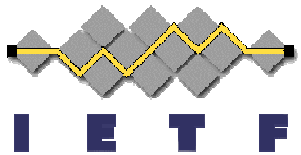
Key MAnagement for Routing Transports (KMART)



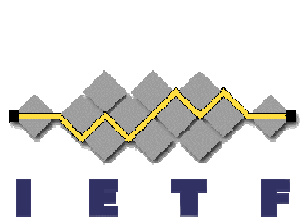
IETF 74, Rtg Area WG

Tuesday, March 24, 2009

Gregory M. Lebovitz, Juniper

gregory.ietf@gmail.com

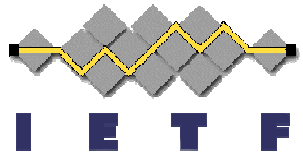
Intellectual Property



- When starting a presentation you MUST say if:
  - There is IPR associated with your draft
  - The restrictions listed in section 5 of RFC 3978/4748 apply to your draft

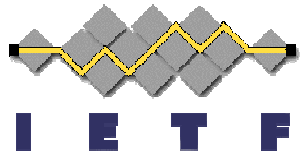
- No IPR that I know of on this document. No restrictions.

Take a Deep Breath; Don't Freak Out



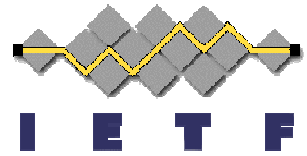
- Routing Transports are the routing protocols themselves
  - E.g. BGP/LDP, PIM-SM, OSPF etc.
- "Key Management" includes
  - Manual Key Entry, OOB or otherwise
  - Key Management Protocols (like IKEv2, or whatever)
- We are going to discuss both, starting with Manual Keying

We have a “Big Harry Audacious Goal”



- Harden the Internet’s routing infrastructure
- Achieve via incremental improvements
  - Allow routing protocol documents to advance with step by step security improvements
  - Will take some time to get to “best-possible-security-known-to-man-kind”

KMART is more narrowly scoped



- Prevent attacks at the routing protocol bits on the wire
- Threat Coverage (we want to prevent):
  - Rouge sender, non-authorized peer
  - Some DoS attacks
  - Impersonation of peer
  - Changing route messages while in transit

- Cryptographically provide:

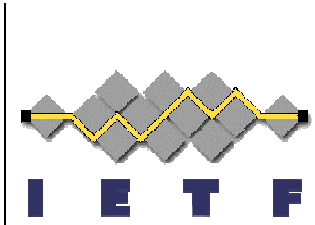
  Neighbor Authentication & Message Integrity

KMART is NOT…

- Message Confidentiality, i.e. encrypting contents so people can't read it on the wire
- Message content validation; that's SIDR's aim

STOP HERE – Everyone On Board?

Auth usage is increasing!!



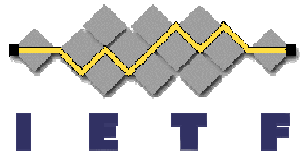
- 57% use TCP MD5 on iBGP
- 73% use TCP MD5 on eBGP
- 50% use MD5 on IGPs

ALL USE 1 KEY , HAVEN'T CHANGED

"A considerable increase was observed over previous editions of the survey for use of TCP MD5 with external peers (eBGP), internal peers (iBGP) and MD5 extensions for IGPs."

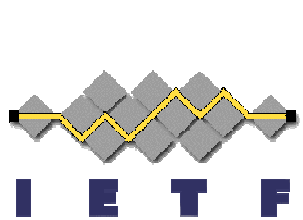
- Arbor Networs **Worldwide Infrastructure Security Report, Volume IV,** Oct 2008

We'll use modified 12 step program, just 2 Steps



- Step 1 (Sect 4.2)
  - Beef up existing protocols' basic authentication mechanism(s).
    - Usually this means some manual key or OOB management mechanism.
    - Strong algorithms, Algo agility, secure use of simple PSKs, Replay protection, mid-session key agility, etc.
    - Get ready for a KMP, or at least don't do anything that would prevent using one.

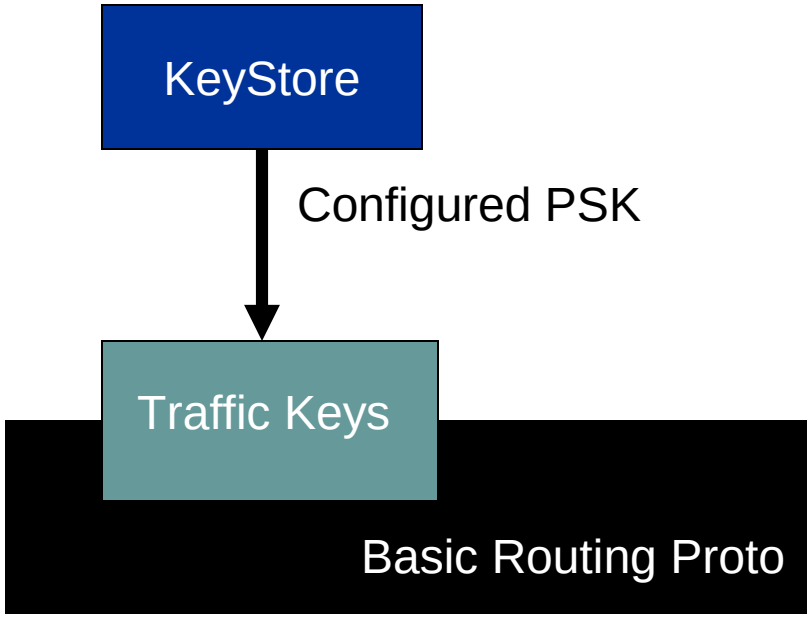
Step 2 of 2



- Introduce a KMP for operational efficiency gains
  - Use a common Framework for multiple routing protocols

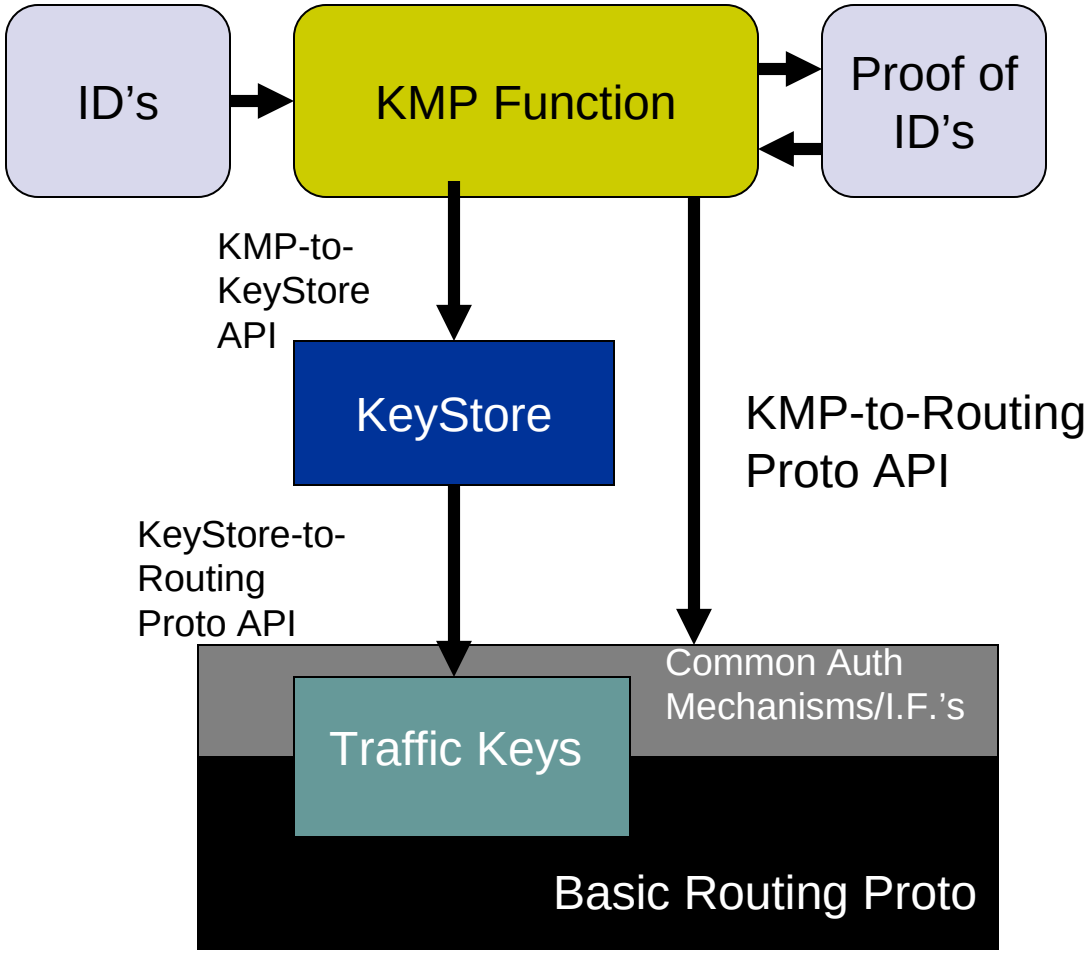
- 2 Step Example: TCP-AO
  - First update manual key mode. Once done…
  - … Introduce a KMP to provide those keys.

Step 1



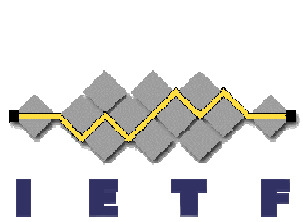
1. Define protected elements
2. Strong algos
3. Algo agility
4. Secure use of simple PSK's
5. Inter-conn. replay protection
6. Intra-conn. replay protection
7. Change parameters forces change of traffic keys
8. Use new key within a connection without data loss
9. Efficient re-keying
10. Prevent in-scope DoS
11. Support manual keying
12. All for future use of KMP

Step 2



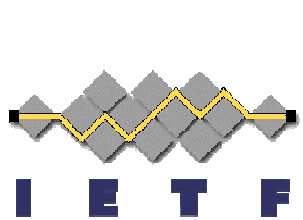
1. Layer in KMP
2. Define Identifier types/formats
3. Define ID proof mechanisms
4. Re-use KeyStore
5. Re-use Routing Proto's Manual key structure
6. Common Elements:
    1. KeyStore
    2. KeyStore-to-Routing Proto API
    3. KMP-to-KeyStore API
    4. KMP-to-Routing Proto API
    5. KMP Function

Categorize the work into like protocols



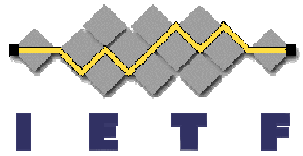
- Re-use as much as possible from common framework
- But not all Routing Protos created equally. Will be uniquenesses for each “grouping”:
  - PIM-SM
  - BFD
  - BGP/LDP/MSDP
  - OSPF/ISIS/RIP
  - RSVP, RSVP-TE

Open Issues



- Finish terminology section
- Forgot PIM-SM / -DM in 4.6 Priorities. Oops.
- New Section: Transition and Deployment Considerations.
- Pull some of Sect 4 out into own top level section
- per AF and even AF/SAF password pairs, as folks setup discrete sessions based on these?
- Define where KMART came from in text
- Capture distinction of OSPF/IS-IS in P2P modes on PtP or NBMA networks, diff than link-local
- Clean up 3.1. Category: Messaging Transaction Type

Open Questions & Answers



Next Steps

- Advertising in SAAG, SIDR, TCPM, RTG WG
- WG Document in RTG Area WG?
- Spin up work teams in parallel for protocol categories identified?

Feedback?