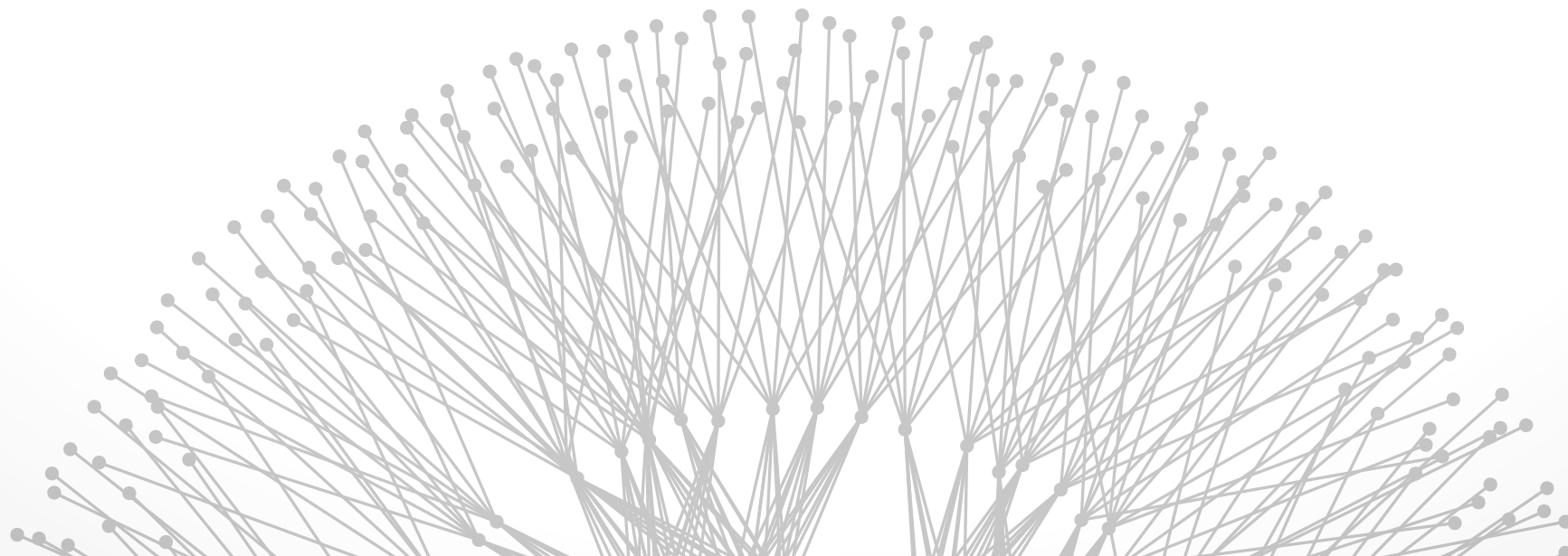


Secure Routing

Brighten Godfrey
CS 538 October 22 2013





Where was security in the design of the original Internet protocols?

- Virtually nowhere!
- All the core protocols (IP, TCP, DNS, BGP) have trivial, glaring vulnerabilities

When security really matters, rely on end-to-end mechanisms

- Public key cryptography & certificate authorities

With e2e security, what can an attack on BGP still do?



Denial of service

- announce “more attractive” path (what does that mean?)
- e.g., more-specific prefix; shorter path; “cheaper” path

Eavesdropping

- like DoS, a kind of traffic attraction
- but somehow get data to destination or impersonate it

Evasion of accountability

- steal someone’s prefix or an unused one; send spam; disappear!

How (much) do secure variants of BGP help?

Infrastructure security



Network Infrastructure Security Practices

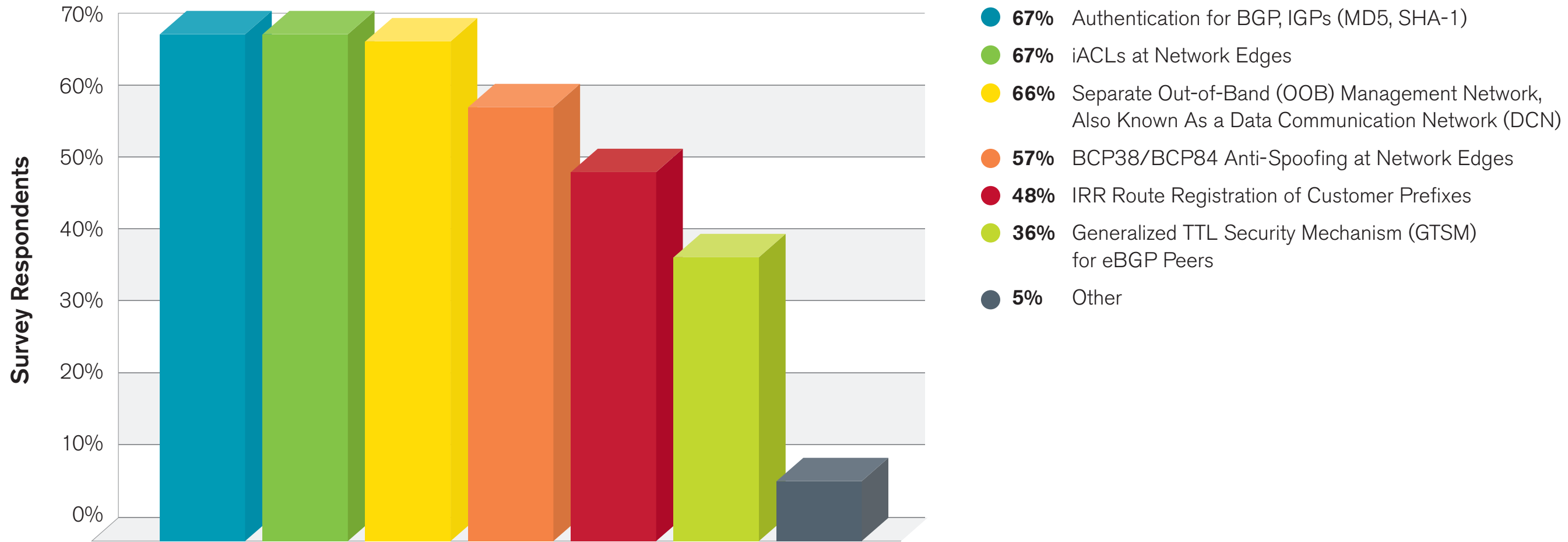


Figure 91 Source: Arbor Networks, Inc.

Three approaches to BGP security



1. Defensive filtering
2. Origin Authentication
3. Secure BGP (S-BGP)

Many others not discussed here

- Active area of research over the last decade
- Many tradeoffs, especially in deployment issues

1. Defensive filtering



Most commonly used class of techniques

Typical implementation

- Filter routes received from customers/peers
- Requires assumptions about what they should be advertising
- Imperfect, requires human maintenance

Filtering of Route Announcements from Peers

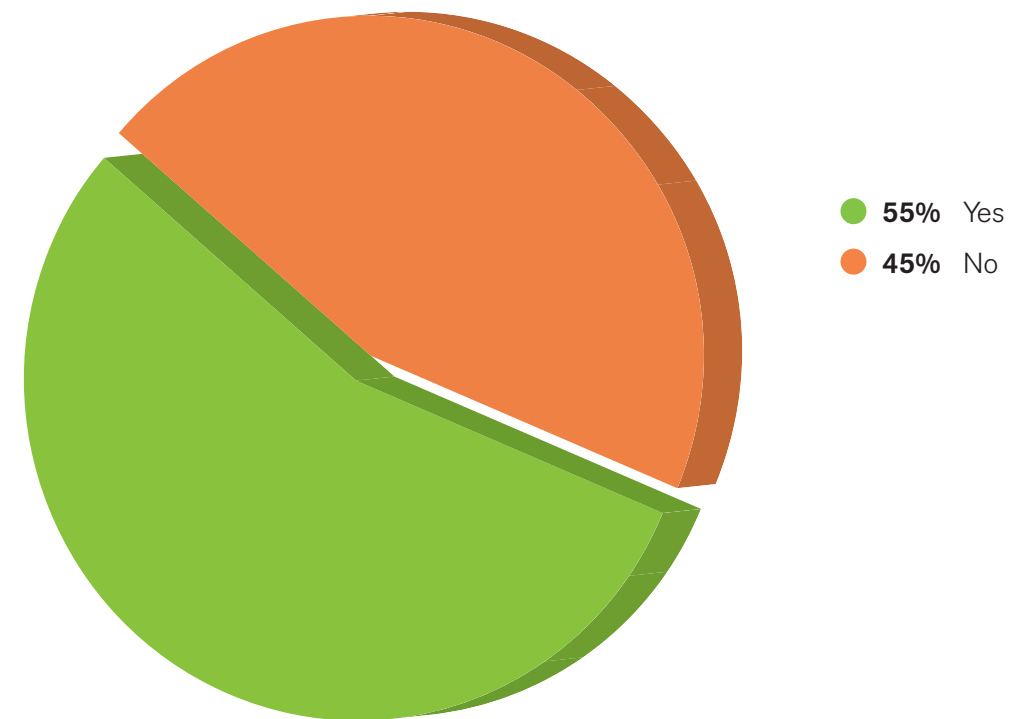
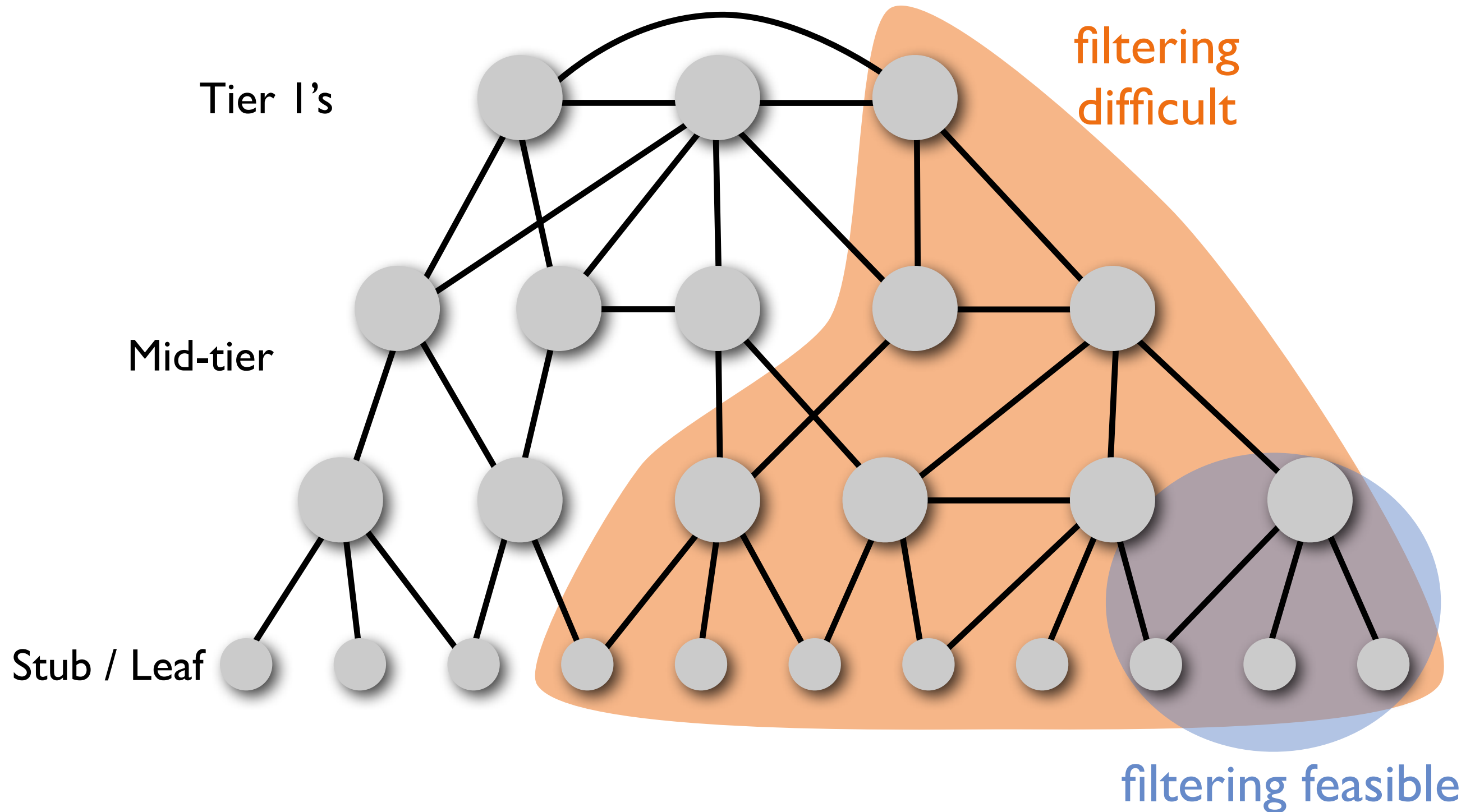


Figure 93 Source: Arbor Networks, Inc.

Arbor Networks survey 2012:
76% filter from customers
55% filter from peers
57% monitor for hijacks

1. Defensive filtering



1. Defensive filtering



Pretty Good BGP [Karlin, Forrest, Rexford, ICNP'06]

- Deprioritize “novel” routes for a period (e.g. 24 hours)
- Routers prefer older (known) routes
- May still pick new route if it's the only option
- Why does this help?

Advantages

- Raises the bar for attacker: route must persist
- Gives time for response
- No protocol changes for deployment

Disadvantages?

1. Defensive filtering



Pretty Good BGP [Karlin, Forrest, Rexford, ICNP'06]

Take-away points

- Prioritization is important: not just good vs. bad route
- Think about human-level solutions
 - # suspicious advertisements is only about 50/day
 - vs. $O(400k/day)$ total

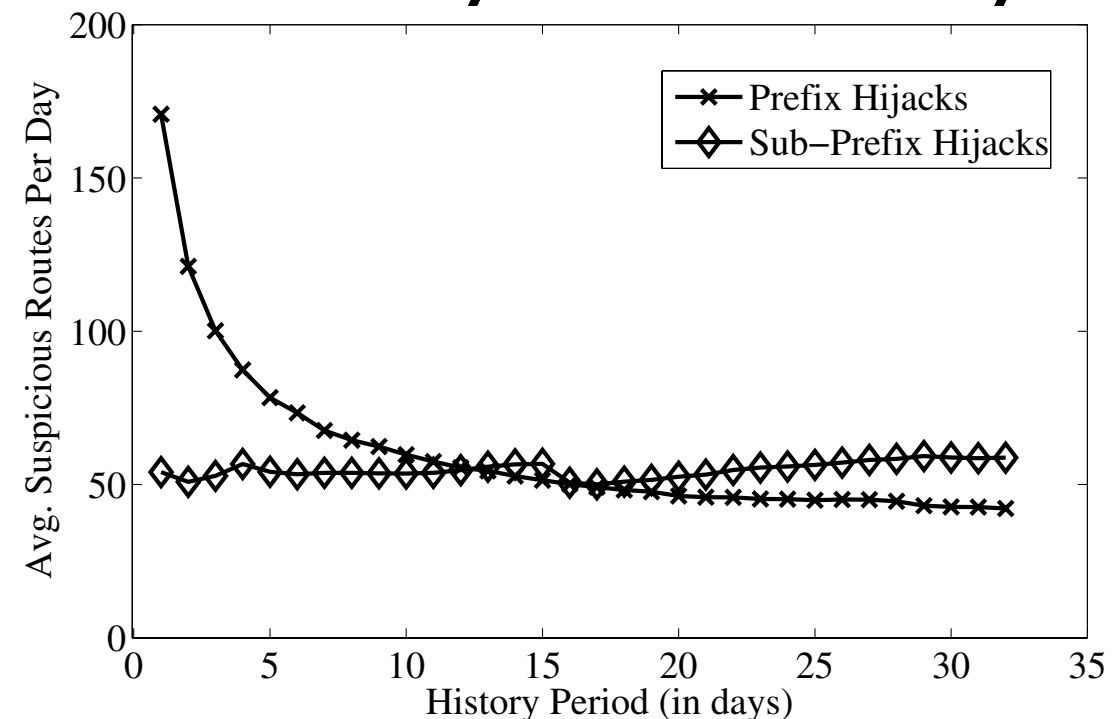


Fig. 1. Average number of announcements (per day) classified as suspicious using a suspicious period of 1 day and a variety of history periods (h).

2. Origin Authentication



Idea

- Use a Routing Public Key Infrastructure (RPKI) to certify AS number assignment and IP address allocation
- An AS can only claim to originate a prefix it owns
- Analogous to PKI for web TLS/SSL security

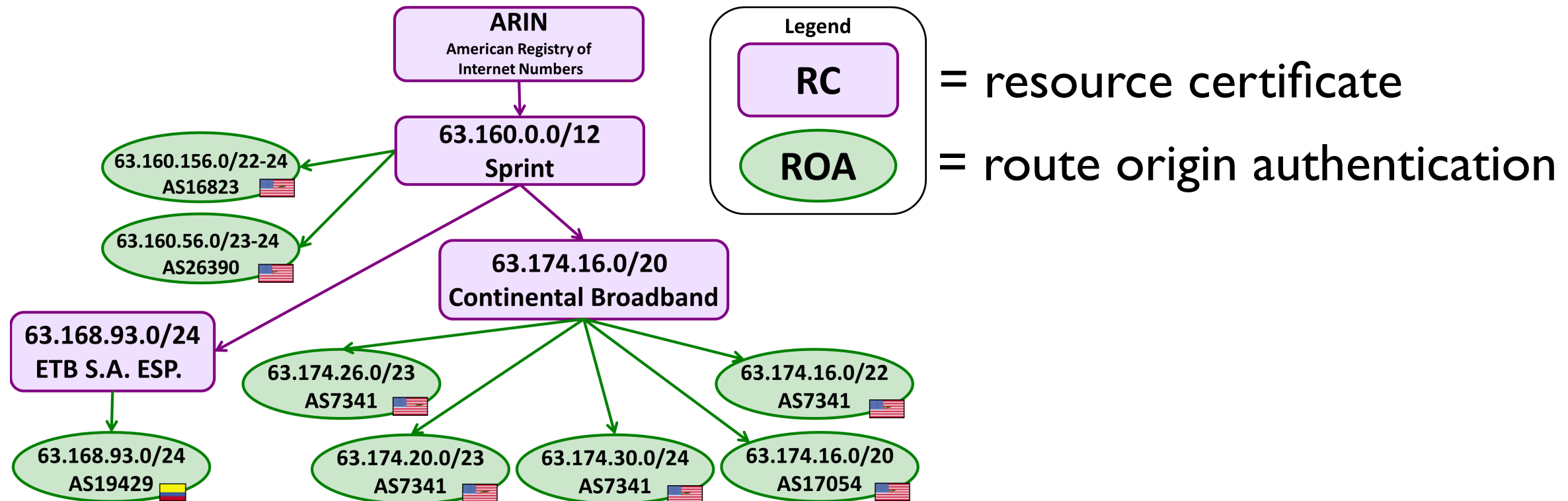


Figure 2: Excerpt of a model RPKI

[Diagram from Cooper, Heilman, Brogle, Reyzin, Goldberg, HotNets 2013]

2. Origin Authentication

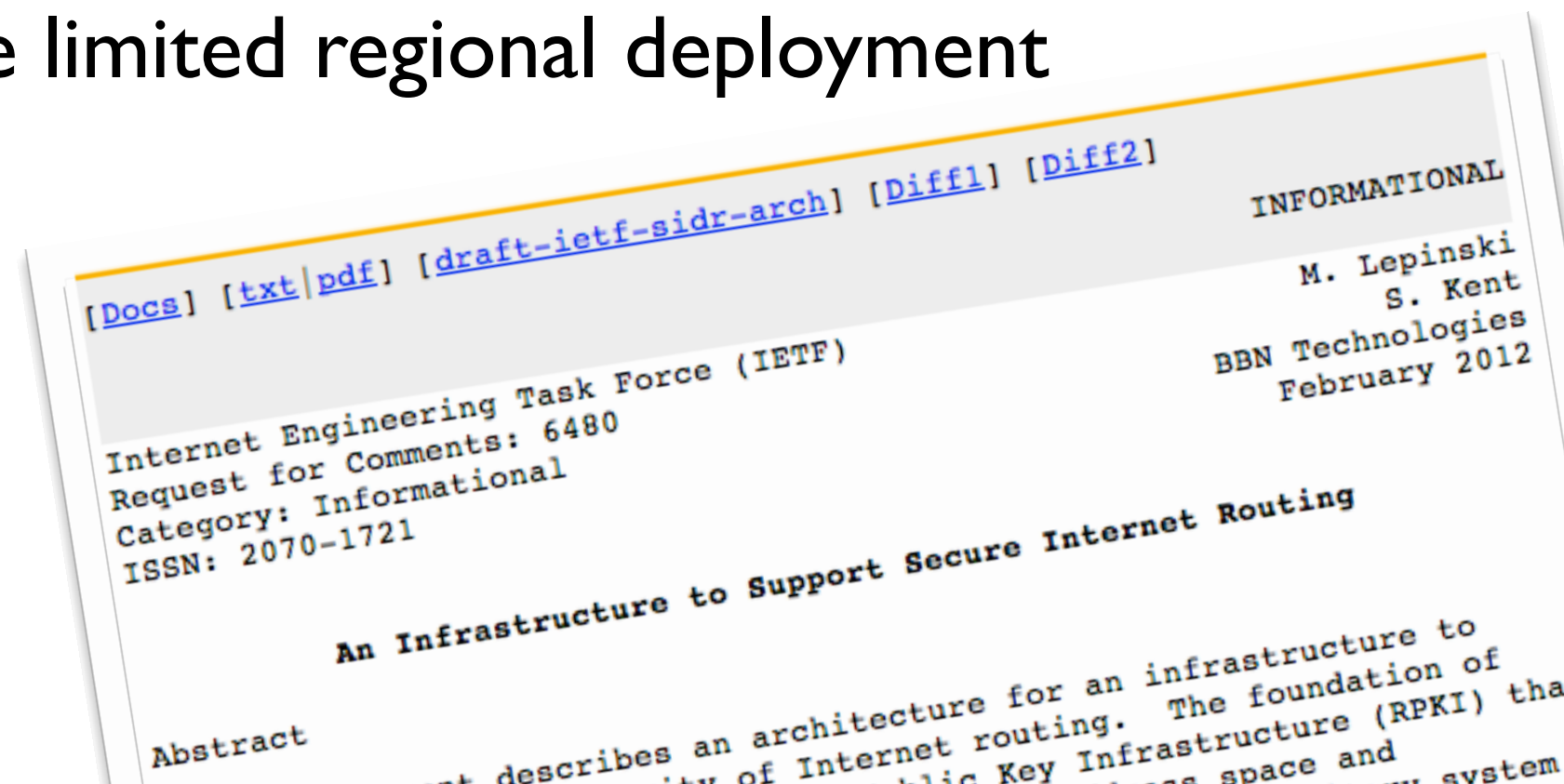


Deployment challenges

- Needs router changes to authenticate, filter
- Needs PKI...

Status

- RPKI just standardized in 2012
- Now seeing some limited regional deployment



3. S-BGP



Scheme

- Origin Authentication + hop-by-hop cryptographic validation

Deployment challenges

- Requires PKI
- Requires significant computational resources

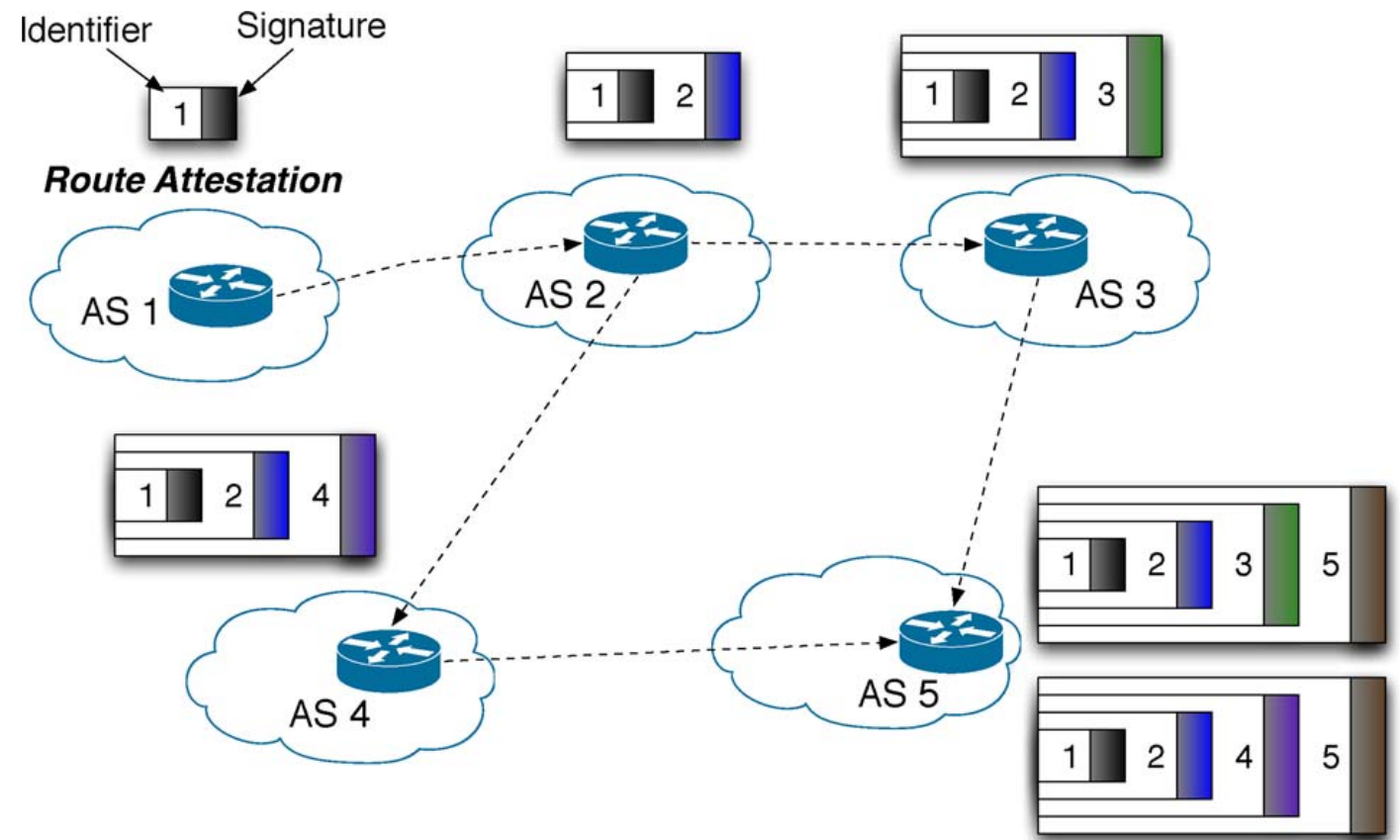


Fig. 5. Route attestations in S-BGP. As UPDATE messages are passed between peers, the receiving peer signs the received message before passing it to another neighbor. The result is an “onion-style” attestation that contains signatures from all routers along the path.

How well do they work?



How Secure are Secure Interdomain Routing Protocols? [Goldberg, Schapira, Hummon, Rexford, SIGCOMM 2010]

Quantifying the attack

- Attacker's goal: attract traffic
- Measure fraction of ASes attacker can "steal" traffic from

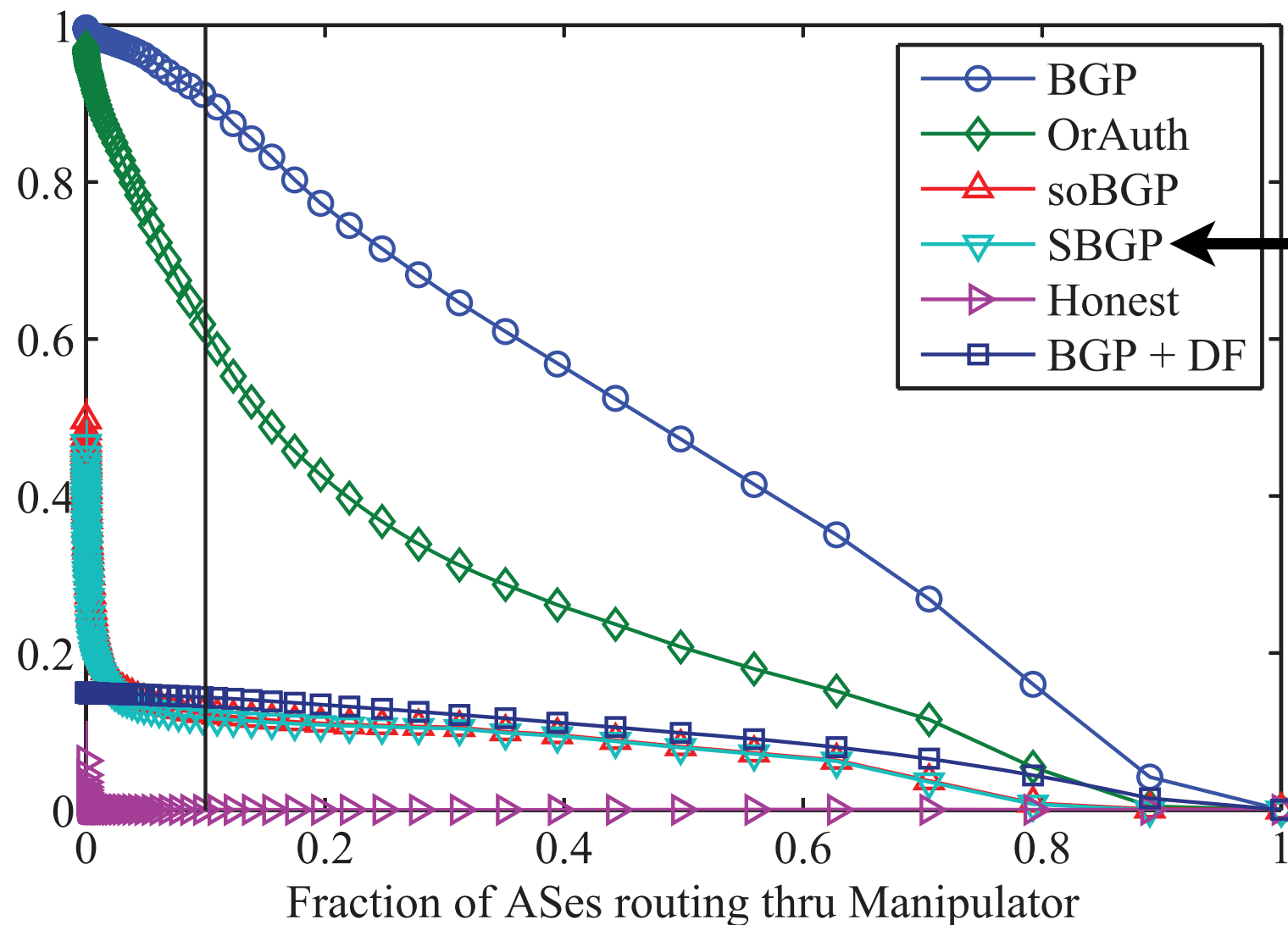
How does the attacker do that?

- Basic "smart" strategy
 - Select or invent the shortest route you can get away with
 - Advertise it to everyone
- Weird fact: this is not actually the attacker's best strategy; that's NP-complete to compute!

Results



How Secure are Secure Interdomain Routing Protocols? [Goldberg, Schapira, Hummon, Rexford, SIGCOMM 2010]



???

Legal but unusual:
Announce routes from
peers/providers to other
peers/providers

Figure 3: CCDF for the “Shortest-Path Export-All” attack strategy.



Is the attack on S-BGP really an attack?

- **No, not technically in the protocol**
 - ASes are allowed to export whatever routes they like
- **Yes, effectively**
 - Key point 1: unusual export can grab nearly as much traffic as prefix hijack!
 - Key point 2: Want protection against accidents well as attackers

Not just malicious attackers



Many or most high-profile outages likely just configuration errors

Natural correspondence between attackers and bugs

- behavior unknown ahead of time
- defense is to limit and contain worst-case effects

What about a bug in the protocol?

- worst-case scenario: zero-day exploit on large fraction of routers across the entire Internet
- many are running the same software!



Many flaws in routing. Which are critical? [Matthew]

Incentives to adopt secure routing? [Mahanth]

Partial deployment crucial. Issues?

Given all this, why does the Internet work so well?
[John, Shambwaditya]

Announcements



Your availability...

- ...Monday 9:30 - 11?
- ...Monday 2:30 - 4?
- ...Wednesday 2 - 3:30?
- ...Tuesday/Thursday 3:30 - 4:30?

Next time: Denial of Service