Keying & Authentication for Routing Protocols (KARP)

draft-lebovitz-kmart-roadmap-03

KARP BoF

IETF76, Hiroshima, Tue, 09 Nov, 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.

Agenda

- Goals / Overview
- Threat Model
- Requirements
- Framework
- What changed in -03

Agenda

- Goals / Overview
- Threat Model
- Requirements
- Framework
- What changed in -03

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”

Direction from RFC4948

- Mar 2006 “Unwanted Internet Traffic” IAB workshop, RFC 4948, Sect 8.1

  "A simple risk analysis would suggest that an ideal attack target of minimal cost but maximal disruption is the core routing infrastructure.“

- Sect 8.2 – Tightening the security of the core routing infrastructure via four steps:
  - More secure mechanisms and practices for operating routers.
    AI: OPSEC WG.
  - Clean up the Internet Routing Registry repository [IRR], and securing both the database and the access, so that it can be used for routing verifications. AI: Liaisons with the RIR's & IRR’s globally.
  - Specifications for cryptographic validation of routing message content. AI: SIDR WG.
  - Securing the routing protocols' packets on the wire. AI: KARP

KARP is more narrowly scoped

- Prevent attacks at the Routing Protocol’s bits on the wire

- Cryptographically provide:

  Neighbor Authentication & Message Integrity

- First with Manual Keys, next with KMPs

Agenda

- Goals / Overview
- Threat Model
- Requirements
- Framework
- What changed in -03

We want to prevent:

- High Level Threat Coverage:
  - Attacks from OUTSIDERS, Rogue sender, non-authorized peer
  - **Some** DoS attacks
  - Impersonation of peer
  - Maliciously changing route messages while in transit
  - Terminated employee issue

A bit more on threat model

- IN scope
  - Spoofing
  - Falsification
    - Brute force attack against keys/passwords
  - Interference
    - Adding noise
    - Replaying outdated packets
    - Inserting messages
    - Corrupting messages
    - Breaking synchronization
    - Change message content
  - DoS on transport sub-system, on keying system,

- OUT of scope
  - Sniffing
  - Falsification before sending
  - Interference due to
    - Not forwarding packets
    - Delaying message
    - Denial of Receipt
    - Unauthorized message content (SIDR)
  - Any other DoS attacks

KARP 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

Agenda

- Goals / Overview
- Threat Model
- Requirements
- Framework
- What changed in -03

Employ contemporary cryptographic best practices

- Define protected elements of the transmission
- Strong algos
- Algo agility
- Secure use of simple PSK's
- Inter-conn. replay protection
- Intra-conn. replay protection
- Change parameters forces change of traffic keys
- Use new key within a connection without data loss
- Efficient re-keying
- Prevent in-scope DoS
- Change of security mechanism / Key causes refresh of route updates or additional route updates to be generated
- Support manual keying
- All for future use of KMP

Agenda

- Goals / Overview
- Threat Model
- Requirements
- Framework
- What changed in -03

We’ll use a 2-steps program

- Step 1 (Sect 4.2)
  - Beef up existing protocols’ basic authentication mechanism(s).
    - Usually 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.

But why do we need a KMP?

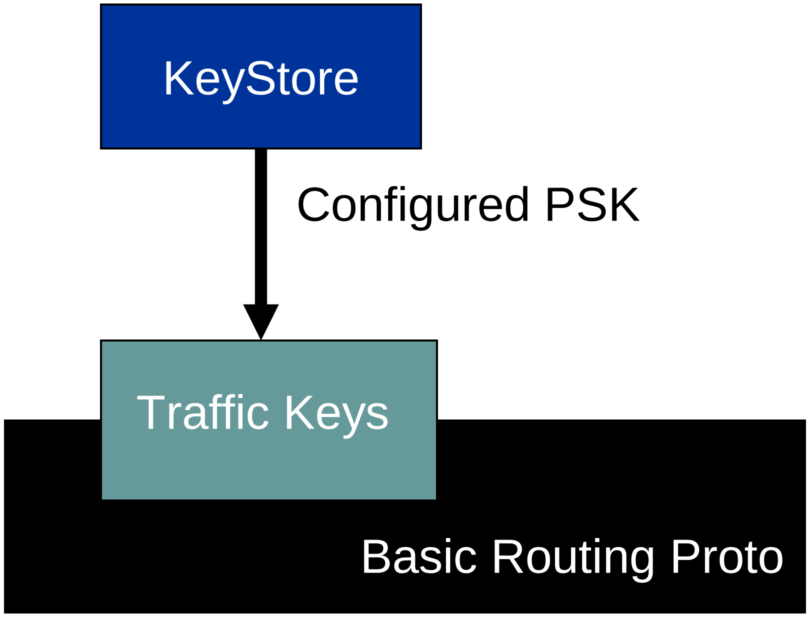
- To address brute force attacks [RFC3562] recommends:
  - frequent key rotation,
  - limited key sharing,
  - key length restrictions, etc.

- Advances in computational power make that management burden untenable for MD5 implementations in today's routing
- Keys must be of a size and composition that makes configuration and maintenance difficult or keys must be rotated with an unreasonable frequency.
- KMPs help A LOT,

IF

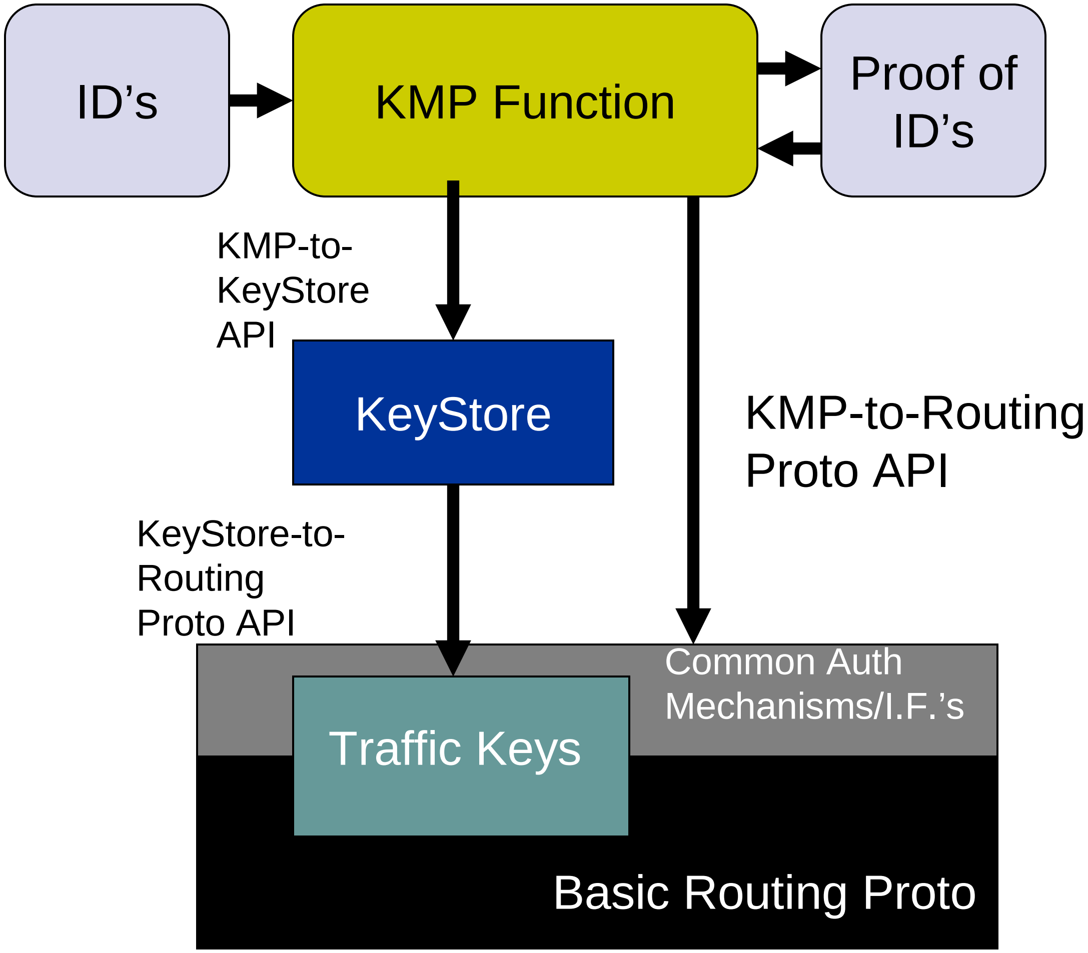
you can make them operationally usable

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

Categorization

- Communication model
  - One-to-One, e.g. BGP, LDP
  - One-to-Many, e.g. OSPF, IS-IS
  - Multicast, e.g. PIM
  - Client-Server, BGP route reflector
  - Discovery (?) – Dave Ward

- Keying Model
  - Peer Keying
  - Group Keying

Categorize the work into like protocols

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

Agenda

- Goals / Overview
- Threat Model
- Requirements
- Framework
- What changed in -03

Changes in -03

- Filled out the terminology section
- Added PIM-SM in 4.6 Priorities. Lowered OSPF & BFD, raised PIM-SM, per feedback on list.
- New text in work plan section: Transition and Deployment Considerations.
- Pulled some of Sect 4 out into own top level section
- Define where KMART and KARP came from in text
- Captured distinction of OSPF/IS-IS in P2P modes on PtP or NBMA networks, different than link-local
- Changed "BaseRP" to "Routing Protocol" throughout the doc
- Changed "KMART" to "KARP" in everything but the title, since the. Will change the title to “KARP” after the BoF.
- added "Brute Force Attacks Against Password/Keys" to Threats Section 2.1 section.

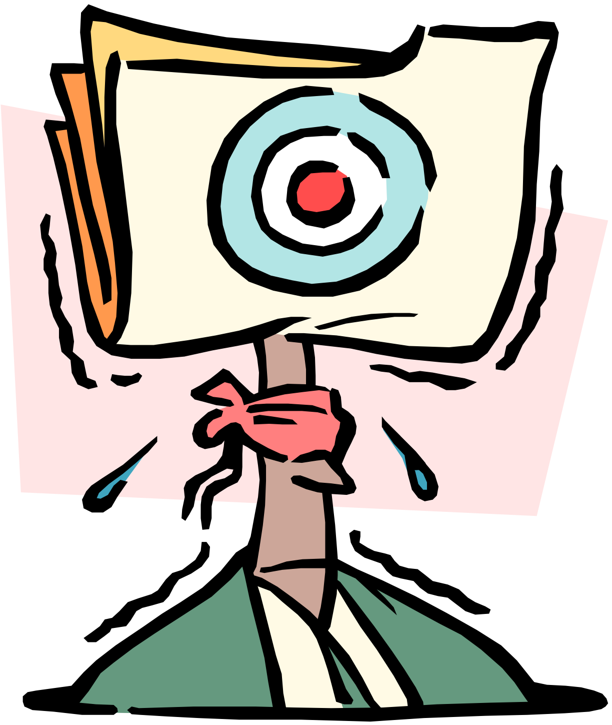
… Changes in -03

- Significant updates to Security Considerations section
- 4.3 2nd to last Paragraph - added a comment to clarify that two parties (or an org) must discuss ahead of time what they want their connections' security properties to be. - dward
- added 3.3 (but not sure if this is right)- endpoint discovery mechanisms? endpoint discovery mechanism (L2VPN, L3VPN, etc). Discovery is much different security properties than passing Routing updates. - dward
- More requirements: Added to 4.2: X - convergence SHOULD not be affected by what we choose; adding security SHOULD not cause a refresh of route updates or cause additional route updates to be generated; adding auth should not be an attack vector itself.
- updated stats on MD5 usage, and cited [ISR2008]. - mchpherson

Let’s get to work

- Submit draft with new title, changing “KMART” to “KARP”
- Create 4 smaller docs. Additional Editors/Authors:
  - Threat Model
  - Requirements
  - Framework
  - Guidance to Routing Protocol KARP work teams

Feedback?



draft-lebovitz-kmart-roadmap-03