

 Description

Current bid **US \$6,800.00** (reserve not yet met) Starting bid **US \$0.01**

Quantity **1** # of bids **29** [Bid history](#)

Time left **8 days, 0 hours +** Location **Houston**

Country/Region **United States /Houston**

 Bid

Started Jun-09-03 22:34:11 PDT [Mail this auction to a friend](#)

Ends Jun-19-03 22:34:11 PDT [Watch this item](#)

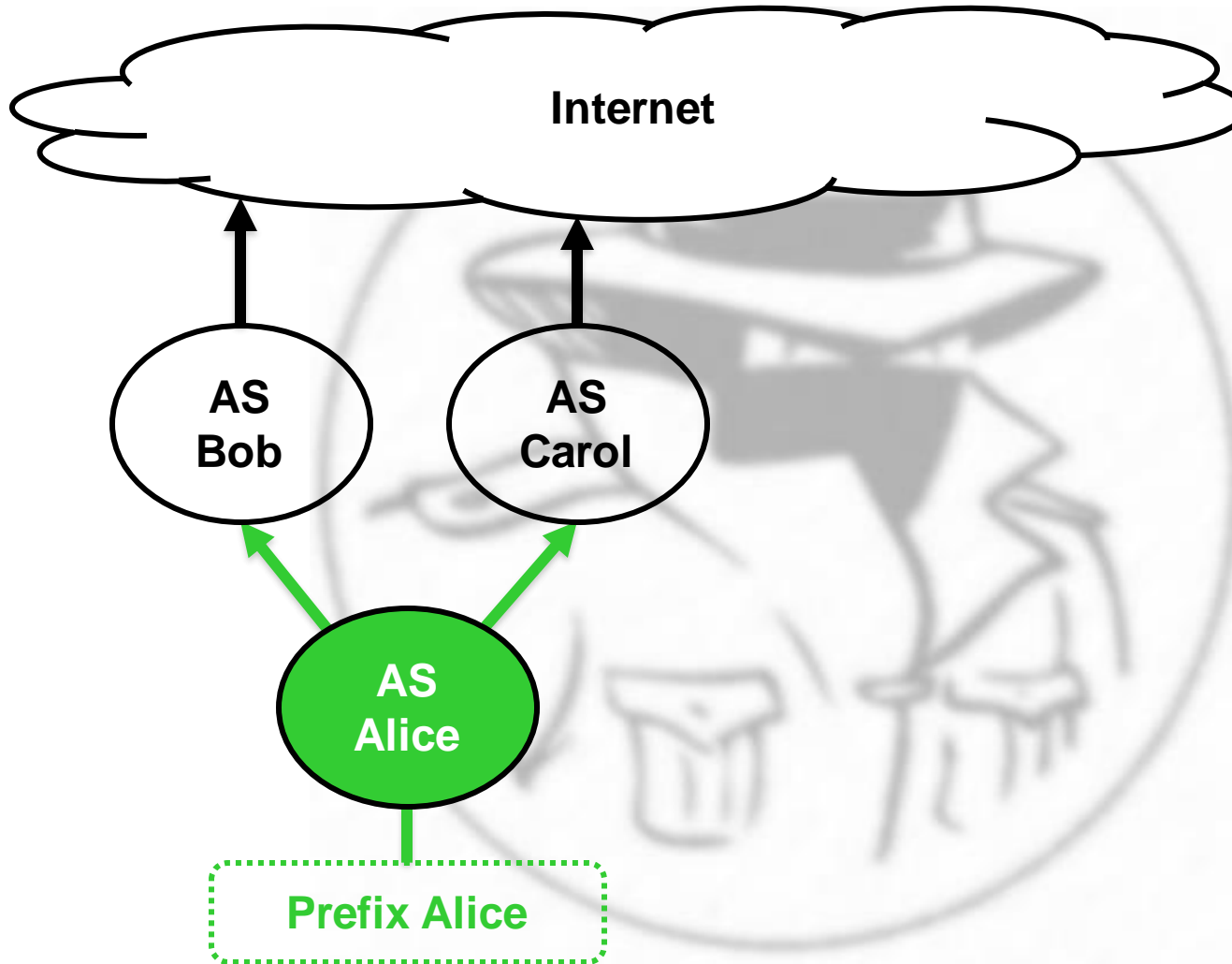
Featured Auction

[csutter2002](#) (170 ★)

Seller (rating) **Feedback rating: 170** with 100% positive feedback reviews ([Read all reviews](#))
Member since: Jun-23-02. Registered in United States
[View seller's other items](#) | [Ask seller a question](#) | [Safe Trading Tips](#)

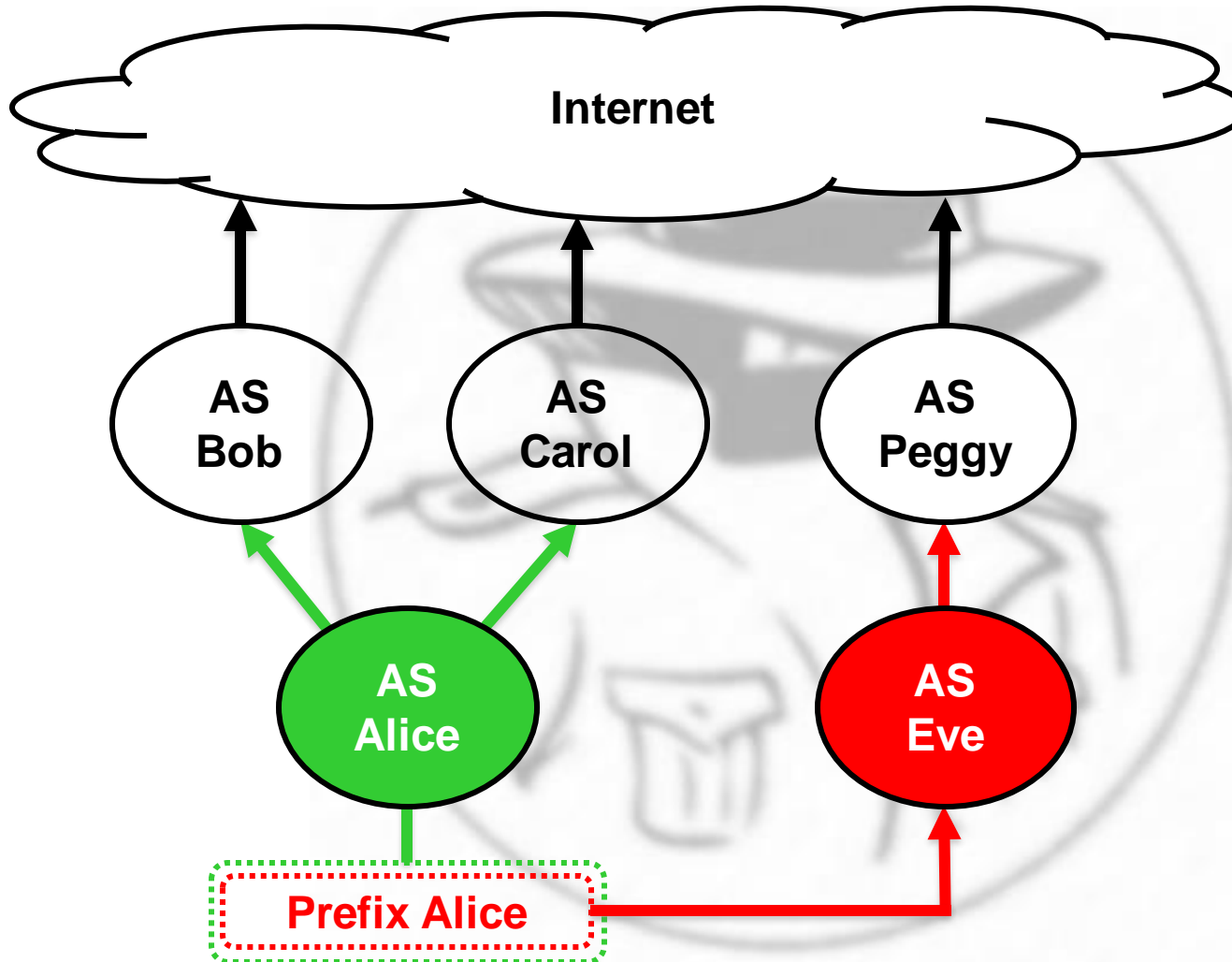
REGULAR PREFIX HIJACKING

The Abandoned Side of the Internet



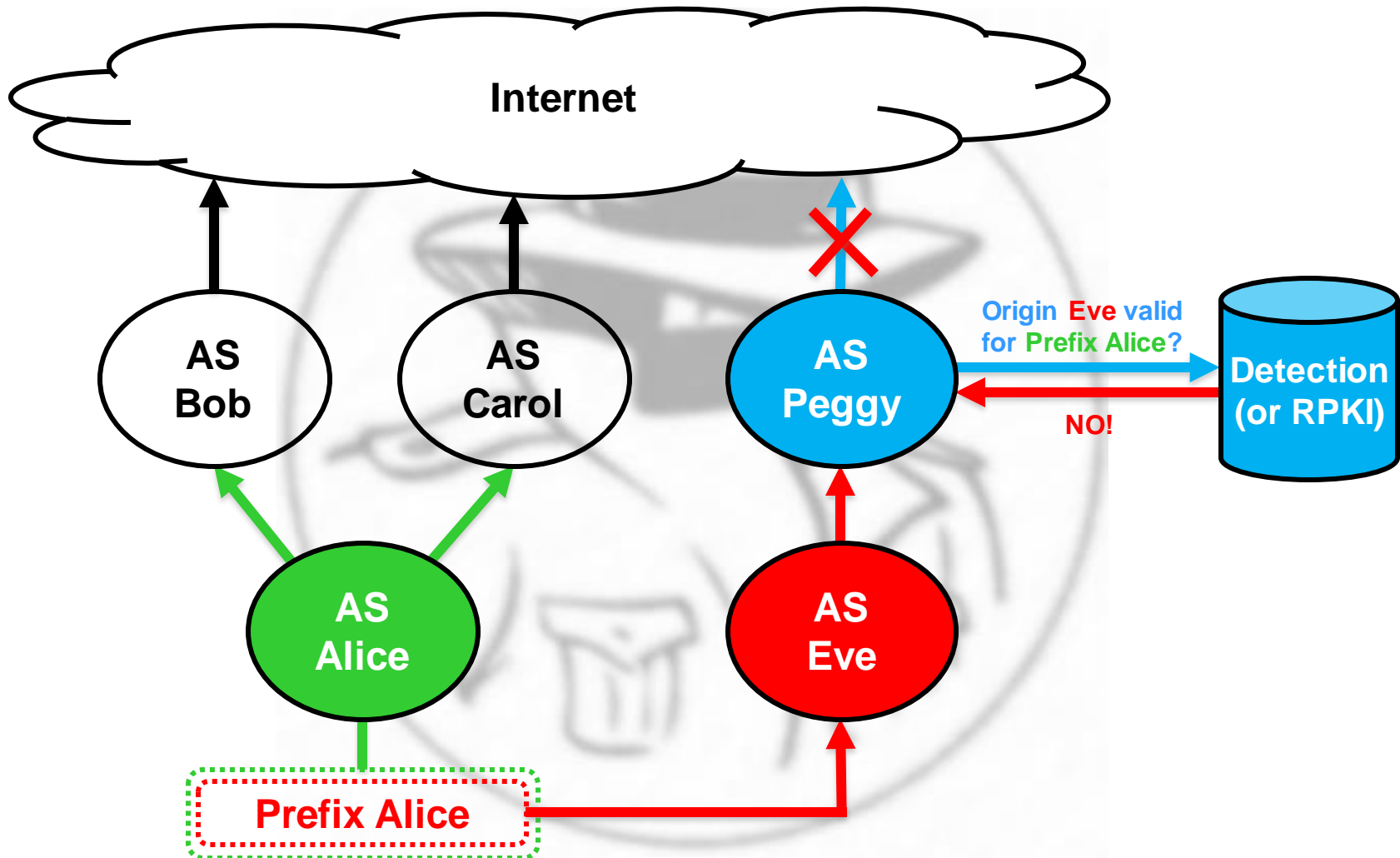
REGULAR PREFIX HIJACKING

The Abandoned Side of the Internet



REGULAR PREFIX HIJACKING WITH RPKI

The Abandoned Side of the Internet



MOTIVATION (II) – THE LINKTEL INCIDENT

The Abandoned Side of the Internet

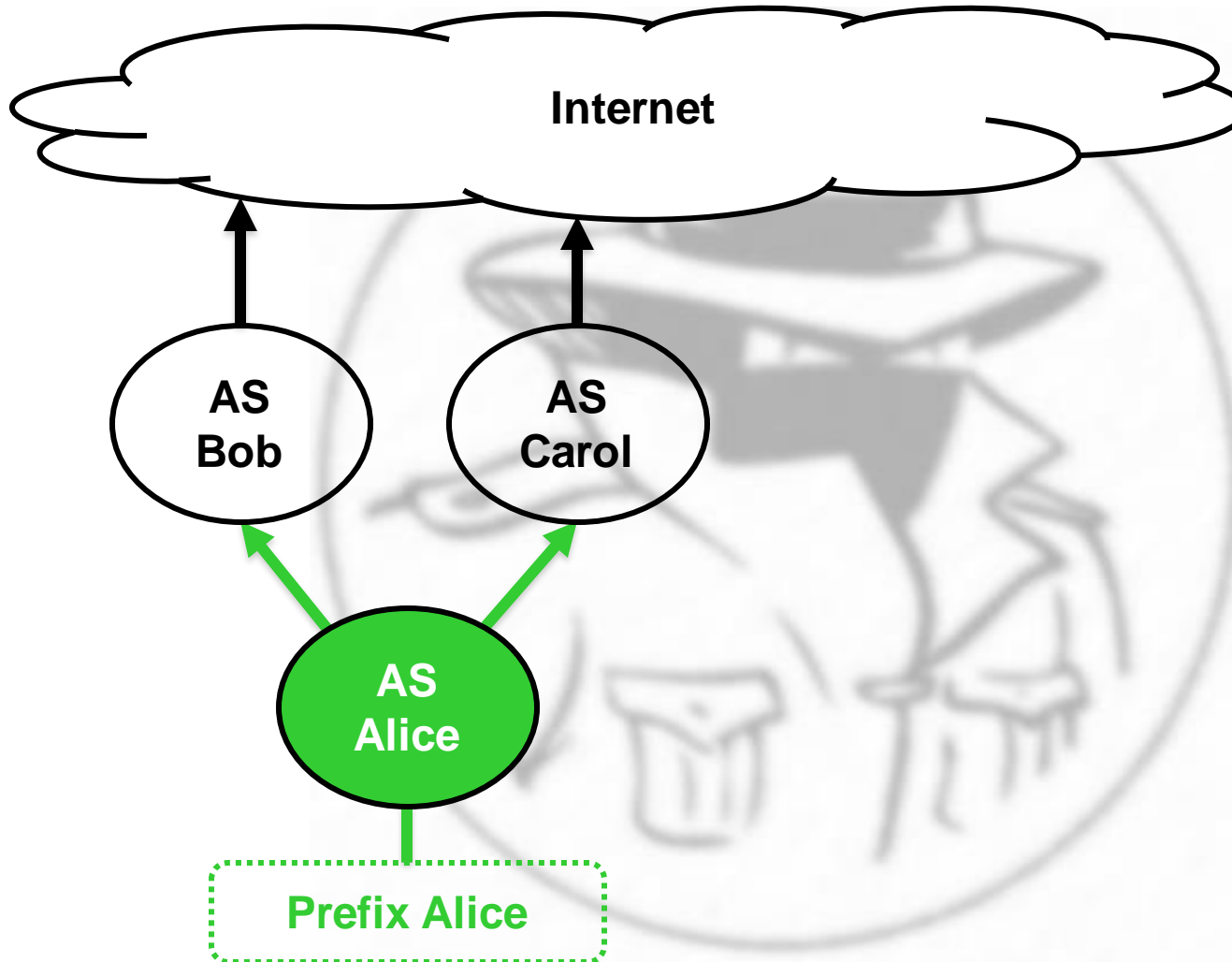
- A new hijacking attack [1]
 - SOS to NANOG from a Russian ISP under attack
 - Unnoticed for 6 months due to business struggles
 - Forensic analysis of the incident one year later

- 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.

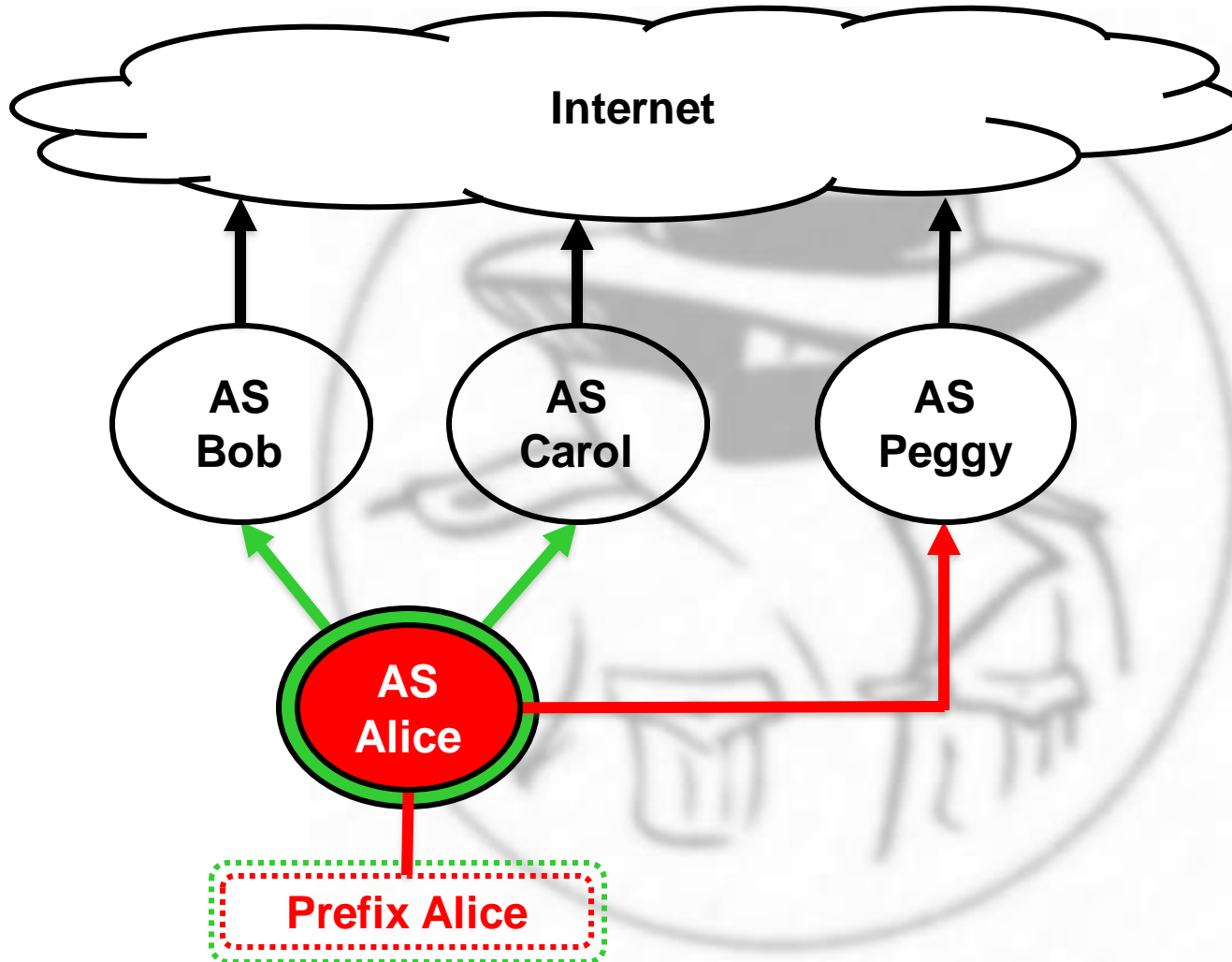
AS HIJACKING

The Abandoned Side of the Internet



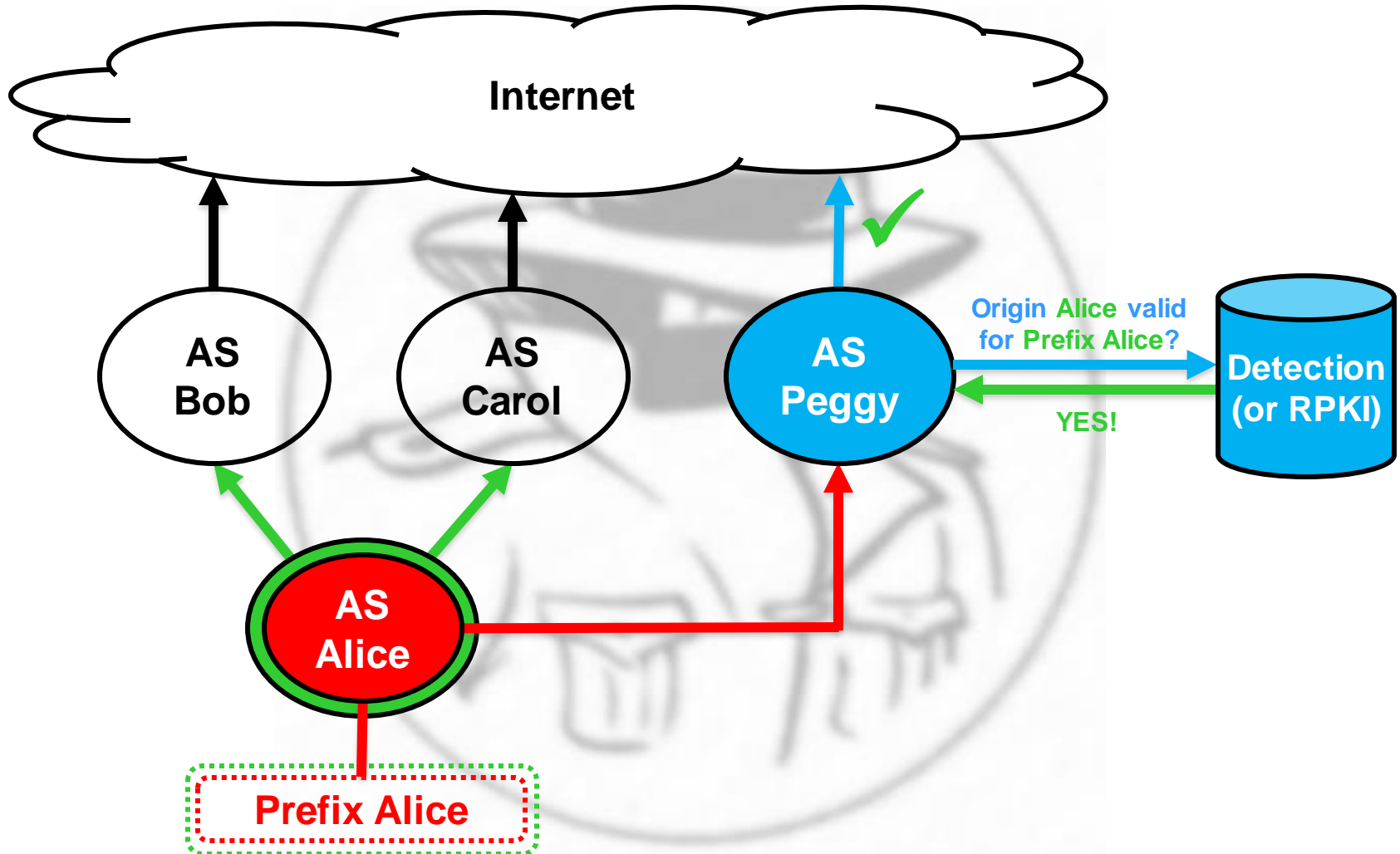
AS HIJACKING

The Abandoned Side of the Internet



AS HIJACKING WITH RPKI

The Abandoned Side of the Internet



Identification of

ABANDONED INTERNET RESOURCES

PRECONDITIONS FOR SUCCESSFUL ATTACKS

The Abandoned Side of the Internet

- 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

The Abandoned Side of the Internet

- 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

The Abandoned Side of the Internet

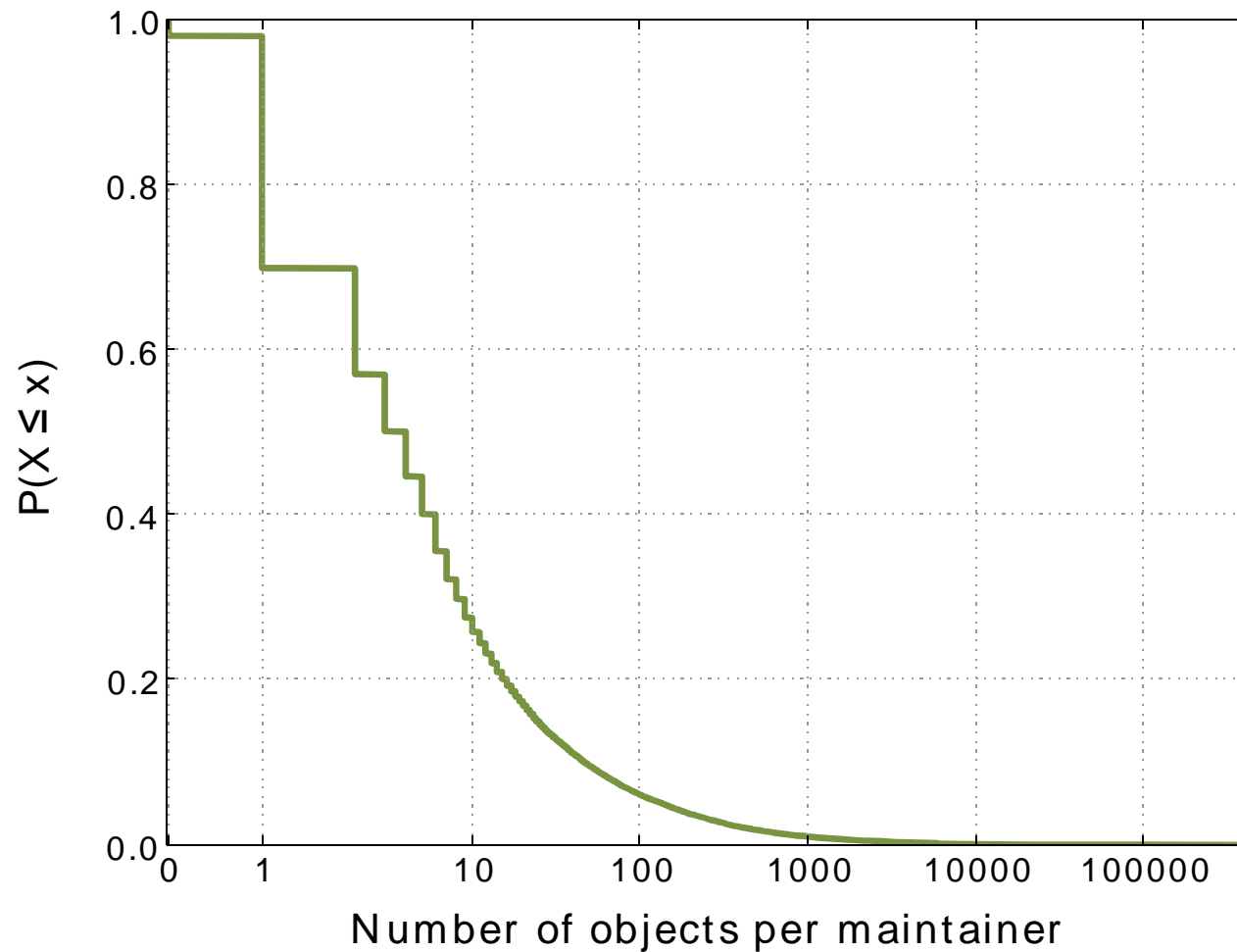
- ❑ Maintainer groups
 - Group by unique mnt-by references of all objects
 - Yields 48,802 disjoint groups

- ❑ 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

The Abandoned Side of the Internet



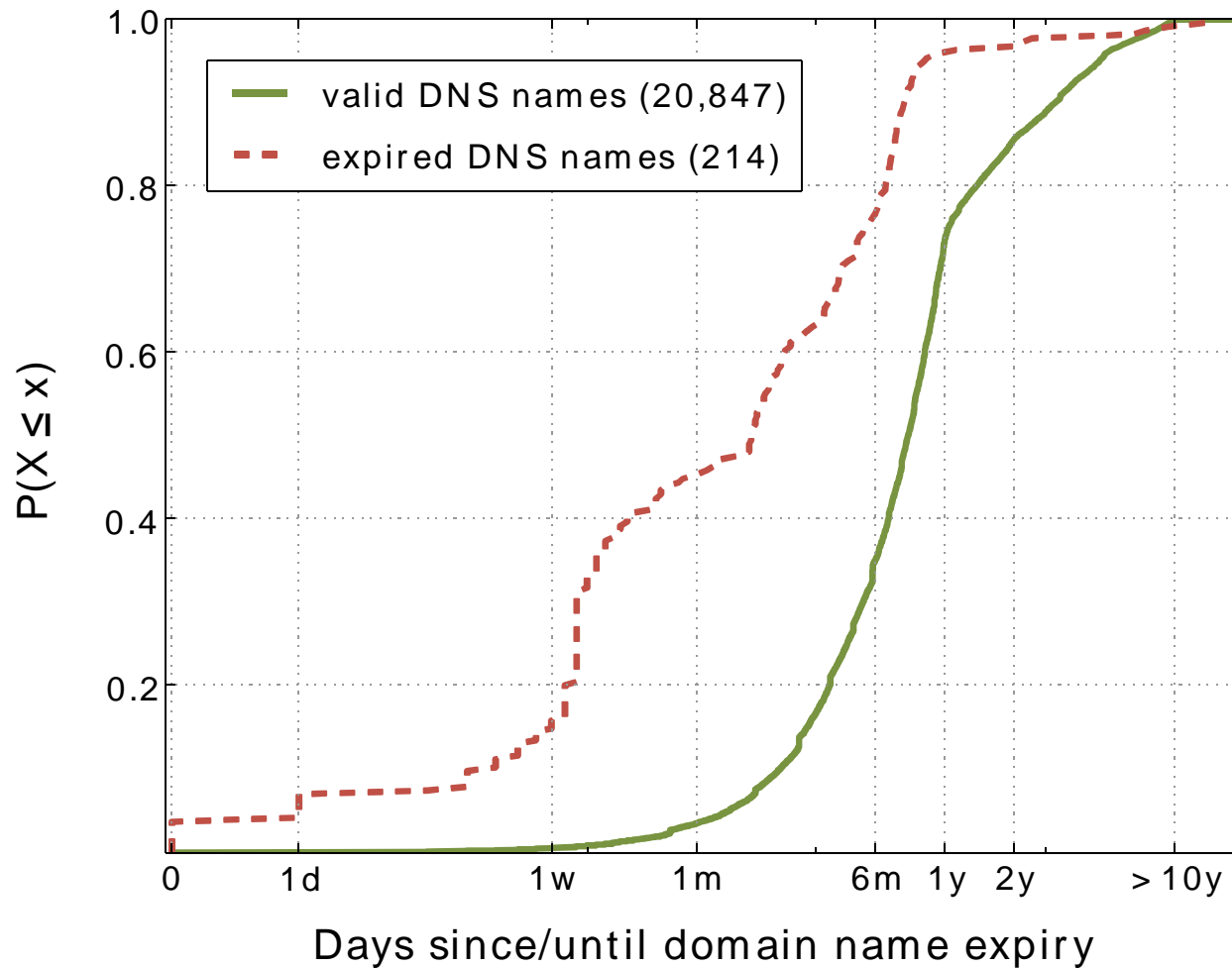
RIPE DATABASE OBJECTS

The Abandoned Side of the Internet

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

The Abandoned Side of the Internet



EXTRACTED DOMAIN NAMES

The Abandoned Side of the Internet

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

Top5 TLDs		Top5 TLDs (expired)	
.com	27.9%	.ru	20.1%
.ru	21.5%	.it	16.4%
.net	13.0%	.com	9.8%
.se	4.8%	.dk	9.8%
.co.uk	3.5%	.net	7.0%

- ❑ 65 of 7,907 groups reference expired DNS names

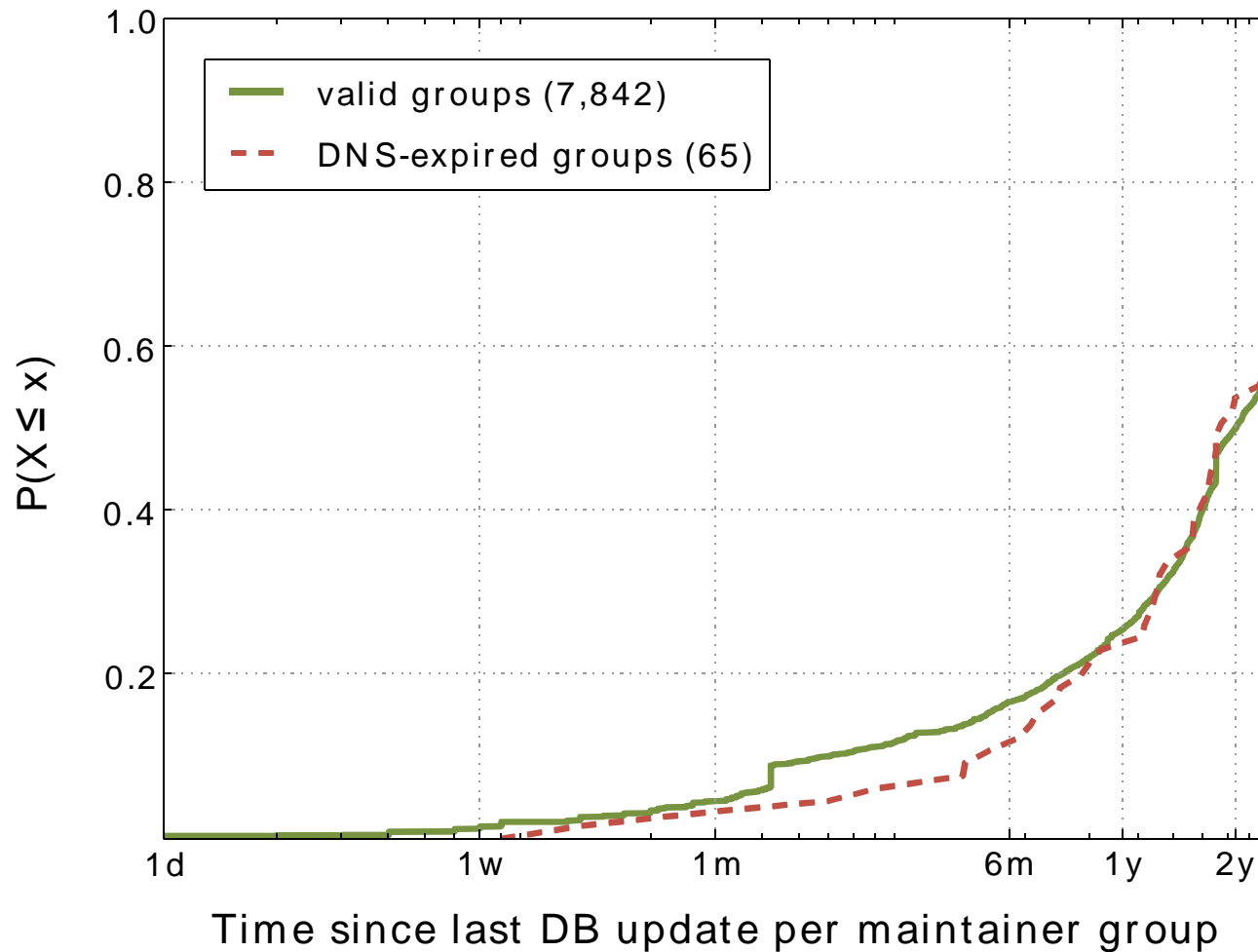
REFINEMENT BY ACTIVITY MEASURES

The Abandoned Side of the Internet

- 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

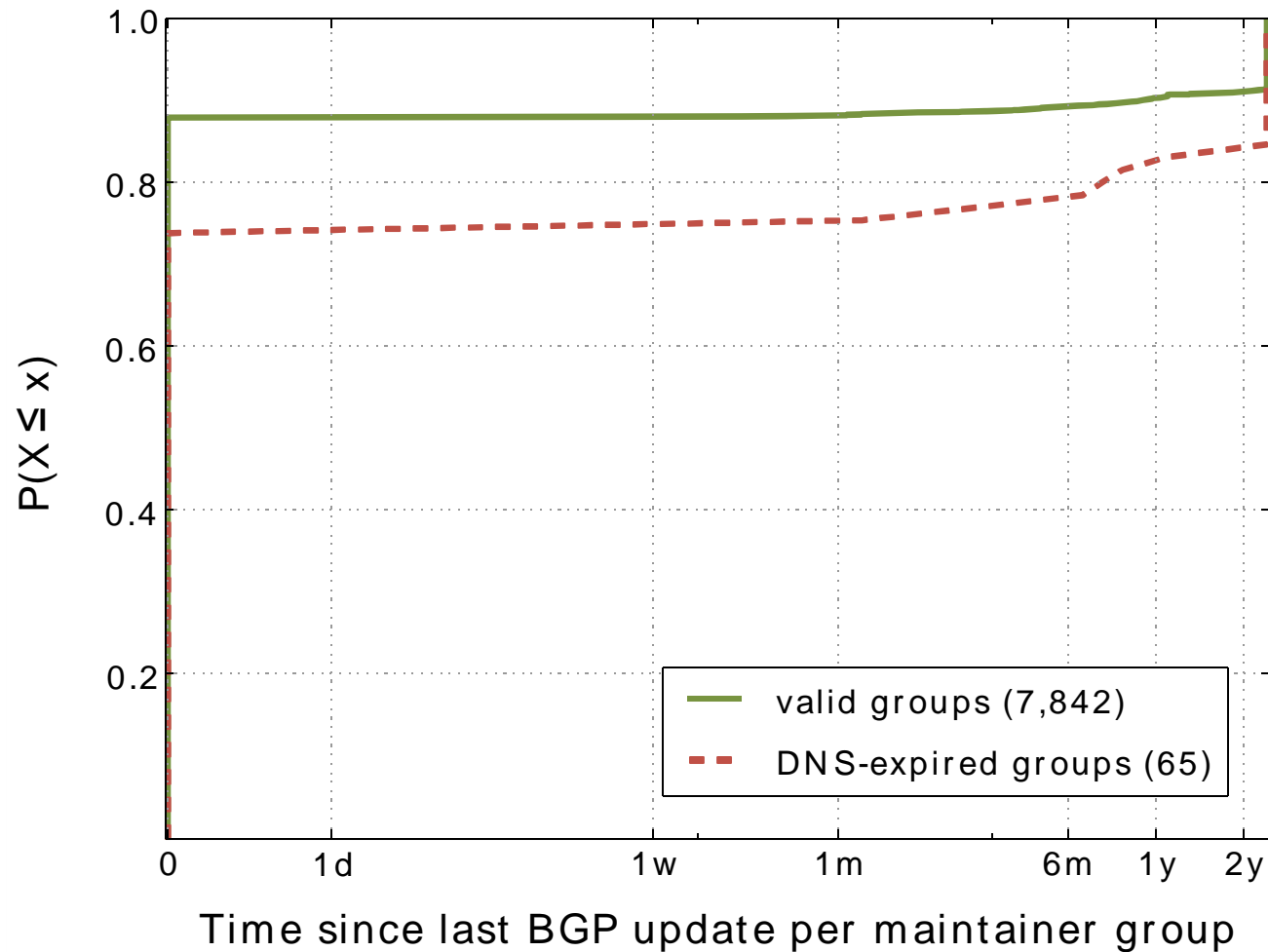
TIME SINCE LAST DB UPDATE

The Abandoned Side of the Internet



TIME SINCE LAST BGP ACTIVITY

The Abandoned Side of the Internet



Our
FINDINGS

ABANDONED RESOURCES

The Abandoned Side of the Internet

- ❑ 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