KARP KMP- Simplified Peer Authentication

draft-chunduri-karp-kmp-router-fingerprints-00

Uma Chunduri, Albert Tian

Ericsson Inc.

IETF 84, Vancouver, Canada

July 29 - Aug 30,2012

Motivation

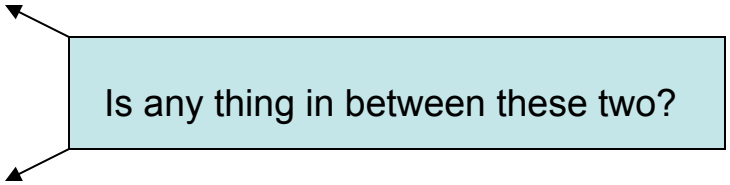
- Minimize usage of Password based authentication in KARP deployments
  - operators don't often change the provisioned keys
  - Reasons listed in Section 2.3 of I.D. **ietf-karp-threats-reqs**

- 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

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



- 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)

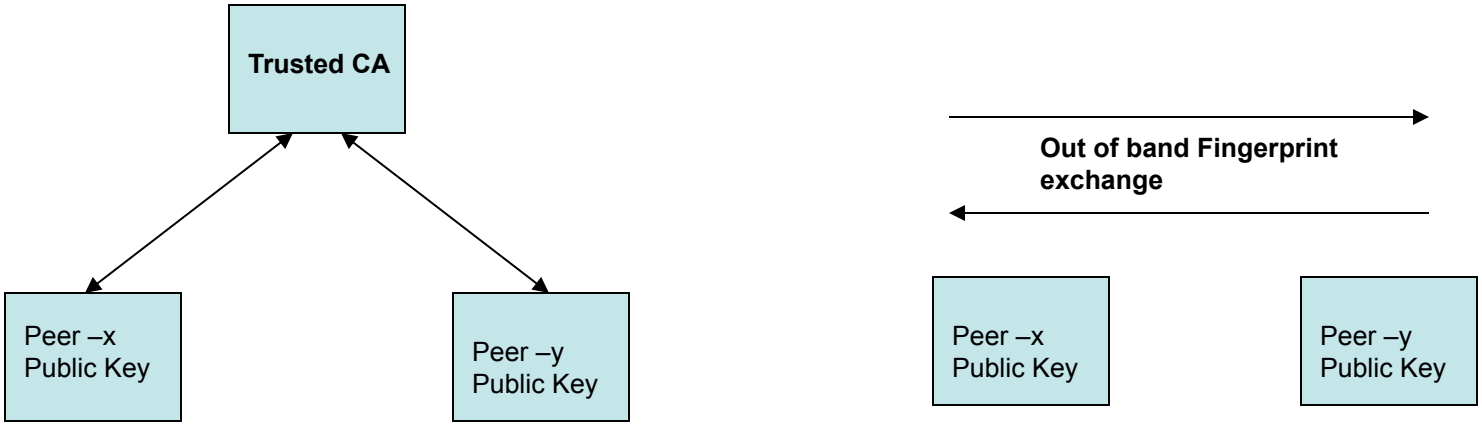
Simplified Peer Authentication using Router Finger prints

- This draft just highlights the usage of an already specified not so popular KMP authentication method
  - **Using “Raw RSA Keys”**

- We tried to analyze this method for KARP to see
  - Benefits
  - caveats
  - and see how this is aligned to KARP WG goals

What is Router Finger print

Router Fingerprint is a sequence of bytes used to authenticate the public key



How it is Router Finger print is generated

- 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

[I-D.kivinen-ipsecme-oob-pubkey] enhances support for other types of public keys (other than RSA) and also recommends x.509 encoding format to carry the public key fingerprint in the CERT payload.

How to Use it in KARP KMP

- Initiator sends CERTREQ with cert encoding set to "Raw RSA Key" and Certification Authority field is empty
- Responder uses PKCS #1 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

How to Publish Router Fingerprints

- Using SLAs
- Should be part of the PAD
- need to resort to out-of-band public key validation procedure to verify authenticity of the keys
- PGP word lists can be used to represent the fingerprints

Summary

- No need to store or change passwords/symmetric keys
- No need to deploy complete PKI for peer Authentication
- Router Fingerprints give a significant operational improvement from symmetric key based systems

Looking for feedback/co-authors to improve and include operational/Security aspects with this AUTH method for KARP KMP.

We thank:

Jari Arkko for initial discussion on this topic
Tero Kivinen for extended discussion in IETF-83

Questions & Comments?

Thank You!