Update of the Adverse Actions document (draft-kent-sidr-adverse-actions-01)

Steve Kent
BBN Technologies

&

Declan Ma
ZDNS

Overview of Changes

- Two major changes
  - Most of the new text was added to describe the impact of actions, as requested by Andrei at IETF-93
  - Reorganized the document to discuss actions in the same order for each RPKI repository data type
- We also made some editorial changes to improve clarity

Order of Analysis

- For each type of RPKI repository object (ROA, Manifest, GB Record, CRL, CA certificate, router certificate) the action order is now consistent and complete
  - Deletion, Suppression, Corruption, Modification, Revocation, Injection
- In the previous version the order varied and 4 cases were missing

Adverse Actions (reminder)

- Actions not requiring the (right) private key
  - Deletion (removal from the repository)
  - Suppression (prevent publishing, removal, or update)
  - Corruption
- Actions requiring the (right) private key
  - Modification (need signature key)
  - Revocation (need signature key)
  - Injection (need signature key)

Detection & Remediation

- Detection
  - Each INR holder checks its published data and compares retrieved RPKI data against its expected values
- Remediation
  - An affected INR holder contacts the CA or repository manager that caused the problem and requests a fix (this should address errors and most attacks)

Minimizing Impact

- We believe a mitigation strategy should rely on
  - Hysteresis (bounded) - to avoid immediate propagation of errors or attacks, but bounded to preserve the legitimate authority of CAs (RIRs, ISPs, etc.)
  - Independent confirmation - an INR holder publishes an indication confirming adverse changes, using an authentication mechanism and data path independent of the RPKI repository system

Going Forward

- Still looking for feedback
  - Do we need to add any actions?
  - Technical verification of impact
  - Editorial improvements
  - Etc.
- We would like to have this document adopted by the WG
- We plan to revise the Suspenders design as a candidate for mitigation

Questions