BGPSEC Threat Model Update

Steve Kent

BBN Technologies

Document Status

- Andrew Chi (BBN) has been added as a co-author. He is a co-author of RFC 6488 (RPKI signed object format) and a developer of RPKI RP code and RPKI tests.
- The -01 version was posted on 2/3, with a number of changes based on SIDR list comments
- The -02 version was posted on 2/22, with a few edits, mostly inserting SIDR RFC citations
- No comments have been received on the -01 or -02 versions, so far

What was Changed (-02 vs. -01)

- Replaced I-D cites with RFC cites for all RPKI documents that have been published
- Expanded discussion of residual vulnerabilities
  - Implications of router key compromise
  - Why route leaks are out of scope
  - Inability to ensure that withdrawals are generated when appropriate

What was Changed (-00 vs. -01)

- Added text to described the scope of the model, citing the SIDR WG charter
- Based on comments from the list we
  - Modified some definitions and changed use of some terms (e.g., switch to “network operator” from “ISP”)
  - Refined discussion of adversary capabilities and motivations
  - Refined discussion of some attacks (e.g., discussion of implications of using stale or expired data from a cache
  - Expanded residual vulnerabilities discussion to address issues re use of stale/expired objects from the RPKI repository

Questions