Dealing with Threats in RPKI for RIPE

Rüdiger Volk, Deutsche Telekom

impromptu @RIPE 62 APWG

discussion and process in RIPE and RIPE NCC activities

- IMHO there are important issues
- but today I focus on the technical and operational system!

threat of unsecured routing information?

- technical detail discussion...
- do operators perceive real threat and need for solution?
  - most relevant point of view because:
    - operators are responsible for reliable network service

solutions?

- current situation & traditionally available tools
  - not sufficient / broken in many ways...
- what solutions have been worked on?
  - in sufficient detail to offer a reasonable deployment road map?

solutions

- RPKI looks like only available horse in town
  - e.g. ISoc round table 9/2009, report RIPE 59

    http://www.isoc.org/educpillar/resources/docs/routingroundtable_200909.pdf
    my slides (routing WG Friday) disappeared from RIPE archive
    but nice summary of my report in

    http://www.potaroo.net/ispcol/2009-10/ripe59.pdf

- utopian proposals always can promise everything...

vulnerabilities of RPKI

- what to do:
  - analyze and identify threats and vulnerabilities
  - what can be done to deal with them?
- "unexpected" revocation / abuse of power of higher hierarchy
  - discussion @RIPE 59 (Lisbon) ...

scope of threats

- make sure that rules and processes of RIPE NCC (+root) provide maximum protection
- reduce threat to rare exceptions! (irregular action by staff, external interference such as court order, ...)
- ultimate authority for use is with the relying party deciding which trust anchors to use
  - this implies that relying party can override parts of the PKI system with information of it's choice
  - some details presented by Steve Kent RIPE 59

empowering relying parties

- specific support for helping with this can be introduced into the RPKI relying party software (the validator)
  - needs work for specifying and implementation of software extensions
- also need to have “exception” information that relying party can decide to use for override – call it “independent RPKI backup”
  - also needs work and infrastructure

independent RPKI backup information

- organize tracking of RPKI information outside of the control of the hierarchy chain
- keep old information of status before potential "unexpected revocation" (short "exception") available
- establish exchange forum and protocol to distribute hints about "exceptions" to/amongst relying parties

expected consequences

- “exceptions” to be dealt with expected to be few and infrequent anyway
- with backup infrastructure and tools for easy use in place the attack vector becomes fairly unattractive for any reasonable parties such as law enforcement
- will exceptions be so rare that no one will pay for this “safety belt” or even to participate in fire drills?

it can be done!

- but resources needed

will it be done?

- who is concerned about the risk?
- where/how work on relying party software?
- how do the backup infrastructure?
- RPKI exceptions exchange forum?

how to proceed?

- refocussed/rechartered/reborn CA-TF?
- substantial contributions and community feedback needed
- careful decision about need/capability/capacity of engagement of RIPE NCC development resources

backup 1

... for any alternate proposed routing security proposal

- at least as severe “will it be done?” questions!
- ✦ how much delay for deployment?
- ✦ how certain is a sufficiently solid result?
- ✦ is separatist/competing standard to IETF feasible/ reasonable?
  - includes: global Internet ./. regional standards