Inter-domain routing security and the role of Internet Routing Registries

IEPG meeting, IETF 60
August 1, 2004

Larry Blunk, ljb@merit.edu, Merit Network, Inc.

Overview

- State of IDR security
- State of the Internet Routing Registry
- Historical security use of IRR's - filtering
  - Issues with filtering
  - IPv6 opportunities
- Alternate use of IRR's – anomalous route notification
- Improving IRR security and coordination
- Review

State of IDR Security

- Current efforts have largely focused on link-level security
  - TCP-MD5, IP-SEC, BGP TTL security hack (BTSH)
  - Some progress has been made (recent Cisco TCP reset scare)
- Efforts at securing data validity have seen less progress
  - Secure BGP (S-BGP) – BBN Technologies
  - Secure Origin BGP (soBGP) – Cisco
  - Inter-domain Routing Validation (IRV) – AT&T Research
  - Secure Path Vector (SPV) – Berkeley and CMU
- ISP's have not shown significant enthusiasm
- RPSEC Working Group still working on requirements
- Deployment will likely require some time
- Are there interim measures that can deployed?

State of the IRR

- The IRR is currently somewhat loosely defined
  - Merit hosts www.irr.net and mirrors 41 other registries
  - No formal requirements or authority for presence in IRR
- Currently hold about 304,400 routes, 203,200 unique
  - ~116,000 route objects are actually being routed
- Registries consist largely of smaller ISP's and networks
  - Some large ISP's present - Verio, Level3, and Savvis
  - Two open independent registries - RADB and ALTDB
- 3 RIR's run routing registries – APNIC, RIPE, and ARIN
  - ARIN's is open and not yet integrated with address registry
  - LACNIC has limited “RR-like” functionality (non-RPSL)
- Currently v4-only - RPSLng adds IPv6 and Multicast support

Historical security use of IRR's - filtering

- Filter BGP announcements based on origin AS
- Several public and custom tools for filter generation
  - IRRToolset considered defacto standard
  - IRR.pm perl module
  - Savvis, Verio, Level3 use internally developed tools
- Filtering has been limited to customer peers
- Many ISP's use other non-IRR mechanisms
  - Statically configured prefix lists
  - Coarse-grained security – max prefix limits

Issues with filtering

- Data incompleteness has limited it's use to customer peers
- Size of filter lists is an issue with wider deployment on peers
- Lack of dynamism can be a concern
- Tool issues
  - IRRToolSet is somewhat complex
    - Does not compile with recent versions of C++
  - IRR.pm not widely known and does not support RIPE syntax
  - Better documentation, examples, and best practice guides could be useful

IPv6 Opportunities

- RPSLng Internet Draft adds IPv6 and multicast support
  - Has gone through IESG Last Call review
  - Final draft should be out after IETF meeting
- IPv6 Internet is currently fairly small (about 500 prefixes)
  - A global filter list is more practical than with ~135,000 IPv4 prefixes
- Does not have issues with legacy allocations
  - All allocations have been made by RIR's
  - RIR data should have strong validity due to newness
- Could be a driver for IPv6 deployment
  - Validate claims of improved security with IPv6

IRR's and anomylous route notification

- Use data from IRR as input for notification system
  - Monitor data from BGP collection services
    - e.g. Routeviews, RIPE RIS, etc.
  - Alert via Email, SNMP Trap, SMS, etc.
- Some similar services implemented, not integrated with IRR's
  - RIPE's MyASN service
  - Renesys GRADUS product (commercial)
- Other systems examine IRR data, but are not real-time
  - e.g. RIPE RRCC, Nemecis, radb-reports
- Operators may prefer locally run tools to a service
- Would be useful to aggregate BGP collection data
  - summarize specific events, e.g. Origin AS or AS path change

Improving IRR security and coordination

- Security of the registry repositories
  - Important if greater reliance is placed upon them
  - May want to include signature within objects
- Security of queries and mirror operations
  - RFC 2769 defines a “repository-cert” for securing mirroring
- Better coordination and authority model would be useful
  - RFC 2725 and 2769 define a heirarchical model
  - Need to review and decide how to proceed
- irrc@merit.edu email list has been setup for coordination

Review

- IDR security with to data validity is currently weak
- While work is ongoing, progress has been slow
- IRR's present an opportunity to improve security on an interim basis
- Current filtering tools and documentation could be improved
- Data consistency and accuracy is also a concern
- IPv6 presents an opportunity due to current limited-scale deployment
- IRR utility could be improved with integrated anomalous route detection and notification tools and services
- IRR security and coordination need to be improved to create more confidence in the data

References

- RFC 2622 - http://www.ietf.org/rfc/rfc2622.txt
- RFC 2725 - http://www.ietf.org/rfc/rfc2725.txt
- RFC 2769 - http://www.ietf.org/rfc/rfc2769.txt
- RPSLng - http://www.radb.net/rpslng.html
- RRCC - http://www.ripe.net/rrcc/
- Nemecis - http://www.cs.ucr.edu/~siganos/papers/Nemecis.pdf
- Renesys - http://www.renesys.com
- S-BGP – draft-clynn-s-bgp-protocol-01 (expired)
- SoBGP – draft-ng-sobgp-extensions-02
- SPV - www.acm.org/sigs/sigcomm/sigcomm2004/papers/p352-hu.pdf