KARP KMP- Simplified Peer Authentication

draft-chunduri-karp-kmp-router-fingerprints-01

Uma Chunduri, Albert Tian,

Ari Keranen

Ericsson Inc.

IETF 85, Atlanta, GA

Nov 4 - Nov 9,2012

Motivation

- Minimize usage of Password based authentication in KARP deployments
  - operators don't often change the provisioned keys per Section 2.3 of I.D. **ietf-karp-threats-reqs**

    "…manually-distributed key throughout the entire network. These same operators report that the single key has not been changed since it was originally installed, sometimes five or more years ago. …."
  - Other reasons listed in Section 2.3 of I.D. **ietf-karp-threats-reqs**

- Move from Manual Keys to KMP – But:
  - Opens up lot of authentication possibilities
  - Peer authentication method selected may be password based
  - Should not cause Deployment overhead (Operational issues)

KMP possible AUTH methods (Recap)

Section 8.2 of *draft-chunduri-karp-using-ikev2-with-tcp-ao-00* lists the Possibilities

- Symmetric Shared key based
  - Pre-shared key only options worked out by ipsecme WG

Is any thing in between these two?

- Asymmetric (Using PKI, Trust Anchors)
  - RSA, DSS
  - ECDSA
- EAP Based (EAP Only - RFC5998)
  - Non Client/Server mode
    - PAX (RFC 4746)
    - EAP-pwd (RFC 5931)
    - EKE based (RFC 6124)

Simplified Peer Authentication using Router Finger prints (Recap)

- This draft just highlights the usage of an already specified not so popular KMP authentication method using “Raw RSA Keys”
  - **I-D.kivinen-ipsecme-oob-pubkey** for other types of public keys and also defines new encoding format to carry the public key fingerprint in the CERT payload.
- We tried to analyze this method for KARP to see
  - Benefits
  - Caveats
  - and see how this is aligned to KARP WG goals

How To Generate Finger Print

- Generate an asymmetric Private/Public key pair
- Encode with any additional data specific to the router (in the form of X.509 Certificate)
- Hash the result with a cryptographic hash function

How To Use Finger Print

- Initiator sends CERTREQ with x.509 encoding format to carry the public key fingerprint in the CERT payload and Certification Authority field is empty
- Responder uses X.509 encoding for the generated RSA Public Key
- Once this is received verification MUST be done with the already published/ stored fingerprints of the sender to validate the same
- **draft-farrell-decade-ni-10** defines one possible way to do this

Potential Beneficiaries of this AUTH method

- KARP Pair-wise KMPs
  - Potential RPs - BGP, LDP, PCEP, MSDP, BFD etc..
- KARP Group Key Management protocols
  - Potential RPs - OSPF, IS-IS, OSPFv3, LDP (Discovery Keys), PIM, RSVP-TE
- No Manual or symmetric shared keys any where

How to Publish Router Fingerprints

- Out of band sharing for Intra domain (both pair wise KMPs and Group KMPs) usage
  - Finger print is not secret unlike shared key
- Using SLAs (Inter domain outside of SIDR scope)
- need to resort to out-of-band public key validation procedure to verify authenticity of the keys
- The URI format defined in **draft-farrell-decade-ni-10** or PGP word lists can be used to represent the fingerprints

Fingerprint Revocation

- The idea of RFA in the context of KARP KMP is to deploy a better authentication mechanism than the mutually shared symmetric keys
- If a particular deployment (with large number of peers) where frequent key changes (private keys) are possible, operators SHOULD look to full PKI with trust anchor certificates and CRL profiles as specified in the [RFC5280]
- **RFA mechanism should be only seen as substantial improvement from mutually shared manual keying authentication methods**

Summary

	Symmetric Shared Keys	**✓Public Key Finger Prints**	TA Certificates
Out of band Shared Secret exchange - Privacy Req.	Yes	No	No
Operational Issues (Terminated Employees etc.)	Yes	No	No
Automatic Revocation with CRLs	No	No	Yes
Full Public Key Infrastructure for KMP Deployment	No	No	Yes

Questions & Comments?

Thank You!