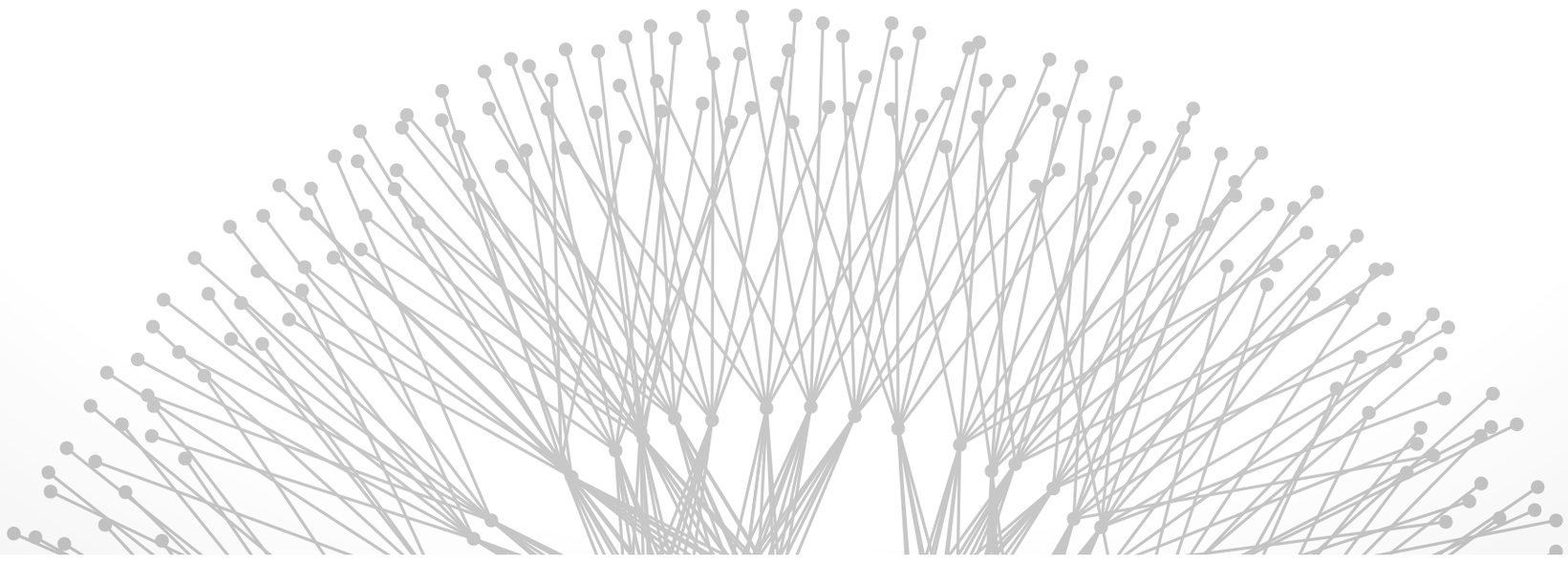
Secure Routing

Brighten Godfrey

CS 538 April 3 2017



Network security

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?

Attacks on Internet routing

Denial of service

- announce "more attractive" path (what does that mean?)
- More likely to be selected: 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 or squat on a prefix; send spam; disappear!

How (much) do secure variants of BGP help?

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

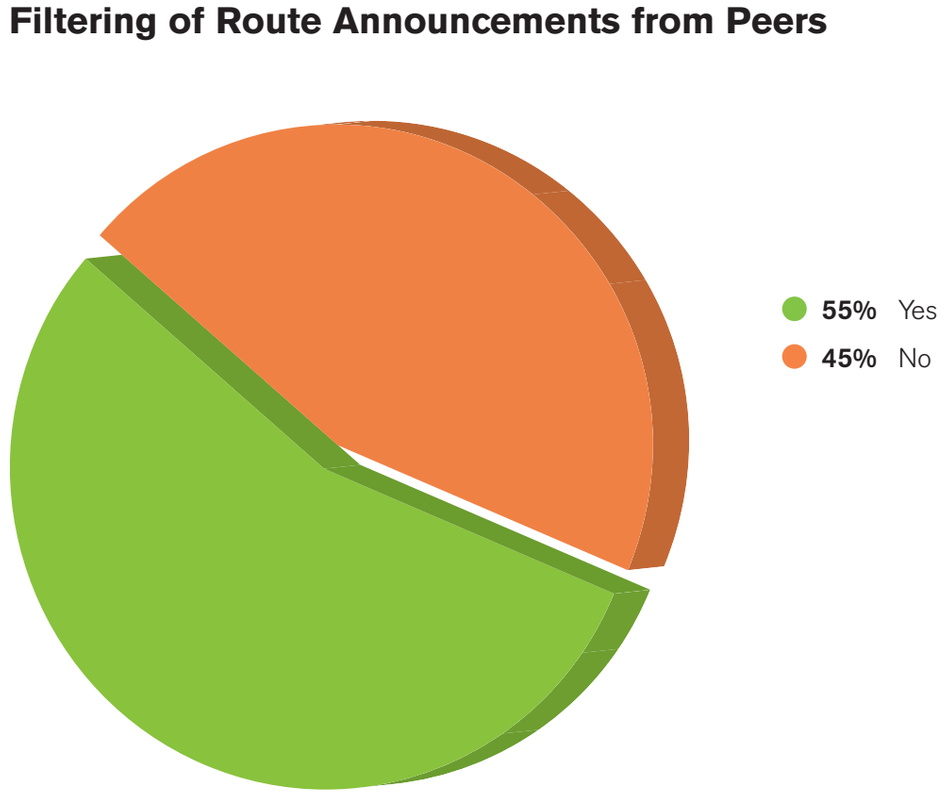
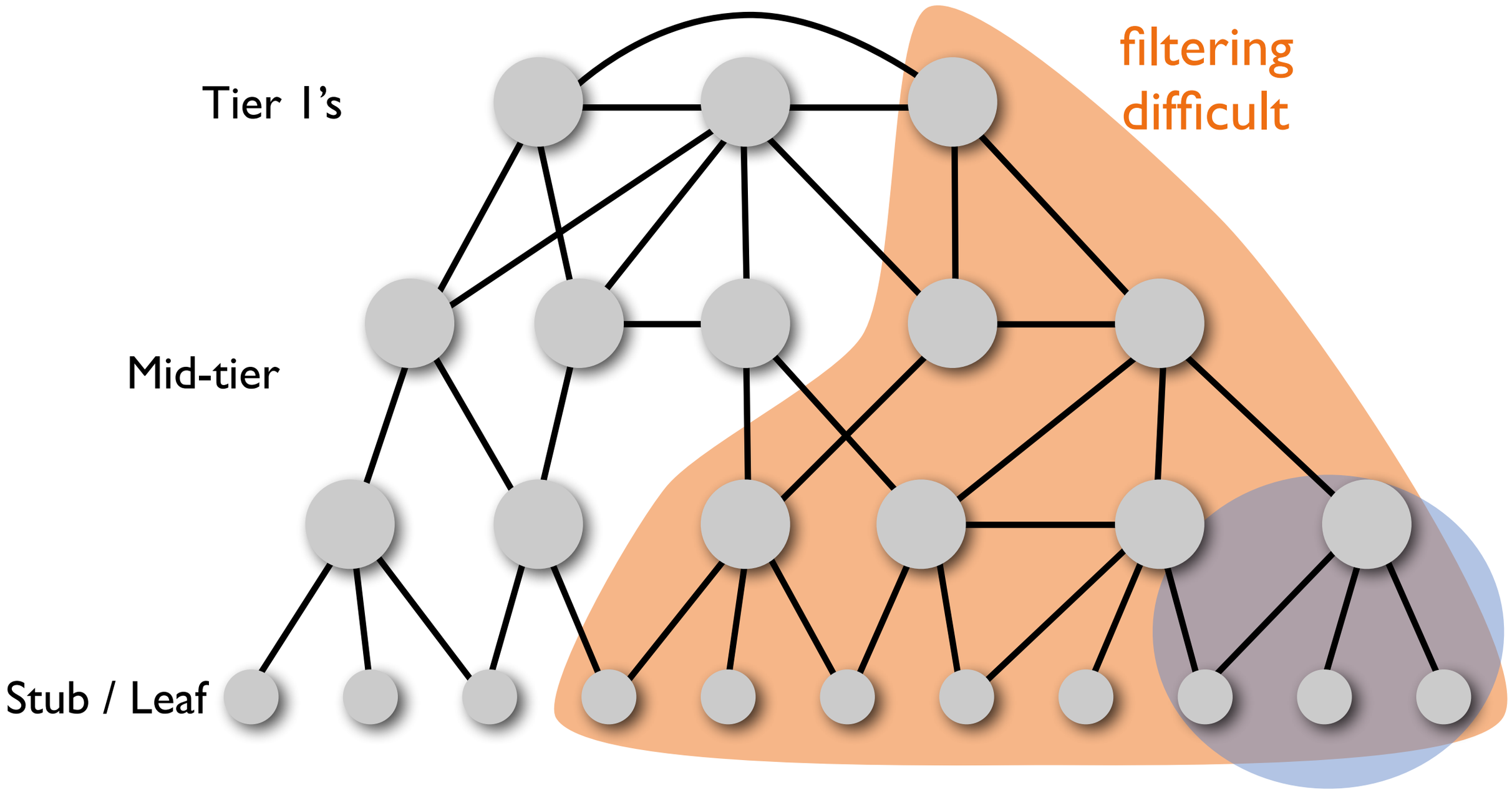


Figure 93 *Source: Arbor Networks, Inc.*

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

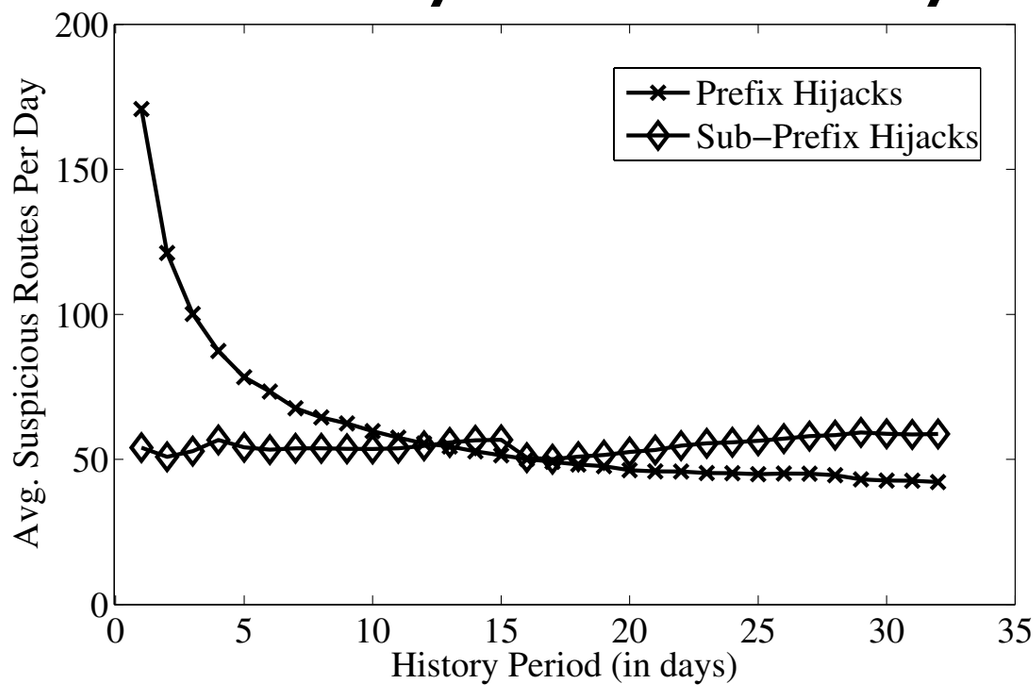


Fig. 1. Average number of announcements (per day) classified as suspicious using a suspicious period of 1 day and a variety of history periods (h).

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

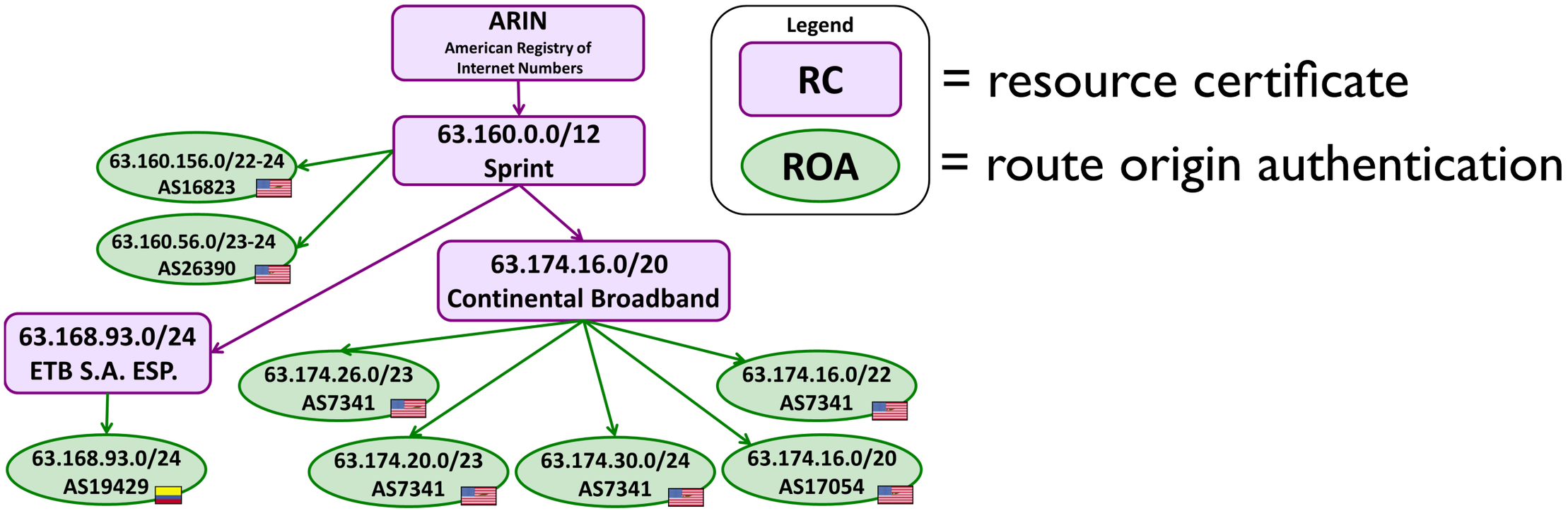


Figure 2: Excerpt of a model RPKI

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

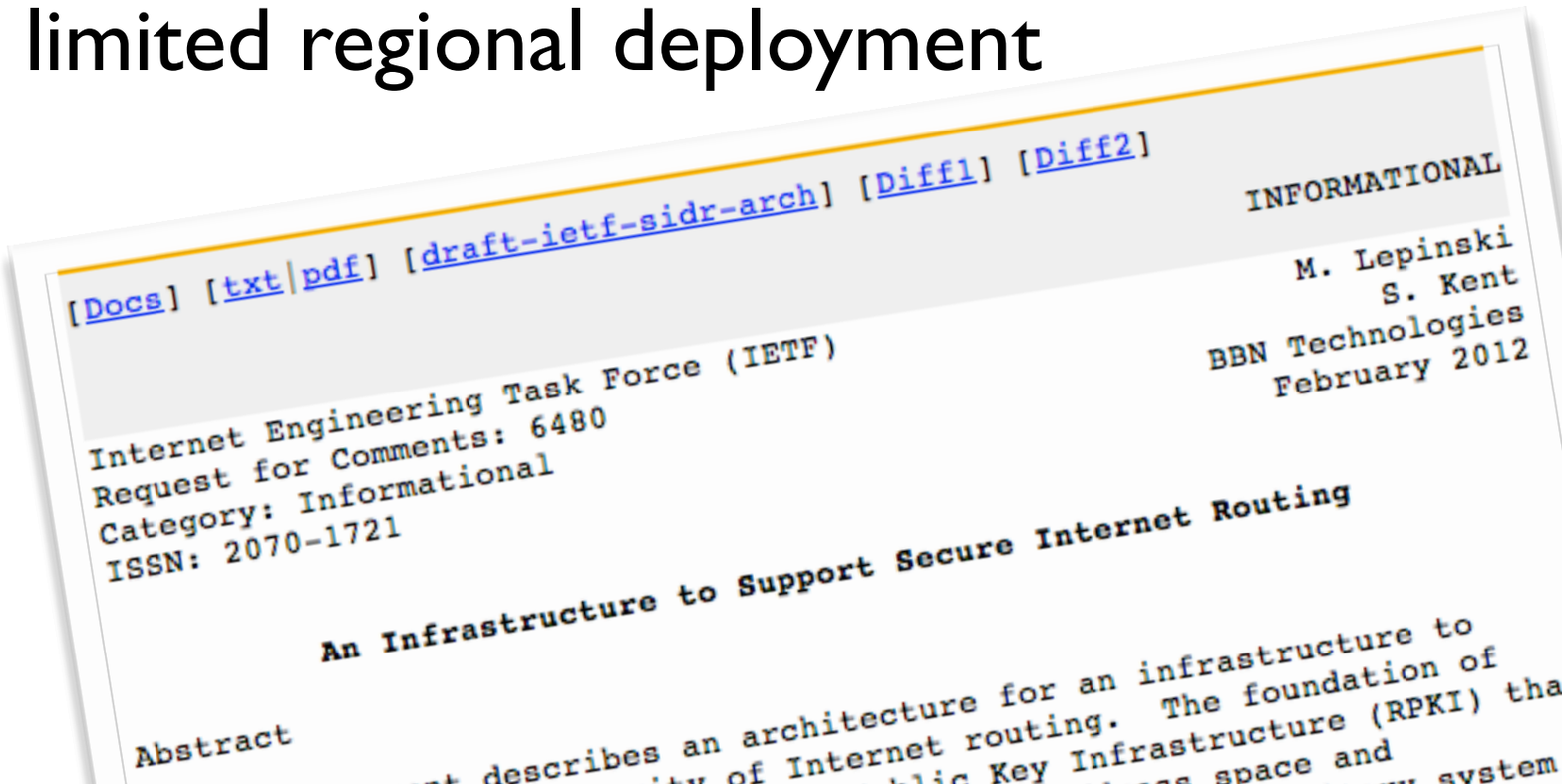
2. Origin Authentication

Deployment challenges

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

Status

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



[Docs] [txt|pdf] [draft-ietf-sidr-arch] [Diff1] [Diff2]

INFORMATIONAL

Internet Engineering Task Force (IETF)
Request for Comments: 6480
Category: Informational
ISSN: 2070-1721

M. Lepinski
S. Kent
BBN Technologies
February 2012

An Infrastructure to Support Secure Internet Routing

Abstract

t describes an architecture for an infrastructure to
ity of Internet routing. The foundation of
ublic Key Infrastructure (RPKI) tha
ss space and
w system

Secure Origin BGP

Scheme

- Origin Authentication + trusted database of AS-level topology
- Announced routes checked against database to see if they are "plausible" (exist in the topology)

Disadvantages

- Requires trusted database
- Route may be plausible without actually having been announced

3. S-BGP

Scheme

- Origin Authentication + hop-by-hop cryptographic validation that path was announced

Deployment challenges

- Requires PKI
- Requires significant computational resources

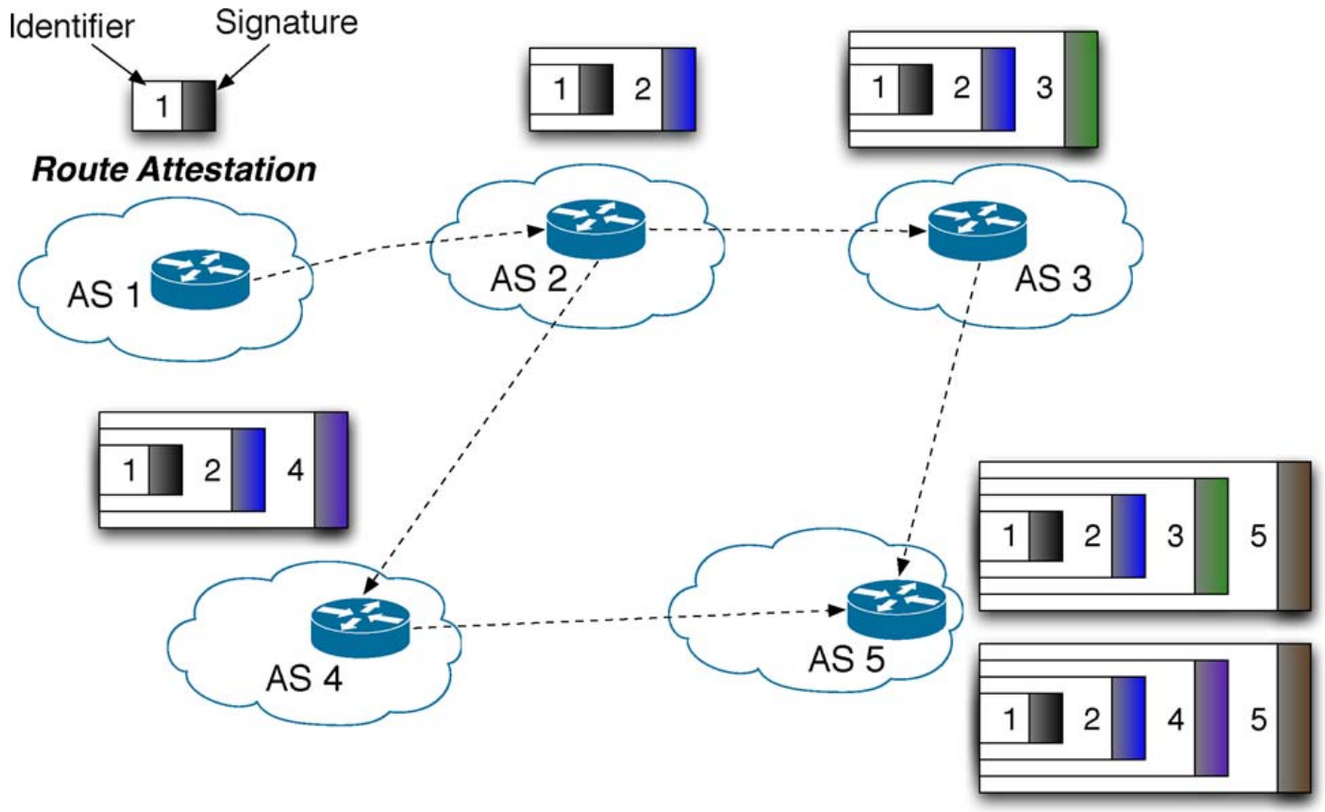
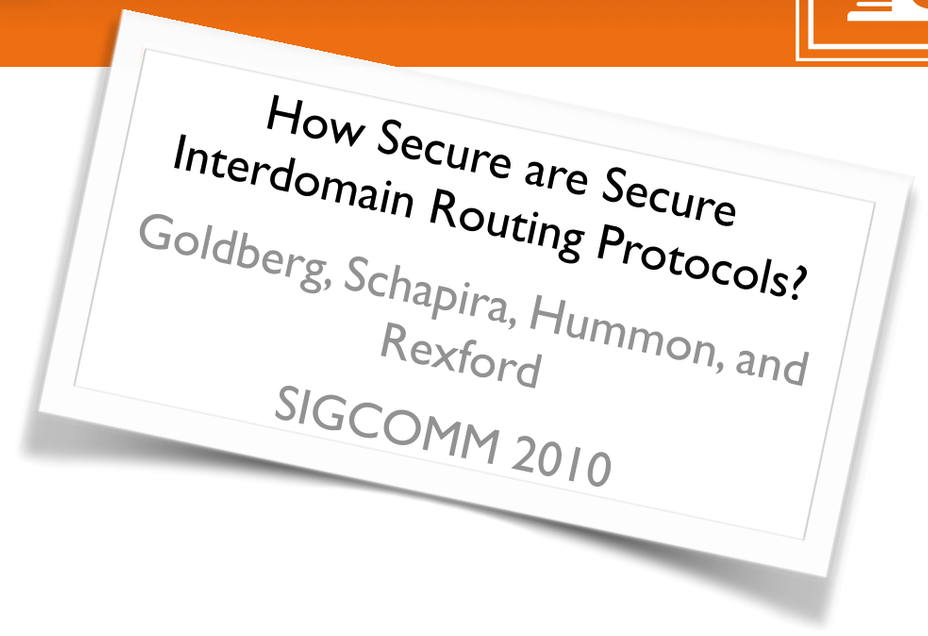


Fig. 5. ***Route attestations in S-BGP. As UPDATE messages are passed between peers, the receiving peer signs the received message before passing it to another neighbor. The result is an "onion-style" attestation that contains signatures from all routers along the path.***

[Diagram from Butler, Farley, McDaniel, Rexford, Proc. IEEE, 2010]

How well do they work?



Quantifying the attack

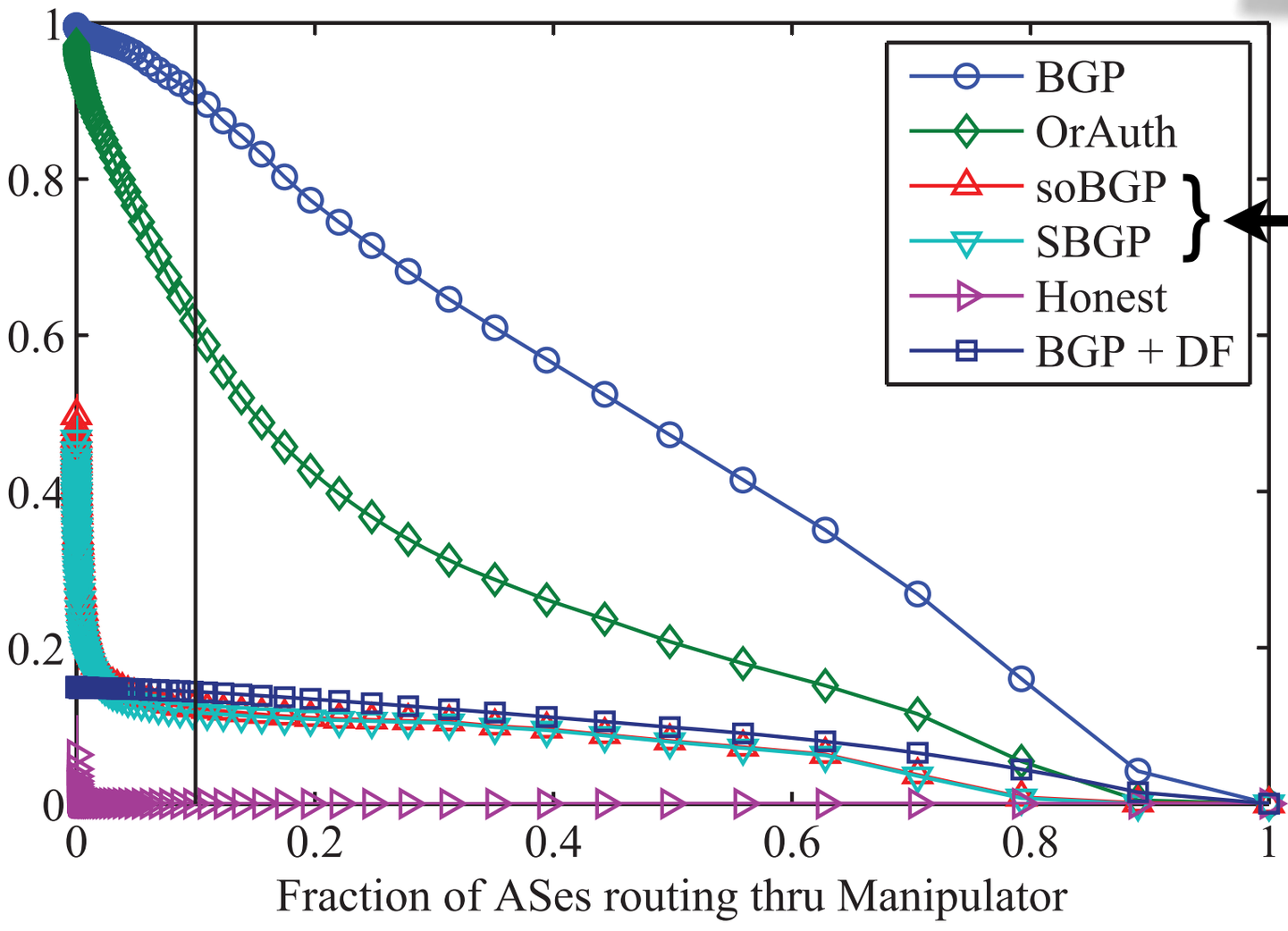
- Attacker's goal: attract traffic
- Measure fraction of ASes attacker can "steal" traffic from

How does the attacker do that?

- Basic "smart" strategy
  - Select or invent 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, and Rexford
SIGCOMM 2010



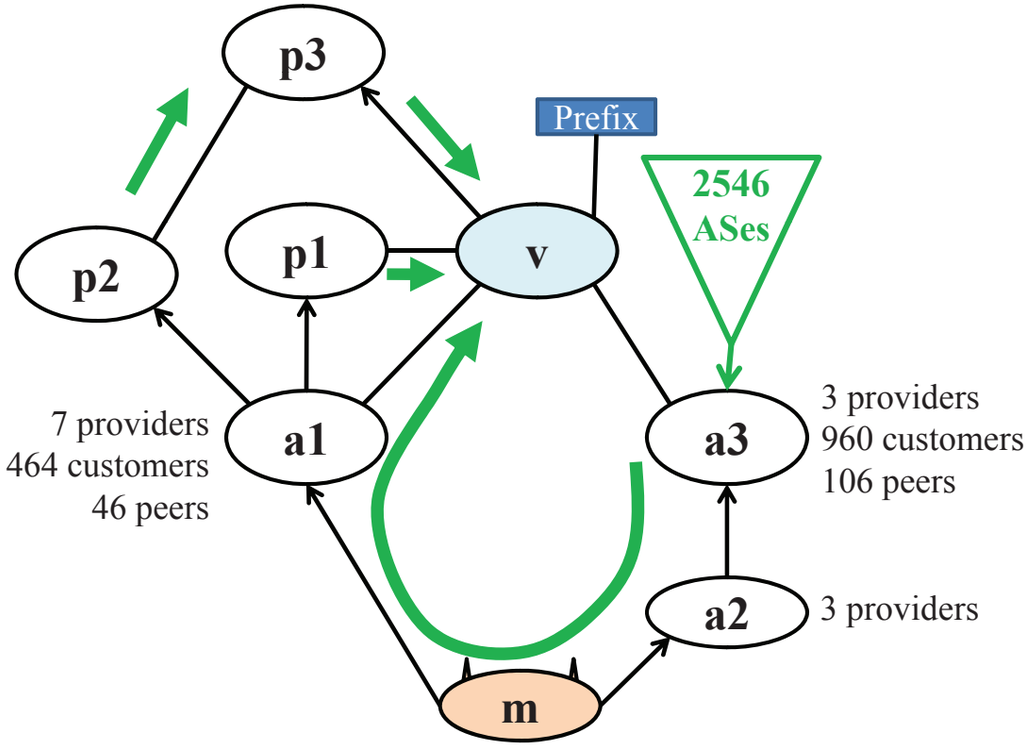
Surprisingly similar

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

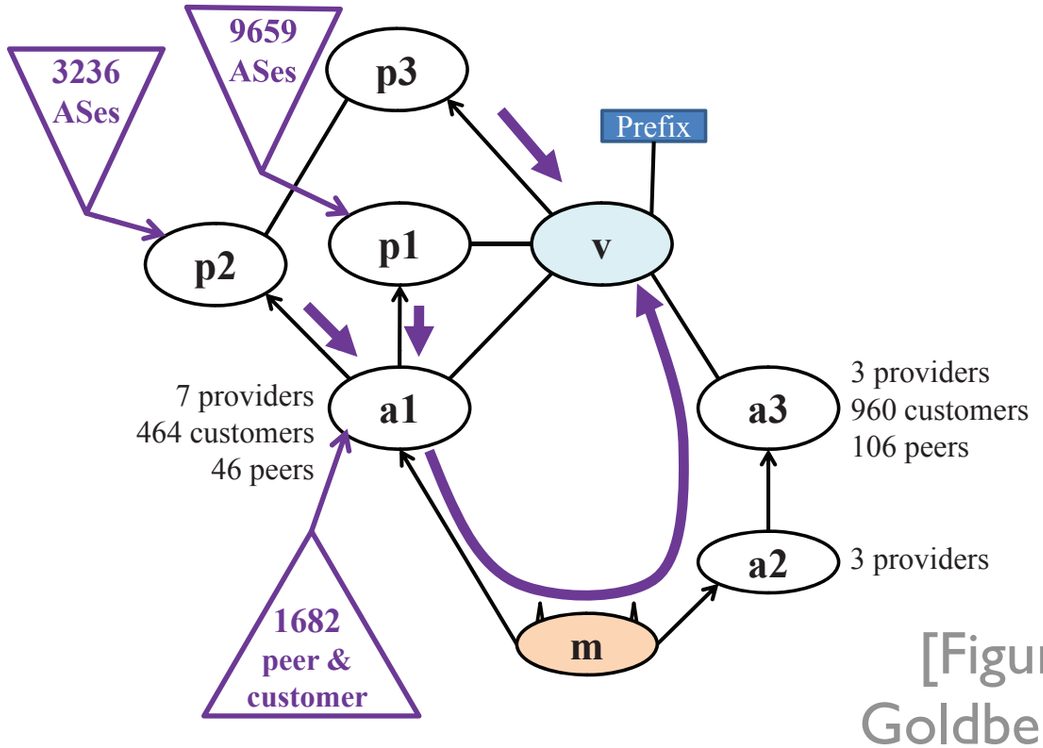
soBGP vs. S-BGP

Two components to successful attack:

- What you announce – soBGP has more flexibility
- Who you announce it to – turns out to matter more



Announce 3-AS path, intercept 5,569 ASes

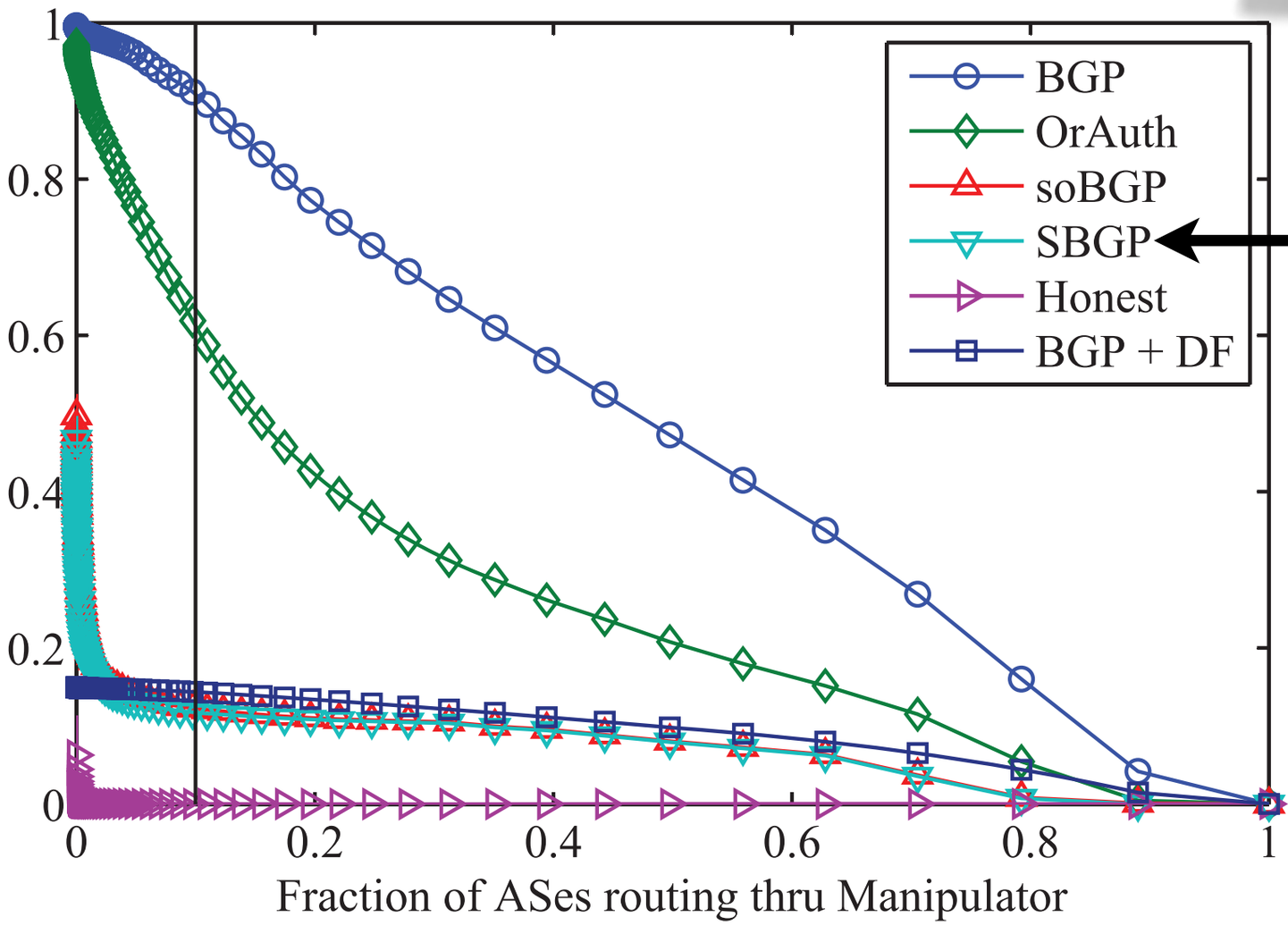


[Figures from Goldberg et al.]

Announce 4-AS path, intercept 18,664 ASes

Results

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



How can this be attacked??!!

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

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

Discussion

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?

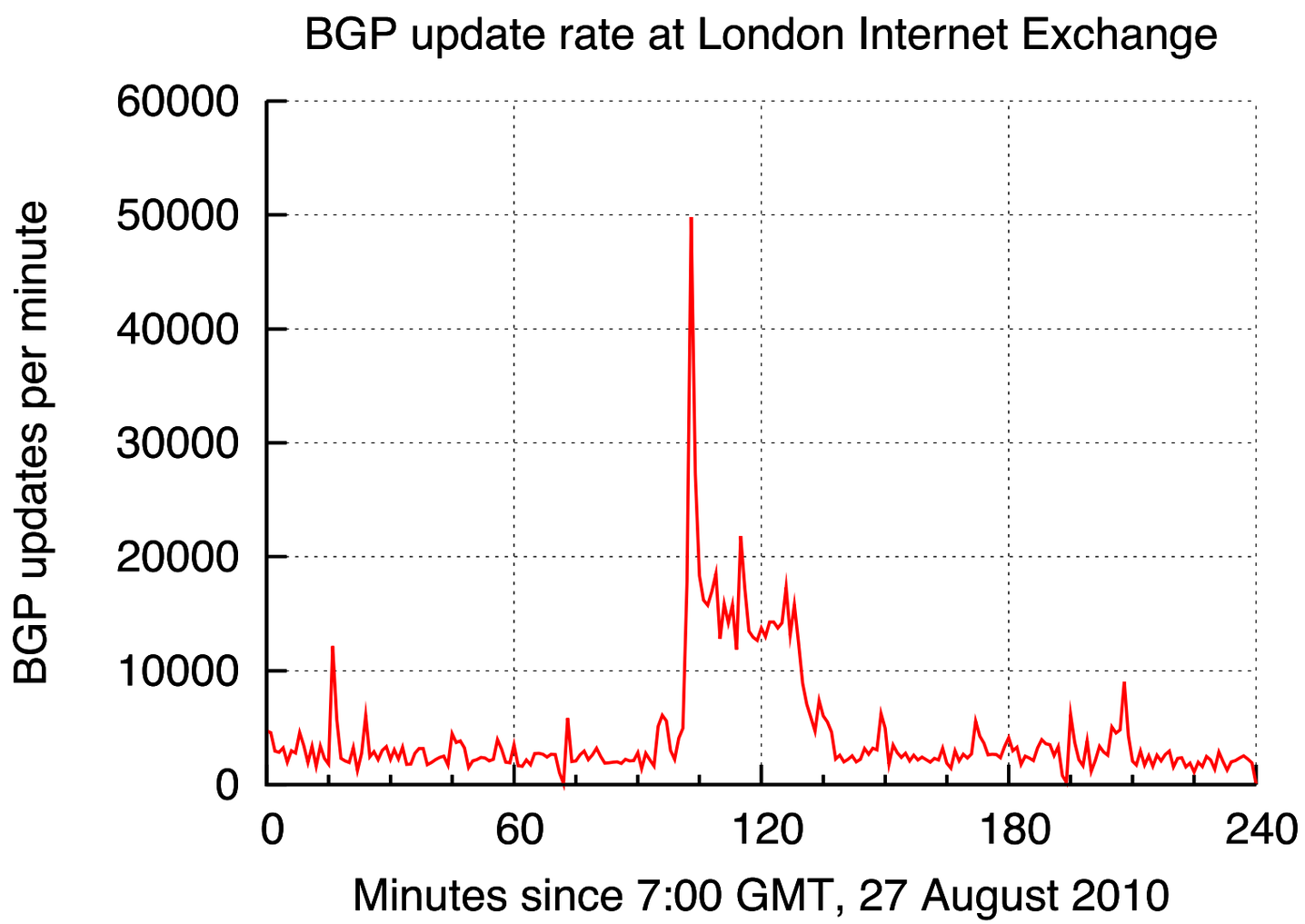
- worst-case scenario: zero-day exploit on large fraction of routers across the entire Internet
- many are running the same software!

A (bad) day in the life of the Internet

About 1% of Internet destinations disrupted for about 30 minutes

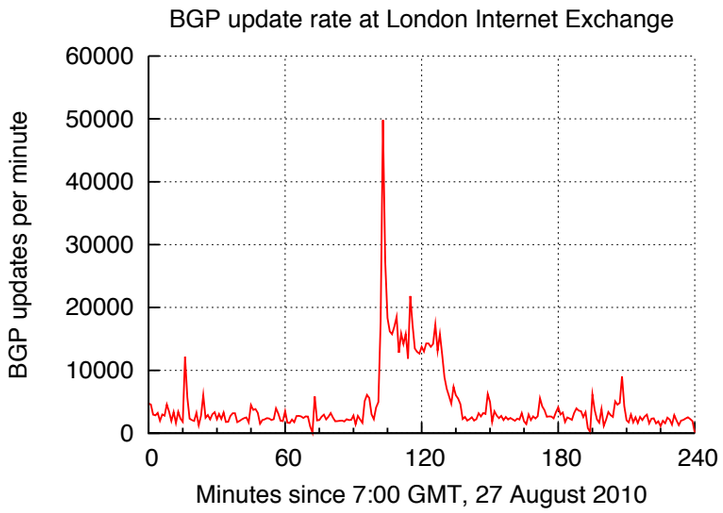
How did this happen?

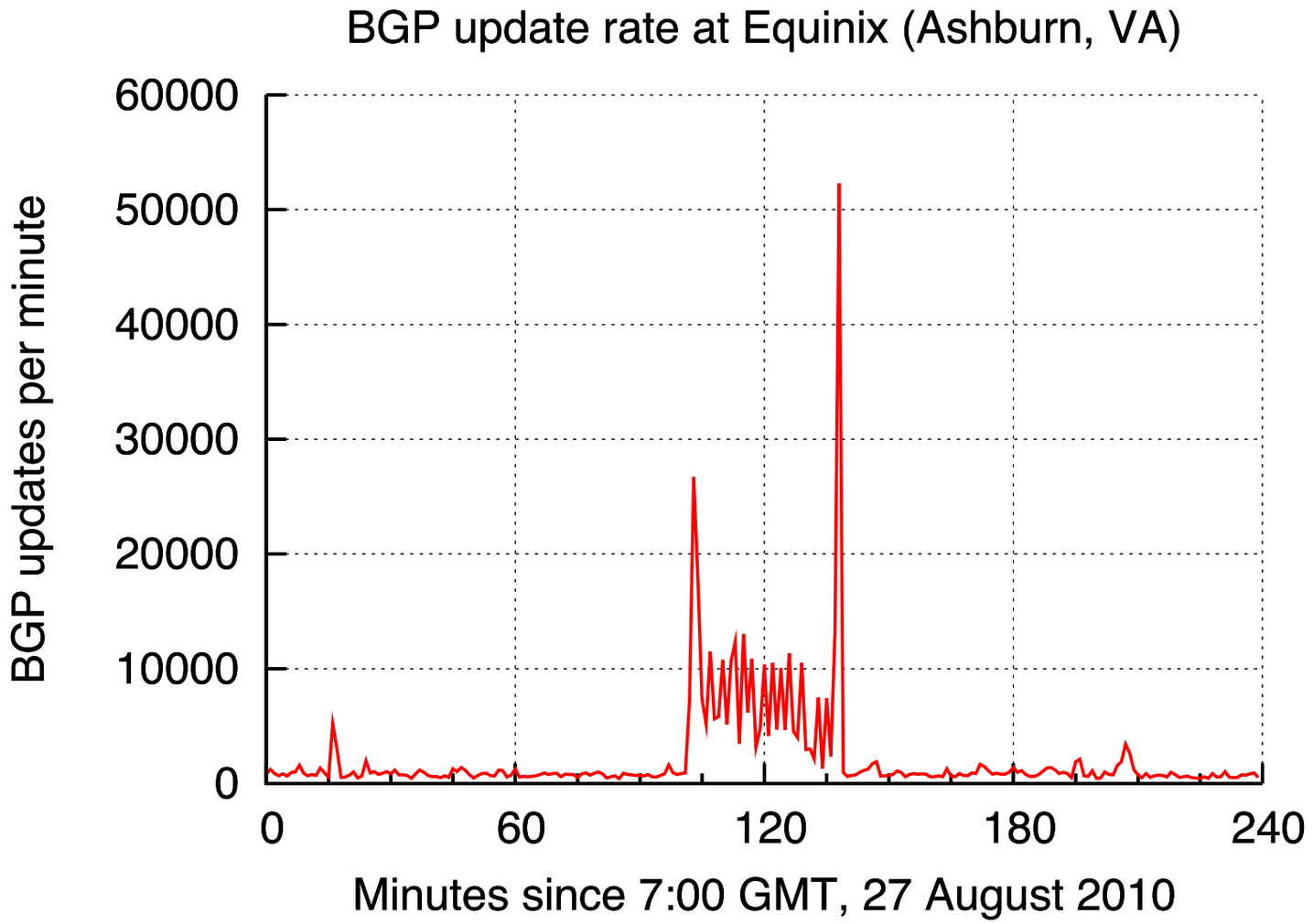
Internet had a bad Friday



[Plots by Brighten based on raw update feeds from Route Views]

Internet had a bad Friday

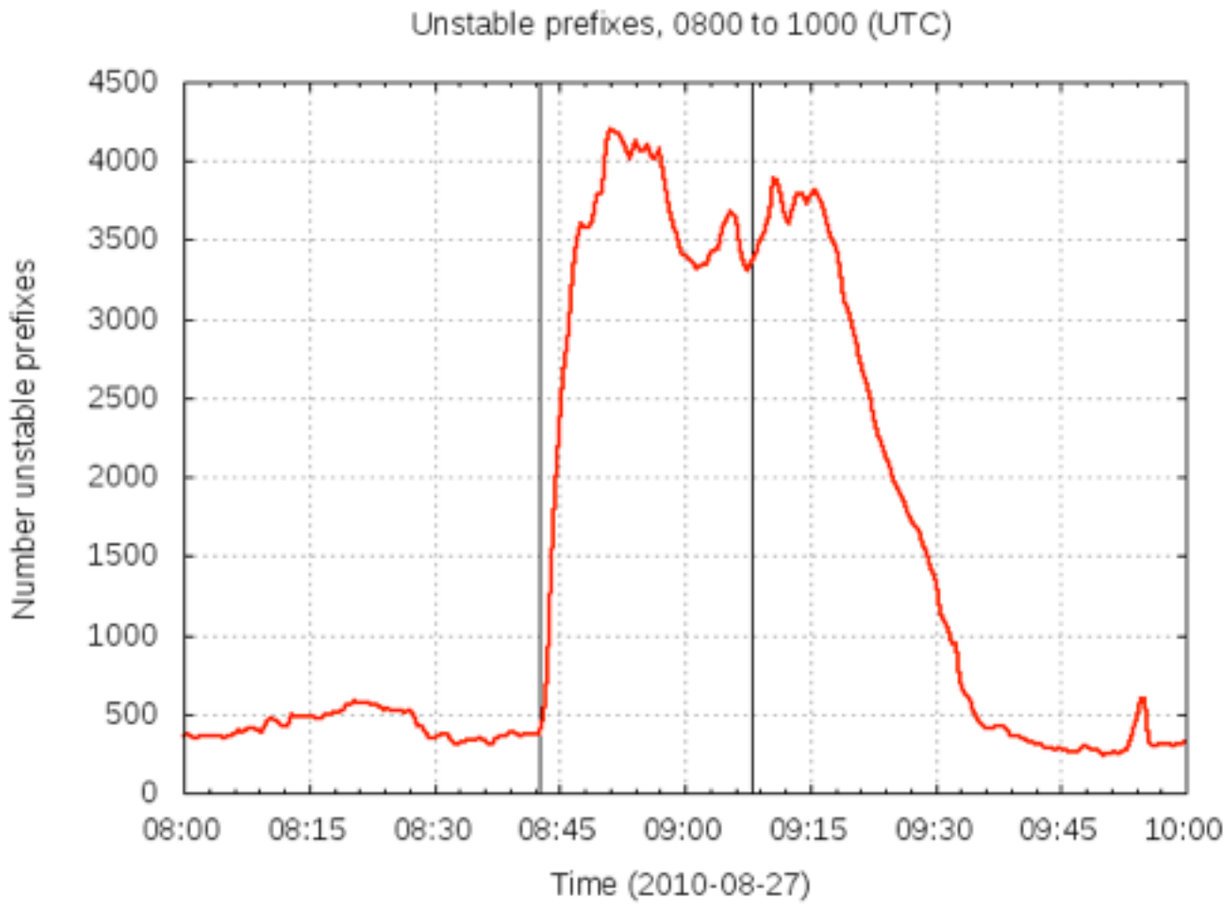


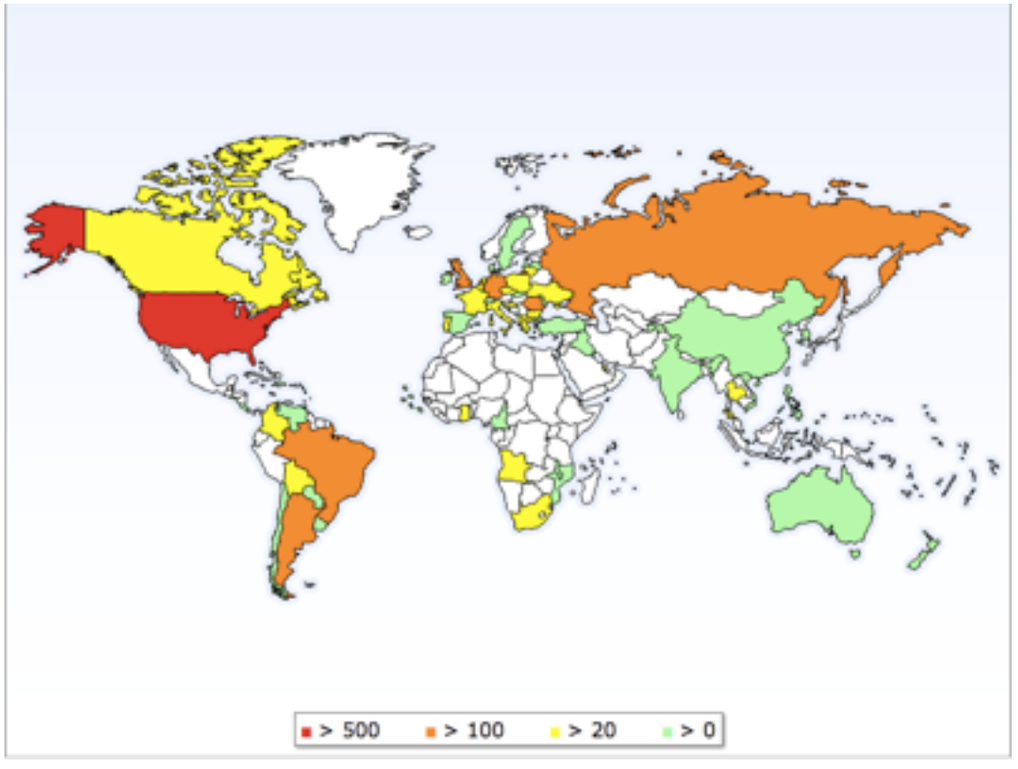


[Plots by Brighten based on raw update feeds from Route Views]

~1% of prefixes affected

[Earl Zmijewski, Renesys]





Brewing a storm

1. An unusual announcement
2. Propagation from router to router
3. Buggy software mangles announcement
4. while(true)
    1. Buggy router propagates announcement to neighbor
    2. BGP session dropped upon receipt of mangled message
    3. BGP session reestablished

Lessons

Many unsavory BGP announcements can be contained, but this one wasn't

- Spread geographically because it was an entirely valid announcement
- Spread to many prefixes because BGP spec lets one bad announcement from a router affect all traffic to that router

Widespread correlated failures from similar software

Bugs and attacks can have similar effects and solutions

- Lucky in this case: bug triggered by researchers, not attackers!

Discussion

Partial deployment crucial. Issues?

Given all this, why does the Internet work so well?

Announcements

Next time: Data Center Network Architecture

Field trip 1:00 pm

- Cars useful to drive over to Blue Waters

Final project presentations Tue May 9, 11am - 2pm

- If you cannot make this, email me by Wednesday; otherwise I will assume you are committed to the 11am May 9 date