

Auto-Detecting Hijacked Prefixes?

Routing SIG
7 Sep 2005
APNIC20, Hanoi, Vietnam

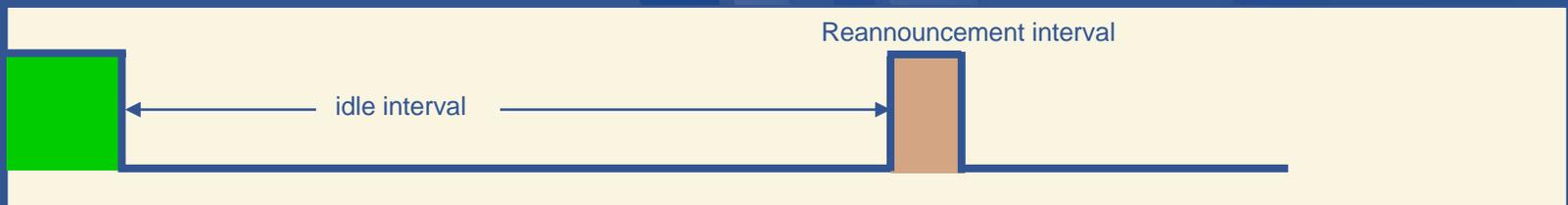
Geoff Huston

Address hijacking

- Unauthorized use of an address prefix as an advertised route object on the Internet
 - Not a bogon
 - address block has been assigned by an RIR for use
 - May include identity fraud
 - may involve misrepresentation of identity in order to undertake a database change
 - Commonly associated with identity cloaking
 - Spam generation, attack launching platforms, etc
- How prevalent is this?
 - Very hard to isolate hijacking incidents

What is a hijack signature?

- What address blocks would not be noticed if they were used for a short period?
 - Has been unadvertised for a 'long time'
 - Is used only for a 'short time'
 - Uses an entirely different origin AS and first hop AS
 - Is not covered by an aggregate announcement



Data collections

- Aggregated BGP route collection data
- Can provide information for any prefix:
 - When was this prefix advertised and withdrawn?
 - What was the announcing AS?
 - What was the first hop AS?
 - What other prefixes were also advertised at the same time?

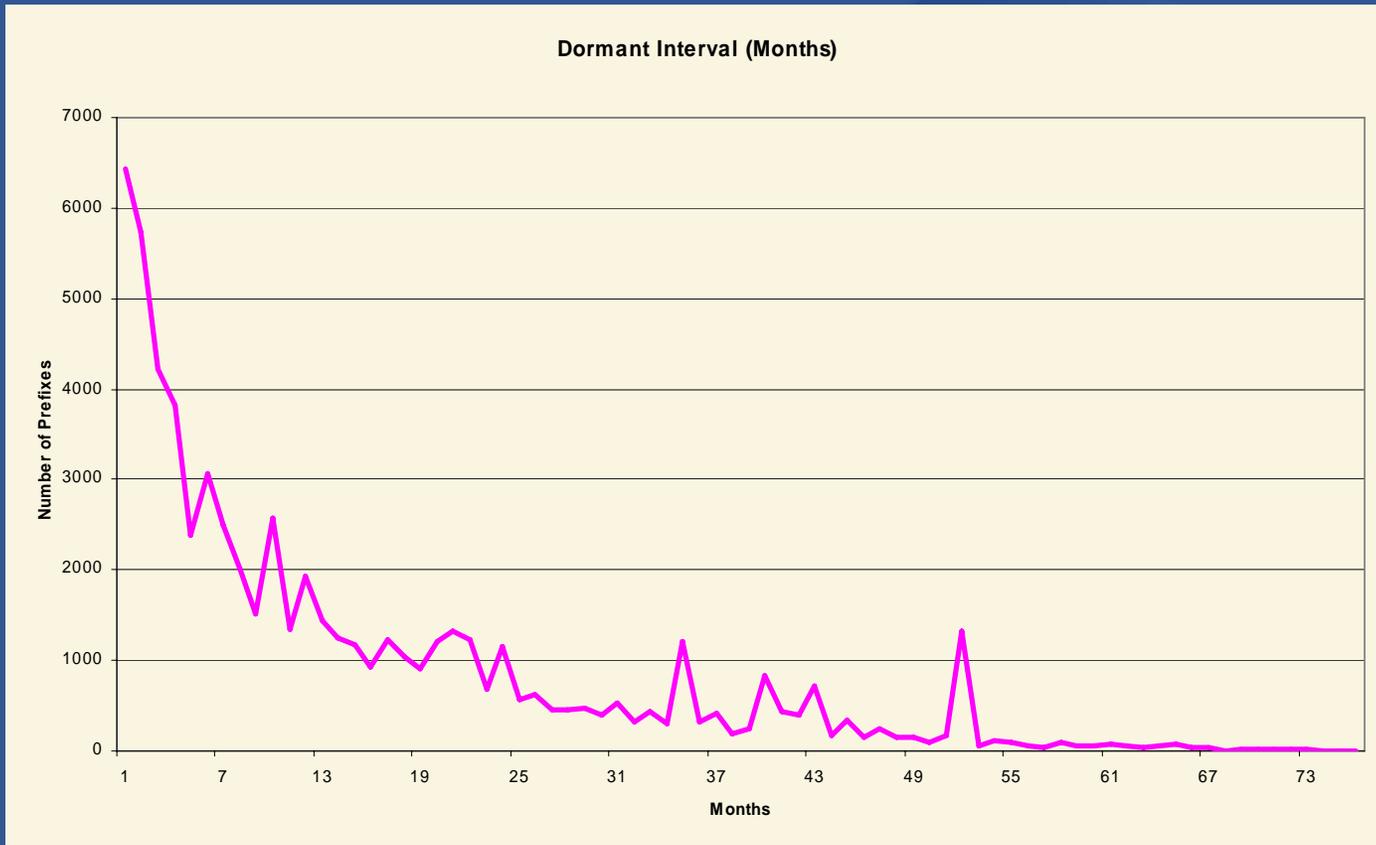
Noise reduction in BGP data

- BGP update logs are possibly unhelpful here
 - High frequency noise of BGP convergence is different from the longer frequency signal of prefix use through network connectivity and prefix advertisement
- Use successive static BGP snapshots
 - Highest frequency component of 2 hours reduces protocol-induced noise levels in the data



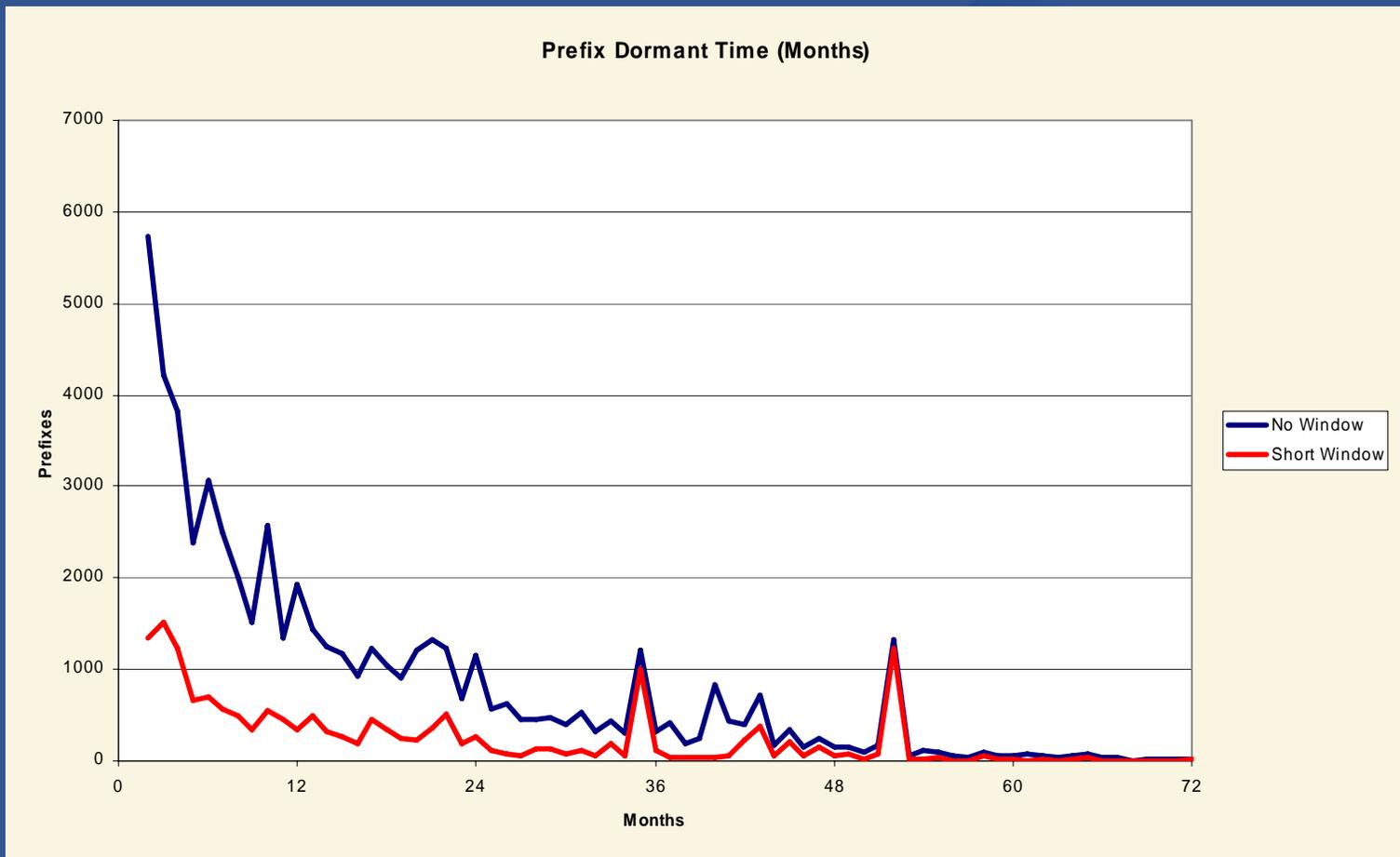
Initial results

- Readvertisement of prefixes with different Origin AS and First Hop AS



2nd Pass

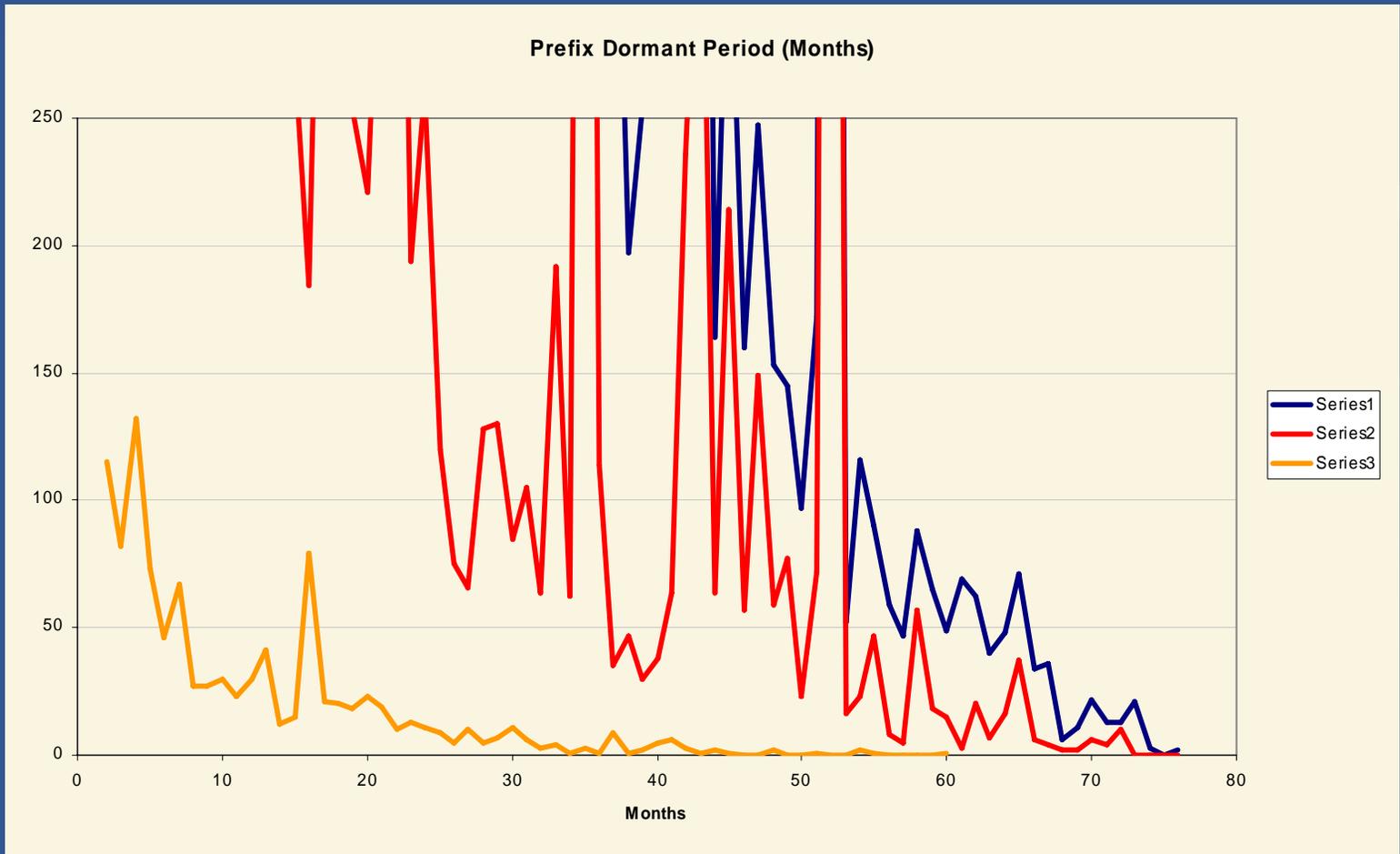
- Very short window announce
 > 2 months down, < 3 days up, > 1 month down



3rd Pass

- Short window

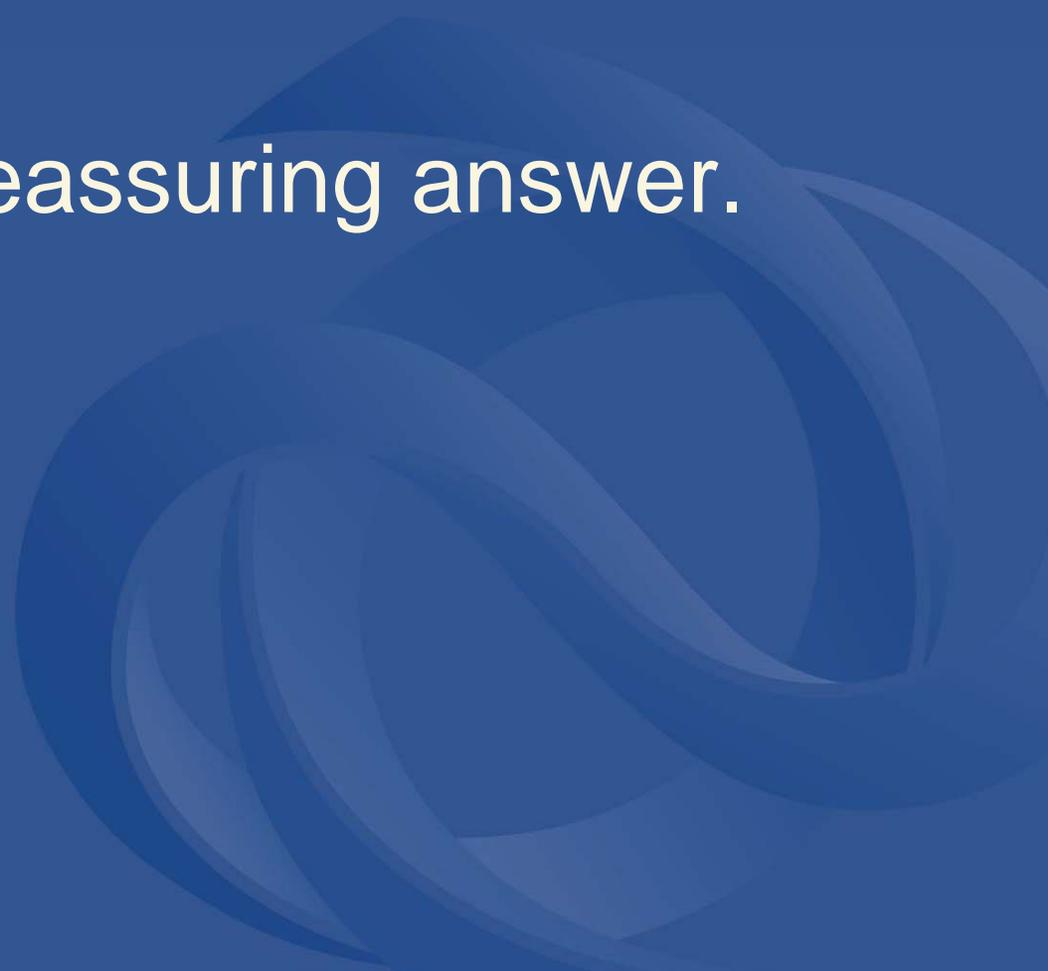
> 2 months down, 5 - 14 days up, > 1 month down



Some comments

- Address announcement patterns do not appear to be a reliable hijack indicator in isolation.
 - There is no clear signature in the patterns of prefix appearance that forms a reliable indicator of misuse.
- Address use profiles can assist in the process of identifying address hijacking for suspect prefixes.
 - Additional information is necessary to reliably identify candidate hijack prefixes.
- Careful checking of the provenance of an address before accepting it into the routing system make good sense
 - But thorough checks of a prefix's history of use as a precondition to accepting it into the local routing session as a valid advertisement consume time and increase an ISPs' operating overhead costs

It's not a very reassuring answer.



Address and Routing Security

The basic routing payload security questions that need to be answered are:

- Is this a valid address prefix?
- Who injected this address prefix into the network?
- Did they have the necessary credentials to inject this address prefix?
- Is the forwarding path to reach this address prefix an acceptable representation of the network's forwarding state?

Address and Routing Security

What we have today is a relatively insecure system that is vulnerable to various forms of deliberate disruption and subversion

Address hijacking is just one aspect of the insecurity of the Internet's routing system

What I really would like to see...

The use of a public key infrastructure to support attestations that allow automated validation of:

- the authenticity of the address object being advertised
- authenticity of the origin AS
- the explicit authority given from the address to AS that permits a routing announcement

What would also be good...

- If the attestation referred to the address allocation path
 - use of an RIR issued certificate to validate the attestation signature chain
- If the attestation was associated with the route advertisement
 - Such attestations to be carried in BGP as an Update attribute
- If validation these attestations was treated as a route object preference indicator
 - Attestation validation to be a part of the BGP route acceptance process

But...

We are nowhere near where we need to be:

- We need more than “good router housekeeping” – it’s trusting the protocol payload as well as trusting the protocol’s operation and the routing engines
- We need so much more than piecemeal distributed 2nd hand bogon and martian lists, filters and heuristics about use patterns for guessing at ‘bad’ addresses and ‘bad’ routes

What I'd like to see...

We adopt some basic security functions into the Internet's routing domain:

- **Injection of reliable trustable data**
 - Address and AS certificate PKI as the base of validation of network data
- **Explicit verifiable mechanisms for integrity of data distribution**
 - Adoption of some form of certification mechanism to support validation of distributed address and routing information

Oh yes, and about address hijacking...

- This type of resource security framework would make address hijacking much harder to perform!

Thank You