Security of BGP

Pehr Söderman
CSC
Pehrs@kth.se

What we will cover today

- Attacks on routing
- TCP security
- The effects of misconfiguration
- The effects of active attacks
- SBGP
- SoBGP

Why would anybody attack BGP...?

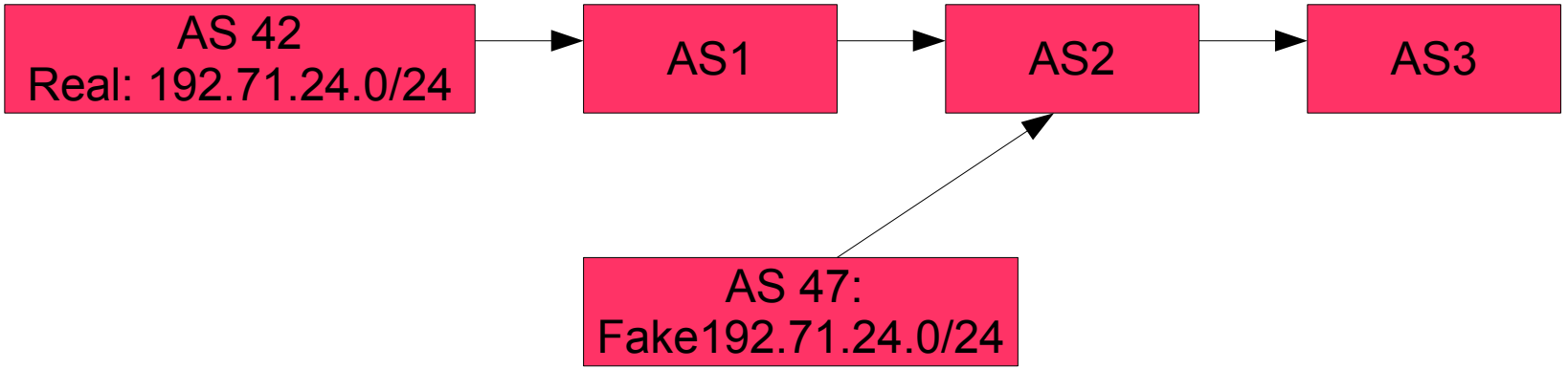
How hard is it to get your hands on a router running BGP?

How much is a router running BGP worth?

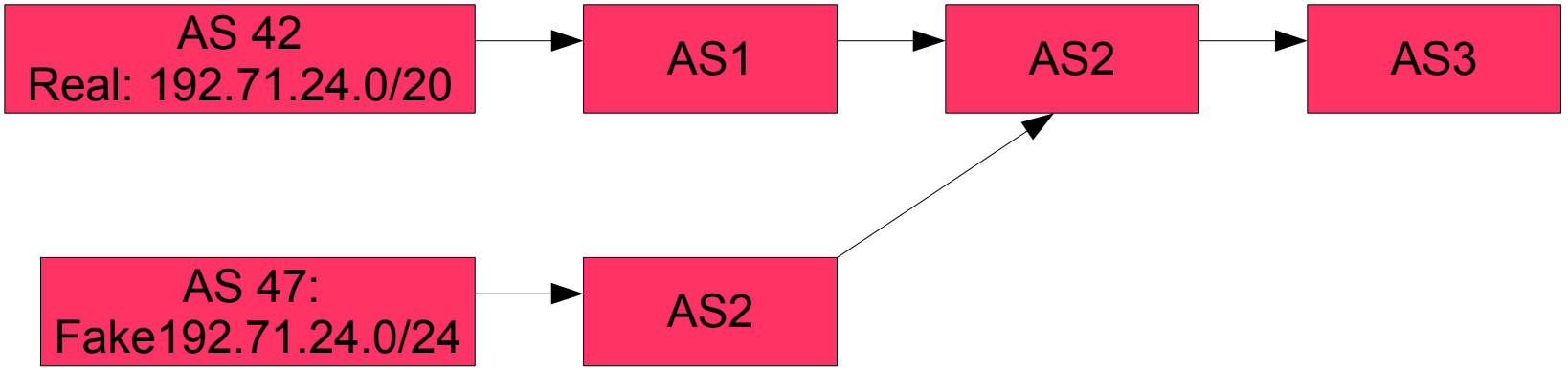
Routing attack objectives

- Blackholing
- Redirection
- Subversion
- Instability

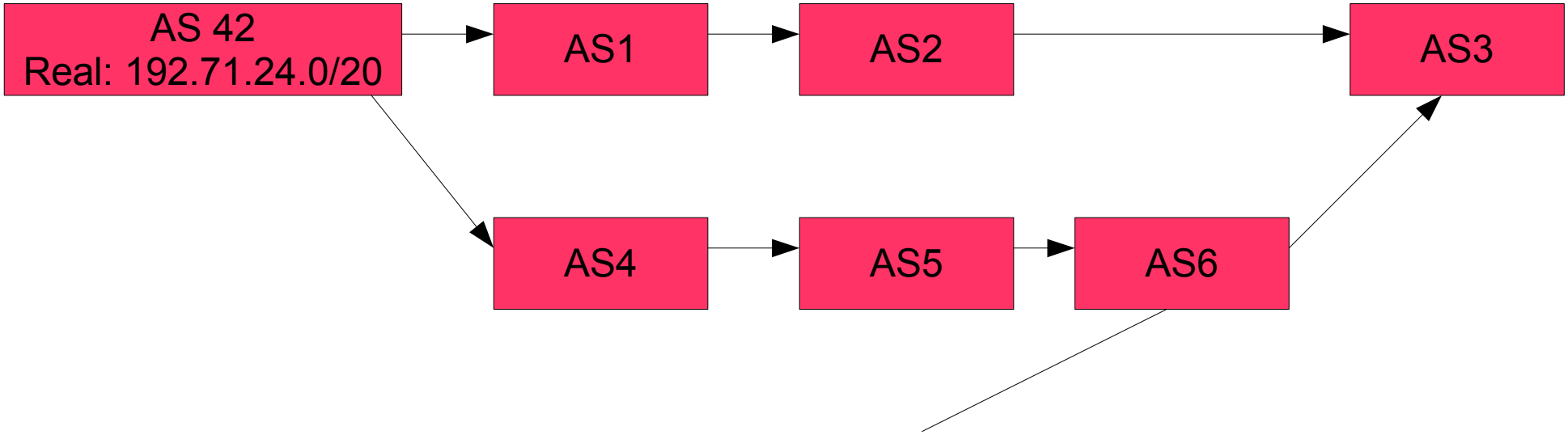
Prefix-Hijacking



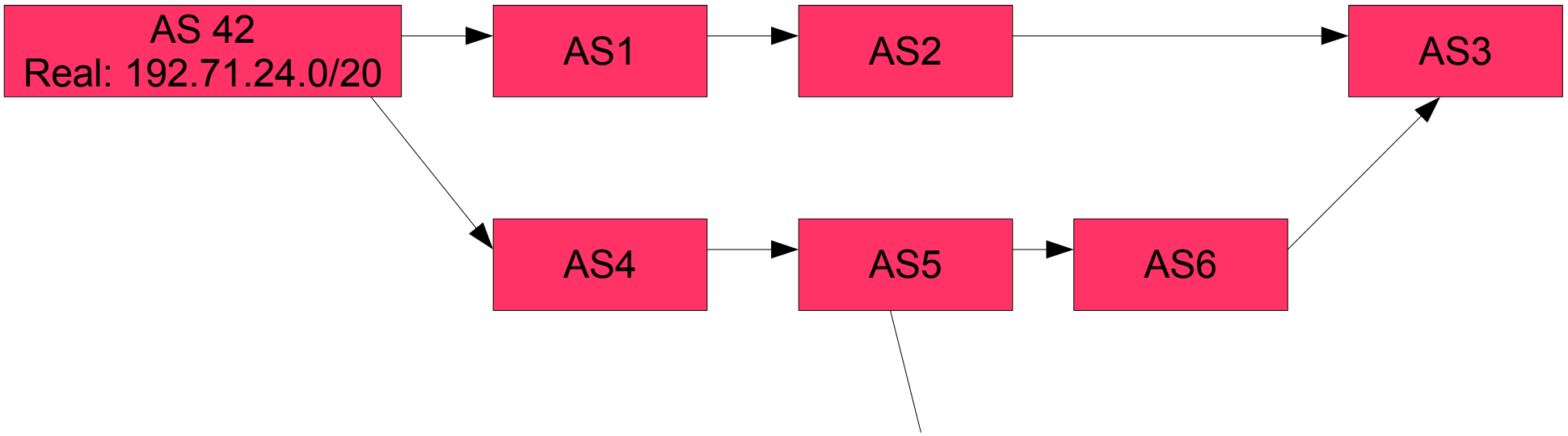
De-Aggregation



Update modifications

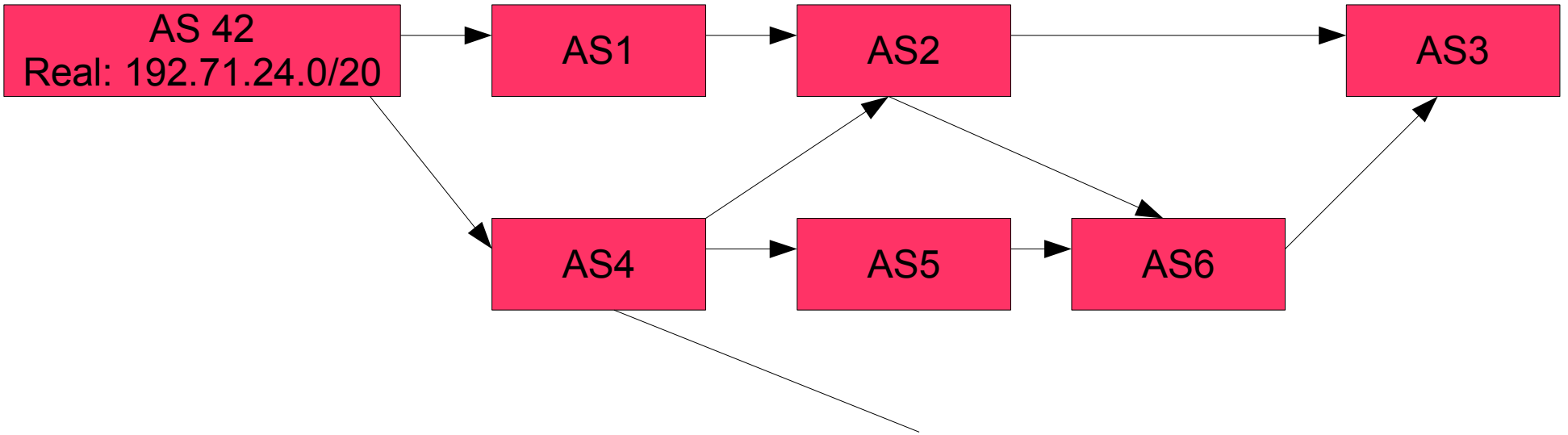


Remote flapping/damping



Up. Down. Up. Down. Up. Down.

General Instability



Flap here. But too rarely for Dampening...

Congestion-induced BGP failure

- The BGP connection runs at the same place as the data
- If we overload the link the bgp keep alive might not get through
  - SQL Slammer
  - CodeRed
  - Nimda
- All caused this kind of failures
- As can large scale DoS attacks.

TCP

- TCP was designed in the happy times when there was no security issues
- TCP was never designed to resist active attacks
- There is NO security in TCP against man-in-the-middle attacks.
- BGP relies on TCP...

Blind injection in TCP

- Match conditions:
  - Source IP (2^{32})
  - Destination IP (2^{32})
  - Source port(2^{16})
  - Destination port (2^{16})
  - Window (2^{32})
- So we need to guess (2^{128}) times to get a packet in... Right?

Major TCP countermeasures

- RFC 2385 (MD5 checksums)
- TTL Security hack
- MaxPrefixLimit
- IPSec

The "AS7007 Incident"

- Catastrophic routing failure 1997
- A single router in AS7007 split Internet up in /24
  - Programming error?
- And announced 2^{24} new routes
  - with itself as the origin
- What do you think happened?
- How would you solve this?
  - As the origin ISP?
  - As any other ISP?

The “AS9121 incident”

- 24 December 2004
- Customer of Turkish ISP spews /24 routes upstream (Over 100000 routes)
- No filtering, possibly malicious attack
- Very slow response due to the date

YouTube off the Internet

Corrigendum- Most Urgent

GOVERNMENT OF PAKISTAN
PAKISTAN TELECOMMUNICATION AUTHORITY
ZONAL OFFICE PESHAWAR
Plot-11, Sector A-3, Phase-V, Hayatabad, Peshawar.
Ph: 091-9217279- 5829177 Fax: 091-9217254
www.pta.gov.pk

NWFP-33-16 (BW)/06/PTA February ,2008

Subject: **Blocking of Offensive Website**

Reference: *This office letter of even number dated 22.02.2008.*

I am directed to request all ISPs to immediately block access to the following website

URL: http://www.youtube.com/watch?v=o3s8jtvvg00

IPs: 208.65.153.238, 208.65.153.253, 208.65.153.251

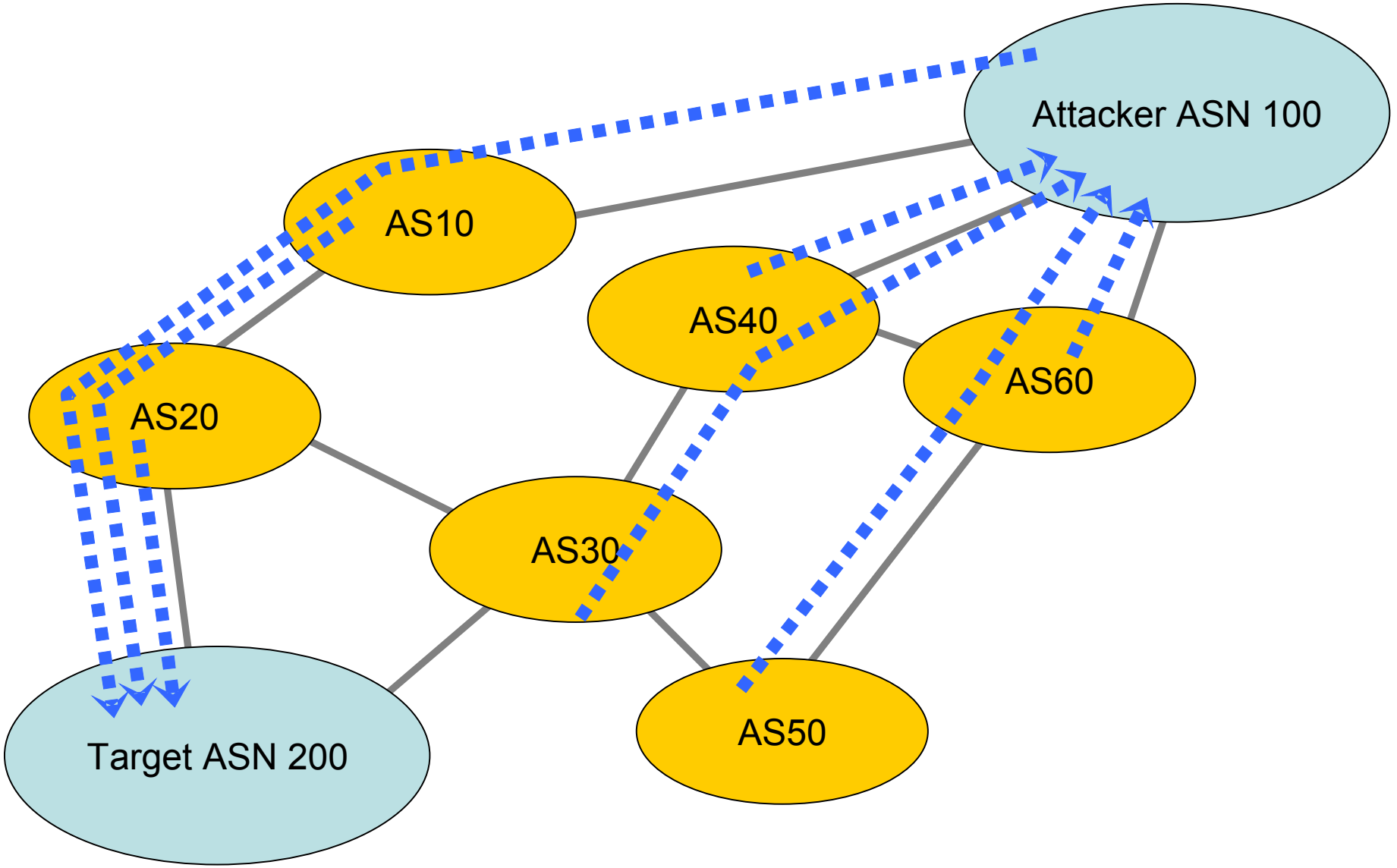
Compliance report should reach this office through return fax or at email peshawar@pta.gov.pk today please.

Deputy Director
(Enforcement)

To:
1. M/s Comsats, Peshawar.
2. M/s GOL Internet Services, Peshawar.
3. M/s Cyber Internet, Peshawar.
4. M/s Cybersoft Technologies, Islamabad.
5. M/s Paknet, Limited, Islamabad
6. M/s Dancom, Peshawar.
7. M/s Supernet, Peshawar.

And these were accidents...
Lets have a look at a malicious attack!

Defcon 2008 HACK



How would you solve these issues?

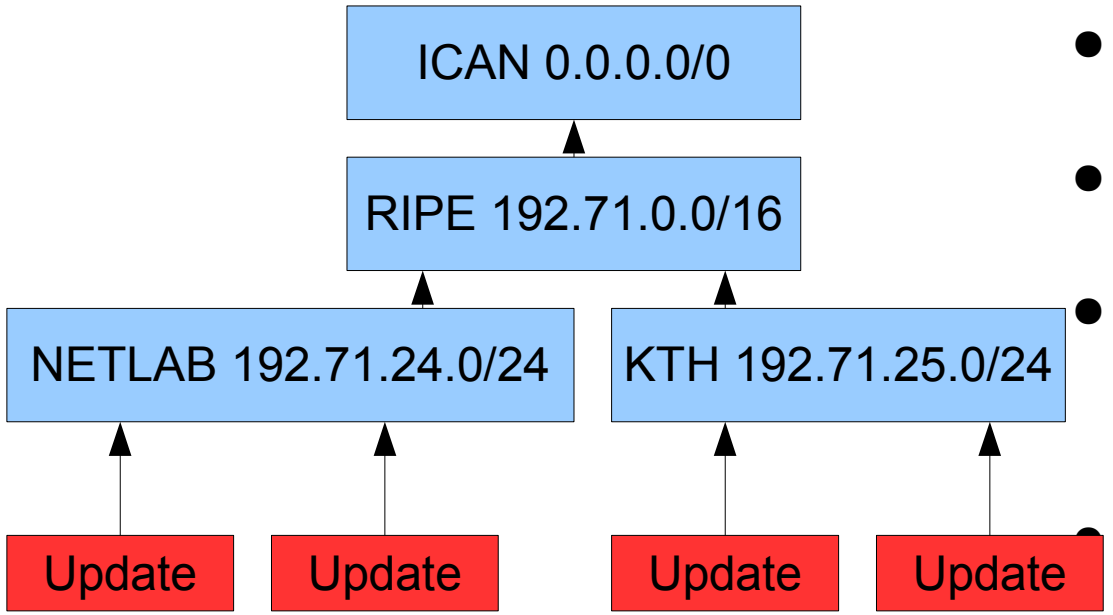
Route filtering

- We have Egress and Ingress filters
  - Egress protects us against becoming transit
  - Ingress protects us against everything else
- It's especially important to filter customer data
- We use RIPE and similar databases
  - They are out of date!
- Static filters are against the principles of routing!
- Many ISP just trusts their peers...

The SBGP Proposal

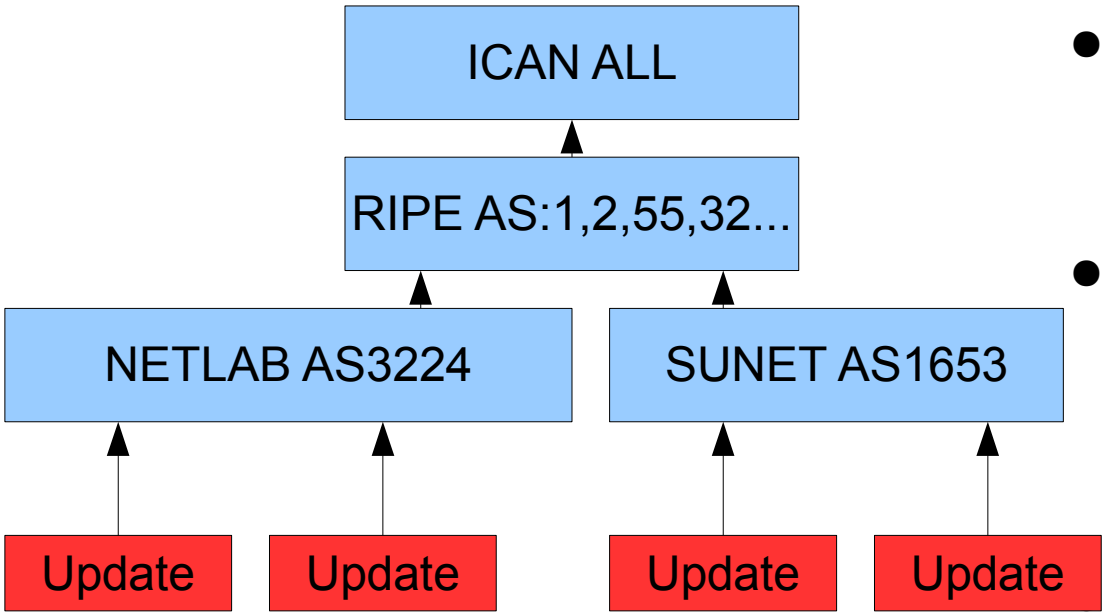
- Use cryptography to secure the infrastructure
- We need:
  - A global, correct, database over prefix owners
  - A globally trusted PKI
  - Cryptographic keys in all routers
  - A new BGP implementation
- Is this hard?

Address Attestation



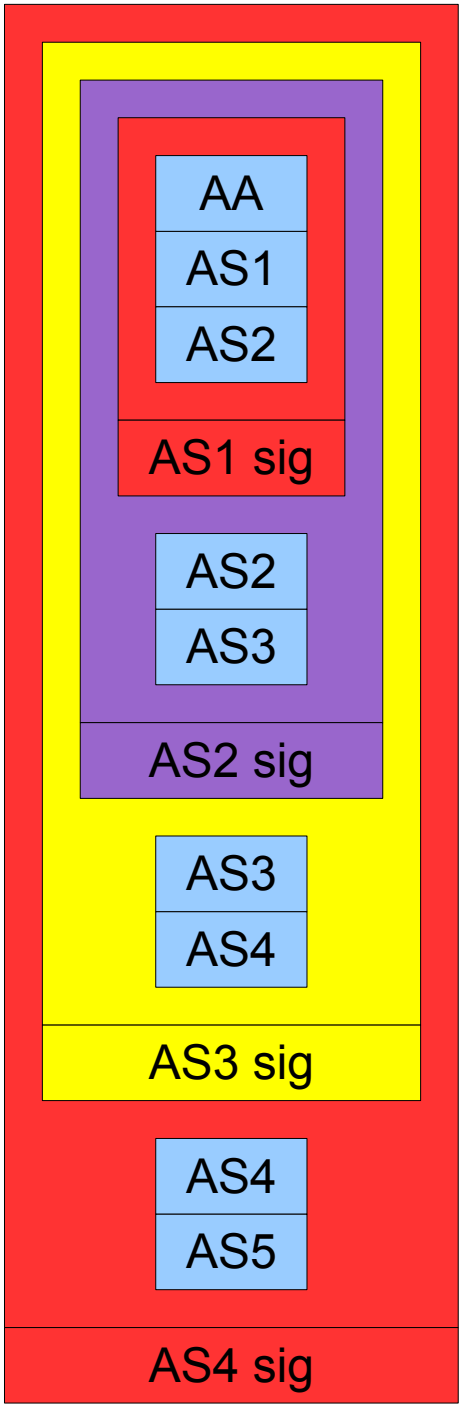
- Binds AS-Prefix
- Hirarchial structure
- Generated by originating AS
- Signed by key from a certificated traceable up to ICAN

Route attestation

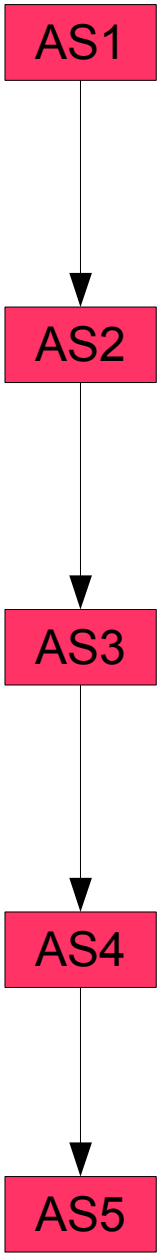


- Each router has a certificate
- These certificates have a similar structure to AA certs

Certs sign each update before it's transmitted



Route Attestation



- Secures one hop in the AS-Path
- A router only creates a signature for the next hop
- But verifies all signature
- Overhead: Around 800%

Limitations of SBGP

- Collusion/Wormhole attacks
- No aggregation outside the origin AS
- Increased risk of route churn
- No binding between RA and AA
- What do we do if we can't read the PKI?
- How effective is it?

Route Filter vs SBGP

Attack	Route Filter	SBGP
Prefix Hijack	Some protection	Secure
De-Aggregation	No protection	Secure
Modified Update	No protection	Some protection
Remote Link flap	No protection	No protection
Instability	No protection	No protection

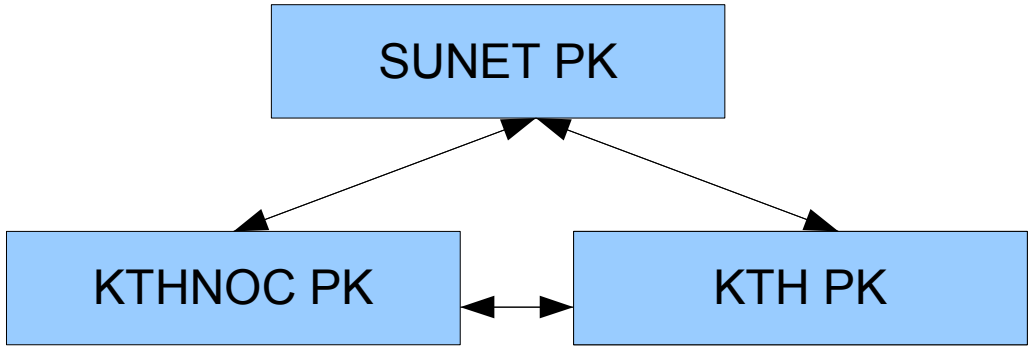
Implementation issues

- The global table is getting close to 300000 entries
  - Assume 5 AS hop/prefix
  - That is 1'500'000 signatures to check
  - Doing this on initialization is not acceptable
- Routers may lack the memory to store the keys
- Online PKI?
- We need new BGPv4 implementations...
- Any other issues?

SoBGP

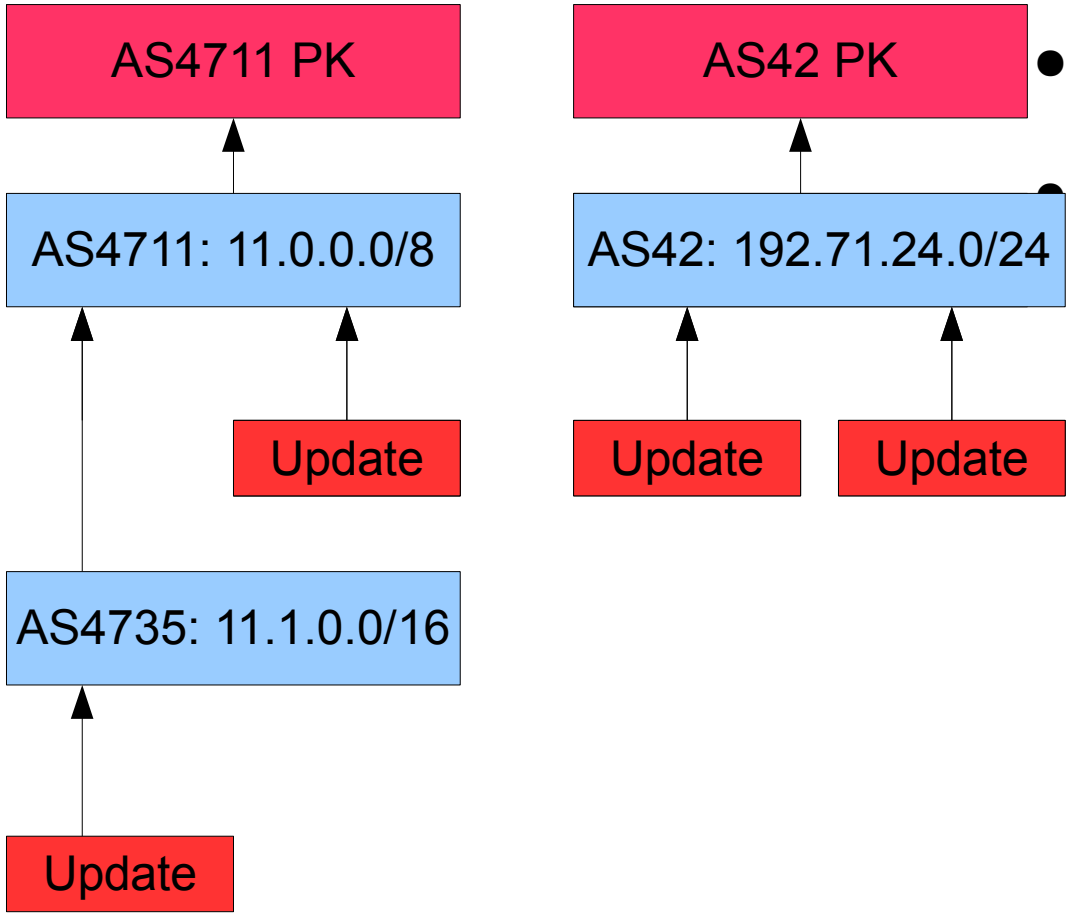
- Proposal from Cisco
- Less computationally intensive than SBGP
- Uses a Web of Trust model instead of hierarchical PKI

Entity certs



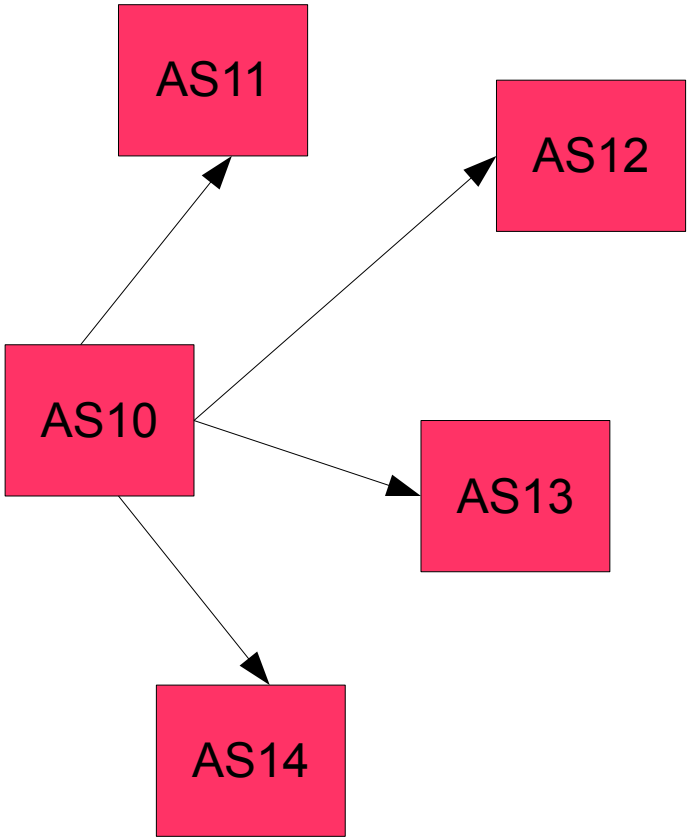
- Binds public key to owner
- Replaces the PKI
- Web of Trust structure

AuthCerts



- Binds AS-Prefix
- Signed by owner
- Web of Trust model
  - As you remember

PolicyCert



- Lists the Peerings of an AS
  - We require symmetric relationships!
  - AS can be marked NoTransit
- Lists policy information
  - Longest prefix
  - etc.
- Combine these to build a global database

Conclusions?

SBGP vs SoBGP vs Route Filter vs Nothing

What you should know now

- Routing attack objectives
- Various attacks on BGP
- TCP related countermeasures
- Some historical attacks on BGP
- Route filtering
- Fundamentals of SBGP
- Fundamentals of SoBGP
- Limitations of SBGP and SoBGP

Recommended reading

- Beware of BGP Attacks (Nordström, Dovrolis)
  - http://www.cs.princeton.edu/%7Ejrex/teaching/spring
  - Much Much better than the book on BGP
- RFC 4272
- YouTube Hijacking: A RIPE NCC RIS case study
  - http://www.ripe.net/news/study-youtube-hijacking.htr
- Wired Coverage of the DefCon Hack
  - http://blog.wired.com/27bstroke6/2008/08/how-to-int