KARP KMP-Using IKEv2 with TCP-AO

draft-chunduri-karp-using-ikev2-with-tcp-ao-02

Uma Chunduri, Albert Tian
Ericsson Inc.
Joe Touch
USC/ISI

IETF 84, Vancouver, Canada

July 29 - Aug 30,2012

Summary of changes in “02” version:

- Extended to capture Gatekeeper interaction with
  - PAD
  - Crypto Key Tables
- Other Security databases not relevant to KARP
- Few other Minor Modifications

Proposal:

```
                                       +-----------+
+-------------+ RP Session             |    PAD    |
| TCP Based   | Configuration     +--->|           |<--+
|    RPs      |------->--------+  |    +-----------+   |
|(BGP/LDP/PCEP|                |  |                   |
|    /MSDP)   |               _|__v_             +-----v----+
+-------------+              |      |  Trigger   |          |
                             |Gate- |----------->| IKEv2    |
                             |keeper| Negotiated |  KMP     |
+-------------+              |      | Parameters |          |
|             |              |      |<-----------|          |
|             |              |______|            +----------+
|  TCP-AO     |                |  |
|             |<---------------+  ^    +----------+
|             | MKT Provisioning  |    |Crypto Key|
+-------------+                   +--->|Tables    |
                                       +----------+
```

KARP KMP: Using IKEv2 with TCP-AO

draft-chunduri-karp-using-ikev2-with-tcp-ao-02 captures:

- TCP-based RP interface to GK
- KMP interface to GK
- TCP-AO interface to GK
- Interface to PAD and Crypto Key Tables
  (more details in the draft)

GK Interaction With PAD:

- PAD Contains all information related to Authenticate the Peer
- Used for creating CHILD_SAs at KMP
- Multiple GK Records can point to same PAD Entry (for the same DIP used by multiple RPs)
  - Multiple MKTs or CHILD_SAs corresponding to each RP
  - Provisioning change at RP SHOULD lead to re-negotiation of MKT
  - Provisioning change at PAD entry SHOULD re-authenticate the peer and all MKTs need to be re-negotiated

```
Gatekeeper Record                          PAD Entry

+------------+                       +------------+
| RP1(BGP)   |<--------------------->|  Peer X    |
|            |                       |            |
|            |      +--------------->|            |
+------------+     /                 +------------+
                  /
+------------+   /
|            |  /
| RP2(LDP)   |<--+
|            |
+------------+

+------------+                       +------------+
|            |                       |            |
| RP1(BGP)   |<--------------------->|   Peer Y   |
|            |                       |            |
+------------+                       +------------+
```

KARP KMP: Gatekeeper interface to the PAD

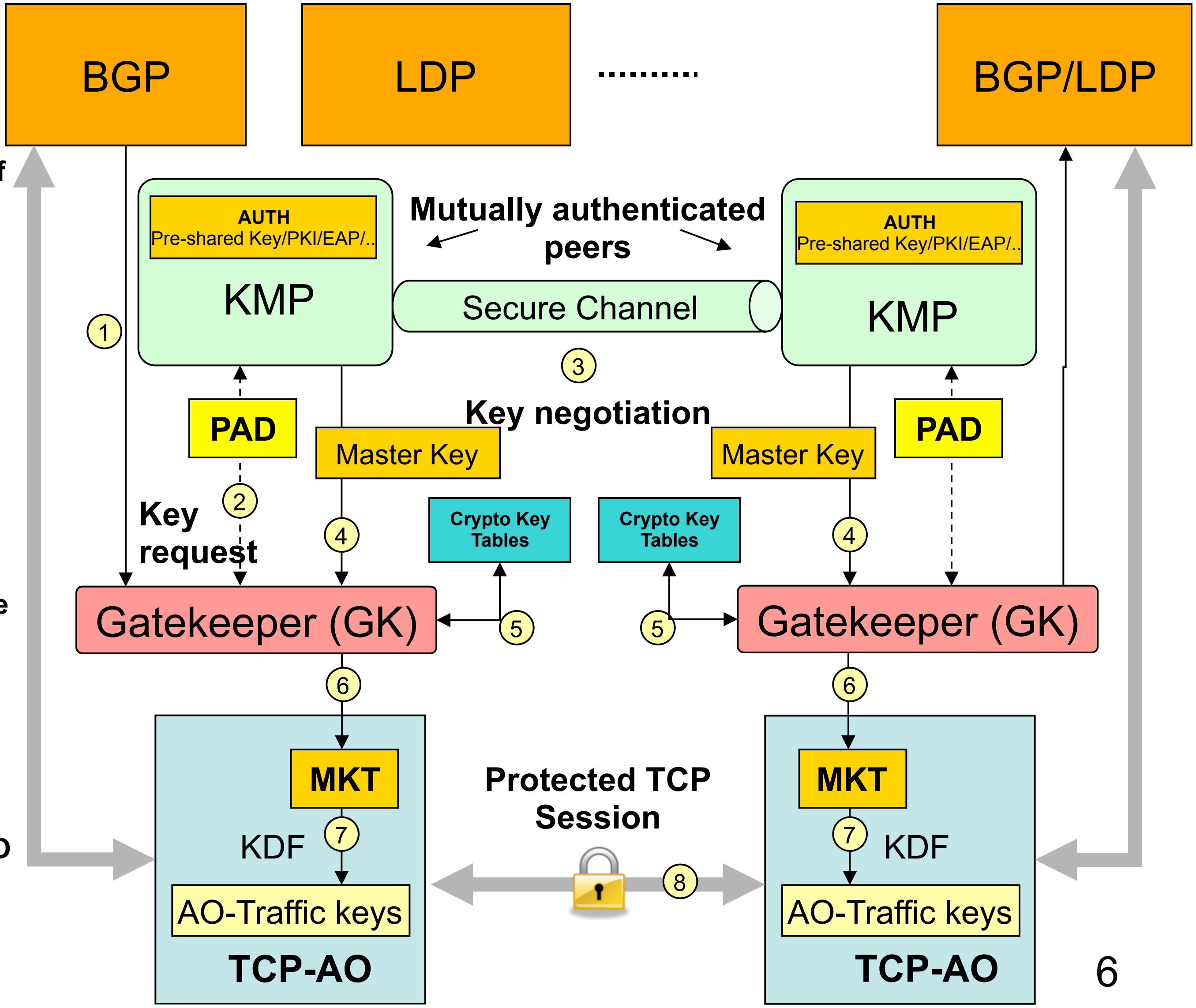
GK Interaction With Crypto Key Tables:

- KMP negotiated parameters are kept in the crypto key table database as specified in [ietf-karp-cryoto-key-table]
- The database is characterized as a table, where each row represents a single long- lived symmetric cryptographic key or Master key
- This may facilitate
  - External source other than Gatekeeper to push the Master Keys/ MKTs
  - Access to the Master Keys and Security parameters other than TCP-AO

Using IKEv2 with TCP-AO (cont.)

Solution

1. BGP/LDP sets configured Auth/KDF/lifetime info Ref to PAD Entry in GK and initiate TCP connection
2. GK triggers KMP (IKEv2)/ GK Responds to Peer KMP's trigger
3. IKEv2 negotiate Master key/CHILD_SAs
4. Master keys added to GK
5. Master Key and other negotiated parameters are kept in Key Tables
6. GK converts IKEv2 keys into MKTs, Populates in TCP-AO; revokes and/or retriggers IKE as needed
7. Use KDF to derive TCP-AO traffic-keys
8. TCP session protected



Would like to request for WG adoption.

Questions & Comments?

Thank You!