BGP-Origins: A Public Space System

Eric Osterweil: eoster@cs.ucla.edu
Dan Massey: massey@cs.colostate.edu
Beichuan Zhang: bzhang@cs.arizona.edu
Lixia Zhang: lixia@cs.ucla.edu
Problem

• Automatically mapping BGP prefixes to the AS that are authorized to announce them is challenging
• Allowing operational autonomy and freedom complicates structured approaches
• Can we let real-world trust shed light on ambiguity?
Existing Approaches

- **MyASN**: Based on registered mapping information
  - Information can become stale
- **PHAS**: Based on observed data
  - Easy to operate
  - Low certainty in answers, but useful for prefix owners
- 3rd parties should have the ability to “verify” information about routing announcements
- **SIDR**: Good and needed. However
  - Will take time to roll out
  - Still need to see if needed granularity will be offered
BGP-Origins’ Approach

• Built upon the concept of the *public space*
  – Anyone claiming that an origin is valid for a prefix is simply making their [informed] opinions public

• BGP-Origins avoids the difficulty of verifying authorized origins
BGP-Origins Project

• **Main goal:** providing a complementary origin lookup service
  – Design is geared towards automated clients
  – Strengthened by crypto, see later…

• **Data sources for prefix-AS binding**
  – Observations from announced prefix origins, together with historical statistics
  – From users who publish what *they* think
What BGP-Origins Offers

• Offers a rigorous framework for this lookup system
• Input: cryptographically signed data
  – Observation data: signed by PHAS site
  – User attestations: signed by PGP key (so we can know if you are a dog:-P)
• Output: Quick but not dirty
  – DNS interface for look up: quick, universally usable
  – Signs data so clients can verify that it has come from BGP-Origins
What BGP-Origins Does Not Do

- Does not guarantee data correctness
- Does not guarantee conflict-free data
- BGP-Origins only provides source authenticity
Example

$t_1$: Announce 192.168.0.0/24

$t_2$: 192.168.0.0/24 → \{m,n\}

Which is it: $m$ or $n$?

$t_0$: Announce 192.168.0.0/24

Bob

Alice
Example (2)

$t_1$: Announce 192.168.0.0/24

$t_0$: Announce 192.168.0.0/24

$t_2$: 192.168.0.0/24 → \{m,n,Alice:n\}

Alice says 192.168.0.0/24 Should be $n$

Bob

BGP-Origins
Example (3)

• Which origin is the right one?
• Opinions about valid origins may vary, and trust is subjective
• When querying, BGP-Origins users may ask for:
  – Observations
  – Attestations (trust anchors, such as Alice)
Operational Use

• Operators (or automated policies) can make informed decisions
• Everyone makes her/his own decisions
• BGP-Origins is designed to be a look-aside validation system
  – Rather than in-line validation
Observed Data

• Viewing updates from multiple peers (ala PHAS) provides a comprehensive view
  – PHAS currently uses RouteViews and is working towards integration with RIS (RIPE NCC) data

• BGP-Origins aims to provide a meaningful subset of all available prefix/origin data…
Observed Data (2)

- BGP-Origins will act as a low-pass filter and try to filter out erratic data
  
  Formula = \((T_{\text{announced}} \times \alpha) + (Past \times (1 - \alpha))\)

- Timeline will use a moving average:
  - Will squelch origins based on patterns of transient announce/withdraws
  - Reward consistency announced origins
  - Accept newcomers
What to Squelch?

• Spammers originate /8s for ~10 minutes at a time [Feamster et al]
  – We aim to squelch these

• But, large outages may cause new origins to appear too
  – We aim to present these
Spamming Prefixes
[Feamster - NANOG 37]
User Feedback

• Operational trust can be gained externally to BGP-Origins (i.e. people trust real-life friends)
• The opinions of a trusted associate can be used to make decisions
• Anyone can query with DNS
  – dig works great, and writing tools is easy too
dig 16/0.0.179.131.actions.bgp-origin.org.txt

-bash-3.00$ dig 16/0.0.179.131.actions.bgp-origin.org.txt

; <<>> DiG 9.2.4 <<>> 16/0.0.179.131.actions.bgp-origin.org.txt
; global options:  printcmd
; Got answer:
; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 271
; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDITIONAL: 2

; QUESTION SECTION:
;16/0.0.179.131.actions.bgp-origin.org. IN TXT

; ANSWER SECTION:
16/0.0.179.131.actions.bgp-origin.org. 51 IN TXT "16/0.0.179.131:52:2BFB6AE822636502:Eric Osterweil:1"
16/0.0.179.131.actions.bgp-origin.org. 51 IN TXT "16/0.0.179.131:52::1"

; AUTHORITY SECTION:
bgp-origin.org. 515869 IN NS celtics.cs.ucla.edu.
bgp-origin.org. 515869 IN NS phasmain.netsec.colostate.edu.

; ADDITIONAL SECTION:
celtics.cs.ucla.edu. 14400 IN A 131.179.96.121
phasmain.netsec.colostate.edu. 53368 IN A 129.82.138.5

; Query time: 13 msec
; SERVER: 131.179.128.16#53(131.179.128.16)
; WHEN: Mon Jun  4 16:59:15 2007
; MSG SIZE rcvd: 258
Submitting

• User feedback must be signed by PGP/GPG keys that exist in existing online key-servers
  – PGP is ubiquitous, keys tie signatures to specific users/entities
• Easily done / readily deployable through the use of DNS dynamic updates
bgpo-client.pl -a <prefix>

-bash-3.00$ ./bgpo-client.pl -a 131.179.0.0/16
Origin: 52
How many days until expiration (0 == no expiration):
Are you specifying:
1 - trust
2 - distrust
3 - revocation of former trust
Please enter the number: 1

You need a passphrase to unlock the secret key for user: "Eric Osterweil <eoster@iwon.com>"
1024-bit DSA key, ID 22636502, created 2006-10-09
How BGP-Origins Gets Work Done

• Uses GPG/PGP keys to verify signatures
• Pulls PGP keys from key-servers
• DNS queries lower the bar to access
• DNS updates are used to upload cryptographically signed mappings
• Simple reference scripts offer an interactive command-line interface for this
Conclusion

• BGP-Origins does not determine if data is “valid”
• Users can submit any prefix/origin binding
• The onus is placed on clients to determine whose attestations to trust
• BGP-Origins is a non-repudiation framework
• BGP-origins is readily usable today
  – Utilizes DNS for input/output
Check Us Out

• Further information available at:
  
  http://www.bgp-origin.org/

BGP-Origins

Automatically mapping BGP prefixes to the AS that are authorized to announce them is challenging. It is not always straightforward to know who is authorized to announce a prefix. Allowing operational autonomy and freedom complicates structured approaches.

BGP-Origins fuses global prefix monitoring data from PHAS and user attestations in a rigorous framework to enable operational entities to view current BGP prefix mappings and to use their own policies/decision making to determine the validity of origin mappings.

For additional information about the motivation and scope of BGP-Origins, please see our NANOG 40 presentation.

BGP-Origins uses the DNS protocol as both a lookup and update mechanism. Users can easily query for the mappings of a prefix by issuing a familiar DNS query such as:

```
dig 16/0.0.179.131.actions.bgp-origin.org txt
```

This command returns records in the DNS answer section that are parsable as follows:

```
16/0.0.179.131:52:<Key ID>:<Key Owner Name>:<Trust Code>
```
Thank You

Questions?