Inter-domain routing security

Stocktaking, state-of-the art, and future perspectives
Some context

• Routing security stocktaking was part of project commissioned by ENISA

• Caveat: Results presented are our own observations, interpretations, and conclusions
Goals of Routing Security Survey

• We were interested in:
  – awareness
  – current deployment and experience
  – expectations of (near) future developments
  – policy and governance issues
Approach

• Online survey
  – quantitative data from survey can substantiate interviews with routing security experts

• Interviews
  – insights of network operators, engineers, architects,... from ISPs, vendors, and research labs (profit and non-profit)
Online Survey

• About 130 respondents
  – send out CFPs to RIPE, AMSIX, DE-CIX, LIXN, and Netnod community

• Session security
  – MD5, TCP hack, ...
  – most generally applied, but 45%/45% in observed improvement, even 10% counter productive

• Filtering (and monitoring)
  – deployment base just after session security
  – 80%/17% in observed improvement, 3% counter productive.

• Level of awareness of RPKI is relatively low

• Government involvement: stimulation, not regulation
Interviews

• 20+ interviews with network engineers
  – from tier 1 to small networks
  – vendors
  – researchers from labs (profit & non-profit)
  – typically respected and honorable persons attending IETF/RIPE meetings :-)
  – and... of course this sample is biased
Some general observations

• First concern is network stability
  – people do not care about security as long as they have no problems with it

• Level of routing security awareness relates to the size of the network
  – large networks -> larger NOC staff with security expertise

• Most incidents seen in inter-domain routing are mistakes “fat fingering”
  – no surprise here
Some general observations (2)

• But... large attacks are not spoken about in public
  – just like banks don’t like to talk about large frauds
  – difficult to distinguish intentional attacks from incidents with non-malicious intent
  – smart and sophisticated attacks are difficult to notice
Some general observations (3)

• Security/strict filtering is not a selling point, but reachability and flexibility (in accepting prefixes) is
  – complex and prone to mistakes
  – filtering catches the most obvious errors and incidents, not the smart and sophisticated
RPKI concerns

• Some critical comments on RPKI and its intended usage
  – PKI hierarchy and single authoritative trust anchor
  – costs of certificates and period of validity
  – instability and vulnerability of the RPKI infrastructure
  – “a risk trade-off between the increased complexity and increased routing security is needed”
Weak signals

• Moving toward RPKI will be a major transition for tier 1 and large tier 2 networks
  – but these networks can leverage deployment

• The Internet works because of smart operators
  – need the knob and dials for configuring to make it work

• Shortage of skilled network staff can hinder deployment of routing security technology
Recommendations

• Develop initiatives to lower the economic hurdle of secure routing technologies

• Stimulate investments in development of routers and tools

• Stimulate self-regulation
  – compliance regulation can move players

• Improve awareness of RPKI
  – what it is and what is not

• Leverage by tier 1 and large tier 2 networks with the introduction of routing security technology
Question?

• report will be published by ENISA
  www.enisa.europe.eu/act/res