Keying and Authentication for Routing Protocols (KARP)

Automated Key Management Discussion

IETF 89

Joel Halpern

Brian Weis

KARP Charter

- Analyze a set of RP's, which are the domain of other RTG Area groups
- Work with the RP developers to address gaps found during analysis
- Define common operational and key management constructs
- Specify automated key management needs for routing protocols

KARP Progress

- Several Gap analysis documents have been published in progress, or just starting
  - BGP/LDP/PCEP/MSDP, OSPF, BFD, IS-IS, LMP, RSVP-TE, PIM
- Operations Model for Router Keying is in the RFC Editor Queue
  - Recommendations to operators and implementers regarding management and operation of router authentication
  - draft-ietf-karp-ops-model-10
- Database of Long-Lived Symmetric Cryptographic Keys is in the RFC Editor Queue
  - Specification of key chain objects
  - draft-ietf-karp-crypto-key-table-10

So what have we achieved?

- RP security and interoperability using manual configured integrity keys are both improved when
  - RP providers implement new protocol extensions resolving identified gaps
  - RP providers define key chains that conform to the karp-key-table draft
  - Operators following the best practices documented in the karp-ops-model draft

Manual Configured Integrity Keys vs. AKM

- We have understood that operators distribute integrity keys (manually or using provisioning tools), and this is not going to change in the short term
- Some people believe that this process
  - Can be considered an operational maintenance burden
  - Does not provide the same quality of integrity keys generated from AKM

Issue 1: Is there an operational maintenance burden?

- It is commonly claimed
  - The distribution of integrity keys is sufficient
  - Operators have management methods for distributing and replacing session keys that is good enough
  - Smooth session key rollover can be done today following the karp-key-tables draft

  See draft-rja-smooth-rollover-00.txt

Issue 1: Is there an operational maintenance burden?

- On the other hand
  - AKM authentication keying material does not need to be distributed as frequently as manual keys
    - Suitably protected asymmetric key pairs may not need to be updated due to staff changes, etc.
  - AKM authentication keying material is simpler to maintain than a key chain of session keys
  - BGP transport security is important for RPKI/ BGPSEC deployments, and it would be relatively simple to distribute router certificates using the same mechanisms.

Issue 2: Quality of integrity keys

- It is commonly claimed
  - Keys generated by humans do not usually have as good entropy as AKM
  - We're bad at picking passwords!
- On the other hand
  - Maybe the cost of an AKM doesn't warrant ensuring we have real high quality keys

Issue 3: AKM as attack vector

- Some people say
  - The complexity of AKM brings its reliability into question
  - An AKM itself is a DoS or other attack vector
- On the other hand
  - Newer AKM (e.g., IKEv2) have better DoS protections

AD Questions

- The chairs have not been able call consensus on whether KARP should continue with AKM work
  - A number of individual drafts have been extensively discussed, but there is not sufficient support to adopt them
- Should the work be abandoned?
- Should it be moved to the security area?