Towards a Cohesive Internet Routing Registry System

Inter-domain Routing Workshop - Amsterdam
May 1, 2004

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

Overview

- State of the Internet Routing Registry System
- Review of existing standards work
- Authority issues
- Authentication issues
- Other security concerns
- Replication and availibility
- Data correctness
- Extensibility
- Review
- Future of the IRR System
- References

State of the IRR System

- The IRR System is currently a very loosely defined concept
  - Based upon the RPSL (RFC 2622) standard
  - Merit hosts www.irr.net and mirrors ~50 other registries
    - No formal requirements or authority for mirrors
    - Confusion between RADB and IRR System
  - RIPE NCC also mirrors a number of registries
- 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 integrated with address registry
  - LACNIC has limited “RR-like” functionality (non-RPSL)

Review of standards work

- RPSL (RFC 2622) was published in 1999
  - Follow-on documents
    - RFC 2650 Using RPSL in Practice
    - RFC 2725 Routing Policy System Security
    - RFC 2769 Routing Policy System Replication
  - RPSLng – IPv6 and Multicast extensions – currently I-D
- CRISP Working Group concerns cross registry protocol issues
  - RFC 3707 defines a set of requirements for CRISP
  - Current focus is on domain and address registries
  - Specifications based around IRIS XML schema framework
  - What are the CRISP considerations for routing registries?

Authority issues

- RFC 2725 provides the current framework for RPSL authority
  - Authorization based on AS and IP prefix allocations
  - Currently supported by RIPE and APNIC registries
- Issues when going outside the integrated RIR/RR registries
  - An ISP wants to use their own registry
  - Third-party registries (RADB and ALTDB)
  - Cross registry issues (i.e., Prefix allocation by one RIR, and AS by another)

Authority issues (cont'd)

- Some pieces are puzzle may be already addressed
  - "::" for external references in RFC 2725
  - "delegated:" attr. and "repository:" object in RFC 2769
  - Should these be pulled together in a new document?
- Are there incremental approaches to improving authority?
  - Use of "integrity:" attribute from RFC 2769

Authentication issues

- Initial RPSL spec included poor authentication mechanisms
  - NONE and MAIL-FROM clearly bad choices
  - CRYPT-PW hashes subject to dictionary attacks
  - PGP is strong, but can be difficult for new users
- Several attempts to address deficiencies
  - Dropping NONE and MAIL-FROM support
  - Stronger password hashes (RIPE supports MD5 hashes)
    - Note: stronger hashes still subject to cracking
  - RADB no longer reveals pw hashes on queries/mirroring
  - RIPE deploying X.509 certificate based authentication
- Should authentication requirements be more formalized?
  - Should they be enforced (for participation in IRR system)?

Other security issues

- Security of the registry repositories
  - Is this a concern or can we assume they are safe?
  - Could archive PGP and X.509 signatures w/updates
    - Would allow remote verification of adds/removals
  - Should there be a “signature” attribute within objects
- Security of queries and mirror operations
  - Should registries sign replies to queries?
  - RFC 2769 defines a “repository-cert” for securing mirroring transactions
- What should be the considerations for future Inter-domain routing security enhancements (i.e. S-BGP and soBGP)?
  - Are there issues here routing registries could address?

Replication and availibility

- Currently, replication is handled by a simple near realtime mirroring protocol
  - Protocol is not particularly robust and poorly documented
  - RFC 2769 defines a more robust and secure protocol
    - Fairly complex and has yet to be implemented
    - Could other general replication schemes suffice?
- What availibility requirements should be considered?
  - Multiple mirrors?
  - Anycasting?
- Registries not currently documented in easily machine queried format
  - Could use “repository:” object to list mirrored registries

Data correctness

- Data correctness has long been an issue of concern with IRR's
  - Stale data that is not updated or removed from registries
  - Registration of “route:” objects merely to record allocated prefixes rather than actual announced routes
  - Registering more specific components of a prefix in case they “might” be announced at a future time.
- Some efforts have been made to analyze consistency
  - RIPE NCC RR Consistency Check project (RRCC)
  - Merit RADB “radb-reports”
  - Nemecis project
- Can the tools be better coordinated and easier to use?
- Are more active measures needed (flagging stale data)?

Extensibility

- RPSL recently updated with IPv6 and Multicast support
- Introduced further complexity into an already complex specification
- Has RPSL had its day?
- CRISP Working Group could provide opportunity to start fresh and support better extensibility.
- Should there be a transition or hybrid (XML+RPSL) model?

Review

- The current IRR System lacks a coherent model
- How should the authority model work?
  - Review models presented in RFC 2725 and RFC 2769
  - Where do local ISP and third party RR's fit in?
  - Should the RIR's delegate to external registries?
- Where can security be improved?
- How do we maintain data consistency?
- Is there sufficient reliability and redundancy?
- Where does the CRISP work fit in?
- What are the considerations for future inter-domain routing protocol security enhancements?

Future of the IRR System

- Propose creating IRR System requirements document
  - Could possibly work within IETF GROW working group
  - Should address requirements without necessarily getting into data representation (RPSL or IRIS) issues
  - Need to involve stakeholders (ISP's, end-user's, RIR's)
- Look at CRISP work as requirements are defined
- Consider an IRR Consortium or Association
  - Would set policies and formal requirements
  - Address security and accessibility

References

- RFC 2622 - http://www.ietf.org/rfc/rfc2622.txt
- RFC 2650 - http://www.ietf.org/rfc/rfc2650.txt
- RFC 2725 - http://www.ietf.org/rfc/rfc2725.txt
- RFC 2769 - http://www.ietf.org/rfc/rfc2769.txt
- RPSLng - http://www.ietf.org/internet-drafts/draft-blunk-rpslng-04.txt
- CRISP WG - http://www.ietf.org/html.charters/crisp-charter.html
- RFC 3707 - http://www.ietf.org/rfc/rfc3707.txt
- RRCC - http://www.ripe.net/rrcc/
- Nemecis - http://www.cs.ucr.edu/~siganos/papers/Nemecis.pdf