KARP WG
IETF 83, Paris

KARP Overview, Threats and Requirements

Gregory Lebovitz and Manav Bhatia

What triggered the changes?

- Triggered by an extensive review from the Security and Routing Directorate, IETF LC comments, and some internal reviews

New Document Title

“Keying and Authentication for Routing Protocols (KARP) Overview, Threats, and Requirements”

- Better represents the content in the document.
- Follows same format as companion, KARP Design Guide

Document Structure

OLD

1. Intro
   - 1.1 Terminology
   - 1.2 Requirements Language
   - 1.3 Scope
   - 1.4 Incremental Approach
   - 1.5 Goals
   - 1.6 Non-Goals
   - 1.7 Audience
2. Threats
3. Requirements

NEW

1. Intro
   - 1.1 Terminology
   - 1.2 Requirements Language
2. KARP Effort Overview
   - 2.1 Scope
   - 2.2 Incremental Approach
   - 2.3 Goals
   - 2.4 Non-Goals
   - 2.5 Audience

2. Threats

3. Requirements

Clarifies Nature of how Doc Covers “Threats”

- RFC 4593: Provides a description and summary of threats that affect routing protocols
- Threats-reqs simply applies 4593 in the scope of KARP. Threats-reqs is NOT a full threat analysis
- Encourages analysis teams to read 4593, and apply per threat-reqs “Threats” section
- Changes in Abstract, Intro and Threats Section 3 to clarify the above

Threats Section Restructured

OLD

2. Threats

2.1 Threats in Scope

2.2 Threats out of Scope

NEW

3. Threats

3.1 Threat Sources

3.1.1 OUTSIDERS

3.1.2 Stolen Keys

3.1.2.1 Terminated Employees

3.2 Threat Actions In Scope

3.3 Threat Actions Out of Scope

- Discussed threat sources as separate from actions
- New text to explain how the stolen keys use case is a hybrid between INSIDER and OUTSIDER
- New text to clarify why Terminated Employee case so important, drives so many of our requirements

Requirements Section (1/4)

- Added a note that these requirements are meant for Phase I of the KARP effort. Will deal with Phase 2 requirements as part of the KMP framework effort.
- Req #6 – EDIT: change of security parameters MUST force a change of traffic keys, to saying it MUST change them immediately.

Requirements Section (2/4)

- Req # 5a - Added text more clearly stating that messages protected with a group key must be resilient to an attacker changing the source address on the packet.
  - It requires that a string be added to the protected packet uniquely identifying the sender, such that a change to the identity will cause the MAC to be invalidated.

Requirements Section (3/4)

- Req #10 – Clarified text around “MUST define a default security mechanism settings for all implementations to use when no explicit configuration is provided.”

- #22 – NEW: text warns against circular dependencies.

  If authentication and security mechanisms rely on systems external to the routing system, then there MUST be one or more options available to avoid circular dependencies.

Requirements Section (4/4)

- -03's Req # 17 Removed

"The authentication mechanism does not provide message confidentiality, but SHOULD NOT preclude the possibility of confidentiality support being added in the future."

  - Difficult (impossible) to fulfill without knowing what/if a future confidentiality solution would be.
  - Thread on list: "subject: requirement 17 from karp-threat-reqs-03"

Security Considerations

- Added: When Group Key Used…
  - Though spoofing by a legitimate neighbor is a BYZANTINE attack (insider attacks), and therefore ought to be out of scope,
  - Encourages KARP protocol design teams to at least consider the attack and determine, based on the costs and benefits, if a plausible solution can be employed, then document the decision, <u>either</u> way.

Plan of Action

- Document has cleared one WG LC,
- In addressing IESG review comments, changes were substantial, so decided to come back beforew WG
- Re-initiate WG Last Call
- Rev an -05 w/ latest LC comments
- Progress -05 ASAP through to IESG Review again

NEEDS TO BE DONE QUICKLY, AS OTHER DOCS DEPEND ON IT !!