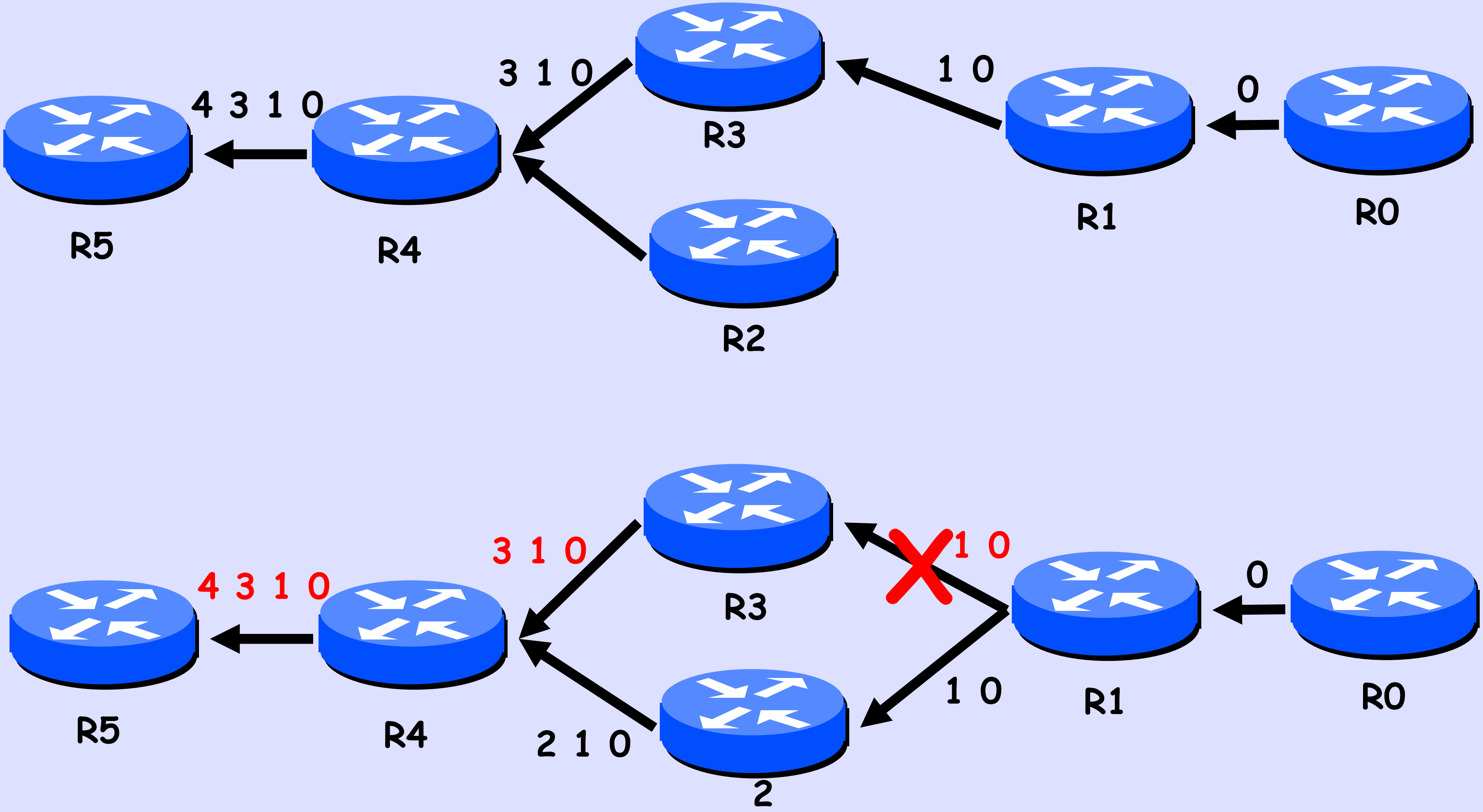
BGPsec Beaconing for Replay Reduction

sidr wg / Québec City

2011.07.28

Randy Bush <randy@psg.com>
Steve Bellovin <smb@cs.columbia.edu>

Replay Attack



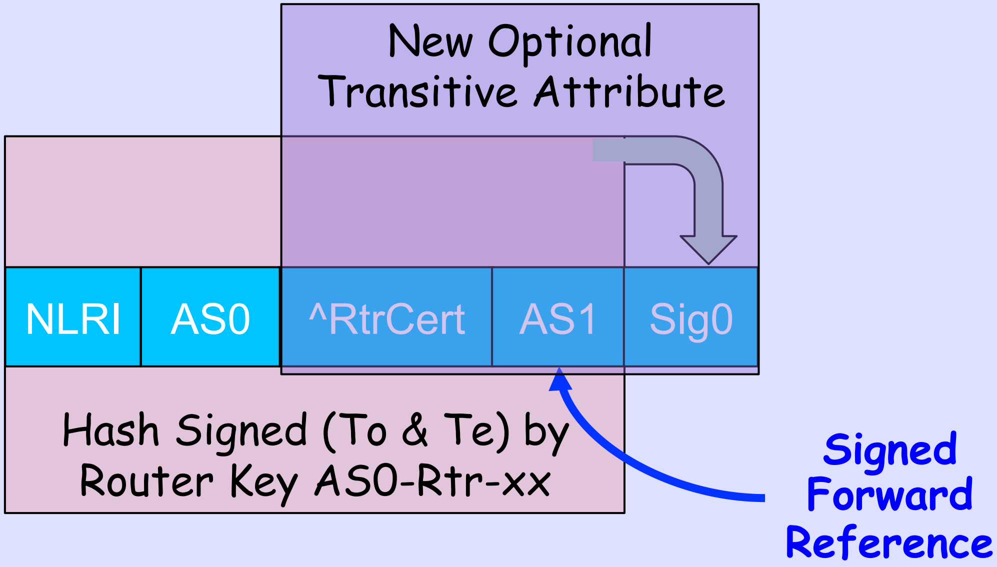
Why Replay?

- Provider is pissed off at customer who switches
- Prefix 'stuck' in router, needs manual whacking
- All these things are at human time scale
- I.e. replay attacks are at human time scale

Replay Reduction

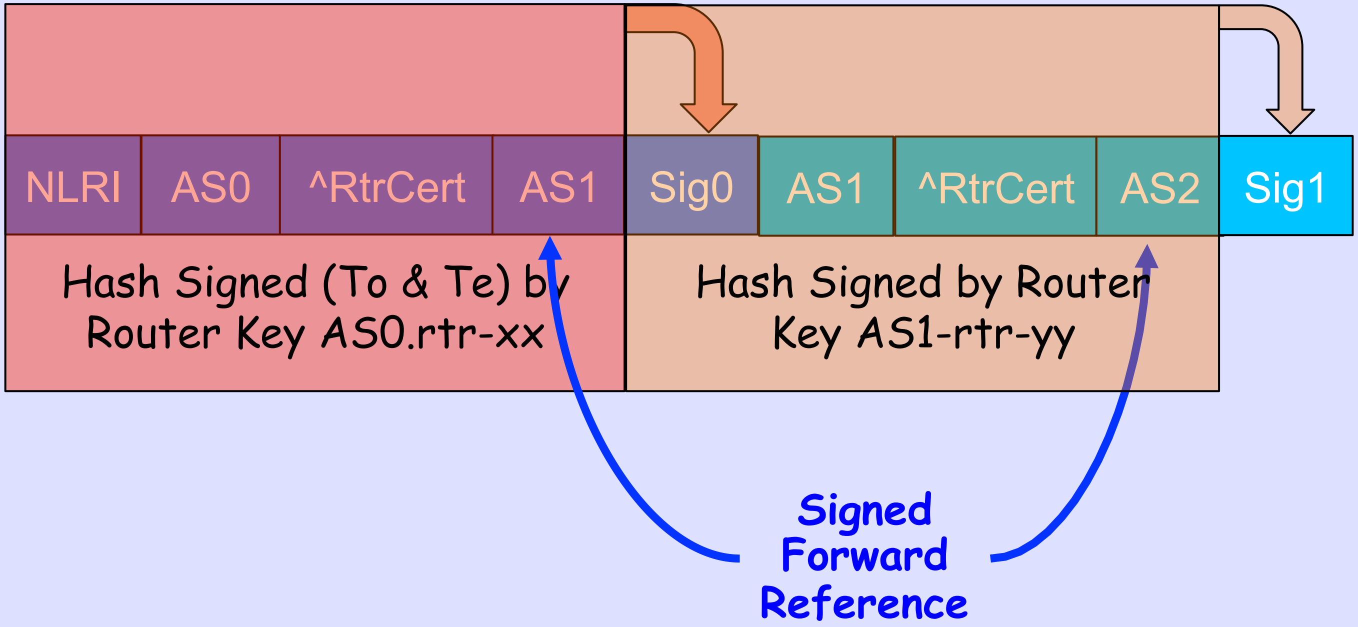
- Announcement replay is a vulnerability
- Therefore freshness is critical
- So originating announcer signs with a relatively short signature lifetime
- Origin re-announces prefix well within that lifetime, AKA ***beaconing***
- Suggested to be days, but can be hours for truly critical infrastructure

Origination by AS0 to AS1


New Optional Transitive Attribute
NLRI
AS0
^RtrCert
AS1
Sig0
Hash Signed (To & Te) by Router Key AS0-Rtr-xx
Signed Forward Reference

- To and Te are times of signature origination and expiration
- Signature has a well-jittered validity end time, Te, of days
- Re-announcement by origin, AKA *beaconing*, every ~(Te-To)/3
- ROA is not needed as prefix is sufficient to find it in RPKI as today

Announcement AS1 to AS2


NLRI
AS0
^RtrCert
AS1
Sig0
AS1
^RtrCert
AS2
Sig1
Hash Signed (To & Te) by Router Key AS0.rtr-xx
Hash Signed by Router Key AS1-rtr-yy
Signed Forward Reference

- R1 signing over R0's signature is same as signing over entire R0 announcement
- Non-originating router signatures do not have validity periods
- But when they receive a beacon announcement, they must propagate it

Non-Goal

Replay Elimination

We do not know how to do this

The goal is reducing the vulnerability time window

Protocol Not Intent

- We can not know intent, **should** Mary have announced the prefix to Bob?
- But Joe can formally validate that Mary **did** announce the prefix to Bob
- Policy on the global Internet changes every 36ms
- We already have a protocol to distribute policy or its effects, it is called BGP
- BGPsec validates that the protocol has not been violated, and is not about intent or business policy

Why Multi-Beacon

- Someone four hops down has made a contract with the devil
- They may want to get out of it more quickly than the origin cares
- And this is for the origin's prefix not the contractor
- So this is a kinky far corner case
- Fine if it's cheap, but it isn't

Believe Only Previous TTL

- A originates the announcement
- If everyone beacons, assume the beacon TTL applies only to that hop
- B gets it from A, C gets it from B, D gets it from C
- D can keep sending the announcement, even though C's TTL expired. Oops!

So Believe Minimum TTL

- So try believing minimum TTL in chain
- But are all redundant to the first, since if that one expires none of the others should even be sent
- An intermediate might want a lower one, in case its downstream link goes down, but why?
- The downstream neighbor will announce a different path, but to those further still downstream that is indistinguishable from many other causes of seeing a different path from your upstream
- And there's no real reason for an intermediate node to want to beacon because it has no skin in the game

Alternatively

- RPKI mechanisms could be used to achieve the same goals
- With O(day) propagation times, which is probably OK
- But with manual intervention, not automagically, ops pain

What it Costs

- Origin-only beaconing O(once a day) costs a few percent
- Every hop beaconing raises that cost by a significant factor
- And if a large ISP does a Dollar Attack on a vendor and cranks the beacon time down, this could all be quite expensive

Bottom Line

- For the small benefit, are beacons worth it at all?
- For the small cost of origin-only beacons, and iff they can be kept O(day), they are probably worth it
- They do help clear wedgies! ☺
- But multi-beaconing is neither useful nor affordable