Practically Improving Security of Routing Information

Rüdiger Volk
Deutsche Telekom

RIPE59 Routing WG
October 2009, Lisboa

about: a recent workshop

- 2 day roundtable invited by ISoc
- experts for routing provisioning and policy
- very large network providers from 3 continents
  + few large content providers
- identify requirements and options rather than building action plan
- publication of report intended/expected

this presentation...

- ***personal*** view and conclusions from workshop
  - report ./. opinion ./. personal conclusions not so clearly distinguished
- work on official report needed for a more balanced presentation
- workshop proves helpful for directing work
- though unspectacular and without huge surprises

road? map

- short term ./. longer term
- *serious* security requires security elements in the routing protocol – agreement/developement/ deployment will take time… :-(
- short term = practical:
  - without change/addition to BGP or
  - minimum development of router SW

high priority items

- pursue RPKI (for both IPv6 and IPv4)
- RPKI system needs to provide uniqueness of resources

- cleanup data for IPv6 while small (even IRR as far as RPKI is not available)
- authentication of resource holders (local)
- need certificate distribution and validation widget

more high priority

- reduce cost of safe business
- what can be done about path validation?
- invalidation of authority to route

  also short term worthwhile:
- origin validation
- more use of route anomaly monitoring...

currently used information...

- (in the RIPE region somewhat nicer than elsewhere)
- lots of bad information around
- ... can get confusing
- mostly trying to track address to organization
  - organizations change etc...
  - no real links to routing system (AS)

RPKI topics

- development dominated NOT by operators
- figure out operators' needs
- what concerns/threats are there for actual routing use?
- no clear picture of RIRs RPKI plans and policies

RPKI ...

- operators need to care about RIRs' CPS
- uniqueness is responsibility of "system" don't bother users
- known threat: surprising transition to invalid
  - minimize by policy
  - document/support workarounds for remaining cases (e.g. Steve Kent yesterday)

origin validation

- server manages/validates cache of RPKI data pairing prefixes with authorized origin AS (also can be used for RPSL originated data)
- simple protocol to serve this data to router see draft-ymbk-rpki-rtr-protocol
- add verification of authorized origin AS as policy element to BGP (very efficient)
- lab implementations by Cisco and Juniper

software tools

- RPKI based widget as drop in replacement for currently used RPSL/IRR tool?
  - ROA2RPSL is solution for some of this
- request for open software for commonly needed functionality – have it available for whole community
  - are existing tools/activities known/
  - how to identify needs?

open questions: business side

- is there a clear business case for routing security?
- how to deal with unclear requirements on router(?) hardware for long term solution
  - investment planning
  - discussing next generation systems with vendors (approx. 5 years cycle/horizon)

- thanks for your attention

- questions?