Overview of the Adverse Actions document (draft-kent-sidr-adverse-actions-00)

Steve Kent
BBN Technologies

&

Declan Ma
ZDNS

Purpose

- The goal of this document is to
  - Establish a taxonomy of “adverse actions” that may result from errors by or attacks upon RPKI CAs and independent repository managers
  - Examine the impact of various classes of adverse actions in the context of several scenarios
  - Provide a basis for evaluating proposals that purport to address some or all of the types of adverse actions described in the document

Document Outline

- Analysis of Adverse Actions on RPKI Repository Objects
- Analysis of Adverse Actions Relative to Scenarios
- Recommendations for Detection and Remediation

Adverse Actions

- Deletion (removal from the repository)
- Suppression (prevent publishing, removal, or update)
- Corruption
- Modification (need signature key)
- Revocation (need signature key)
- Injection (need signature key)

RPKI Repository Objects

- ROA
- Manifest
- Ghostbusters Record
- CRL
- CA Certificates
- Router Certificates
- (add other EE certificate types?)

Analysis of Actions

- Four scenarios
  - INR holder operates CA and manages its publication point
  - INR holder operates CA but outsources repository management
  - INR holder outsources CA (to parent) but manages it own publication point
  - INR holder outsources CA & publication point (to parent)

Detection & Remediation

- Each INR holder checks its published data
  - Compares retrieved RPKI data against expected values during normal RPKI data fetch
- Remediation
  - assumed to be easy in the case of errors
  - maybe hard for some types of attacks

Going Forward

- So far only comments are from Andrei
  - We plan to make changes based on his comments, to improve exposition
- Feedback solicited
  - Technical verification
  - Wording improvements
  - Etc.
- We would like to have this document adopted by the WG

QUESTIONS ?