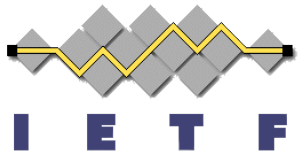
KARP
Threats & Requirements

Draft-ietf-karp-threats-reqs-00



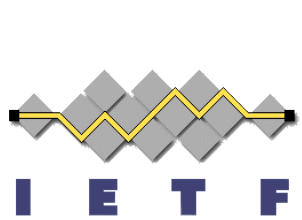
IETF77 Anaheim

Mon, 22 Mar, 2010

Gregory M. Lebovitz, Juniper

gregory.ietf@gmail.com

Intellectual Property



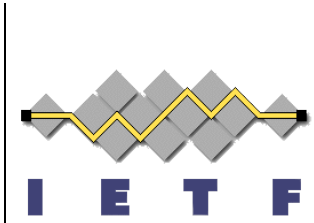
- When starting a presentation you MUST say if:
  - There is IPR associated with your draft
  - The restrictions listed in section 5 of RFC 3978/4748 apply to your draft

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

Intro

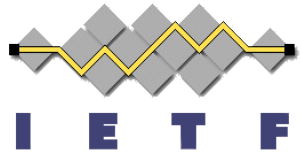
- Terminology, Scope, Goals, Non-goals, Audience → all go in -threats-reqs; -framework will remove and point to this.
- Clarification of main goal:
  - Provide authentication and integrity protection for packets on the wire, i.e. transport, of existing routing protocols,
  - NOT route update contents security. This work is being addressed in other IETF efforts, like SIDR.

A bit more on threat model



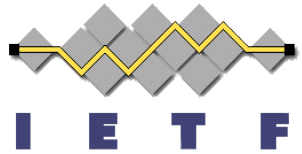
- IN scope
  - Spoofing
  - Falsification
  - Interference
    - Adding noise
    - Replaying outdated packets
    - Inserting messages
    - Corrupting messages
    - Breaking synchronization
    - Change message content
  - DoS on transport sub-system
- OUT of scope
  - Sniffing
  - Falsification before sending
  - Interference due to
    - Not forwarding packets
    - Delaying message
    - Denial of Receipt
    - Unauthorized route origination or announcement (SIDR)
  - Any other DoS attacks

Requirements that may need discussion



- Follow along on pages 15-19 of the threats-reqs-00 draft

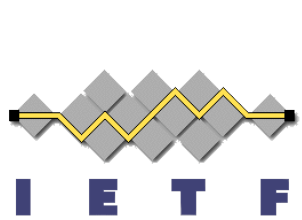
Reqs #5 & 6, Replay Protection



5. Inter-connection replay protection. Packets captured from one connection MUST NOT be able to be re-sent and accepted during a later connection.
6. Intra-connection replay protection. Packets captured during a connection MUST NOT be able to be re-sent and accepted during that same connection, to deal with long-lived connections. Additionally, replay mechanisms MUST work correctly even in the presence of Routing Protocol packet prioritization by the router (see requirement 17 below).Inter-connection & intra-connection replay protection

Clear what this means for BGP's TCP-AO, where TCP has definitive connections. Less clear how to interpret this for something like IS-IS.

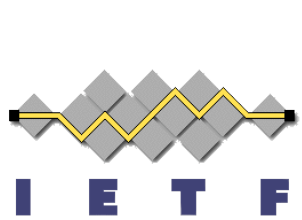
Reqs:
#19 large seq # space



19. The KARP mechanism MUST provide a sufficiently large sequence number space so that intra-connection replay protection will succeed

- More of a design guide item than a requirement?
- Include it with #6, intra-connection replay protection

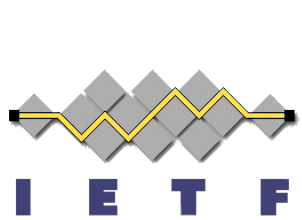
… Requirements #14



The authentication mechanism in the Routing Protocol MUST be decoupled from the key management system used. It MUST be obvious how the keying material was obtained, and the process for obtaining the keying material MUST exist outside of the Routing Protocol. This will allow for the various key generation methods, like manual keys and KMPs, to be used with the same Routing Protocol mechanism.

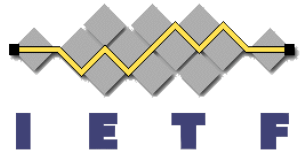
- And it will allow for the various key gen methods to be implemented once and leveraged across multiple RPs.

… Requirement 17



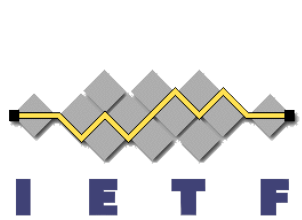
Router implementations provide prioritized treatment to certain protocol packets. For example, OSPF HELLO messages and ACKs are prioritized for processing above other OSPF packets. The authentication mechanism SHOULD NOT interfere with the ability to observe and enforce such prioritizations. Any effect on such priority mechanisms MUST be explicitly documented and justified.

Req #21 – Incremental Deployment into Operational Network



2. The new KARP mechanism MUST provide backward compatibility in the message formatting, transmission, and processing of routing information carried through a mixed security environment. Message formatting in a fully secured environment MAY be handled in a non-backward compatible fashion though care must be taken to ensure that routing protocol packets can traverse intermediate routers which don't support the new format.
3. In an environment where both secured and non-secured systems are interoperating a mechanism MUST exist for secured systems to identify whether an originator intended the information to be secured.
4. In an environment where secured service is in the process of being deployed a mechanism MUST exist to support a transition free of service interruption (caused by the deployment per se).

Req # 22 - performance



The introduction of mechanisms to improve routing authentication and security may increase the processing performed by a router. Since most of the currently deployed routers do not have hardware to accelerate cryptographic operations, these operations could impose a significant processing burden under some circumstances. Thus proposed solutions should be evaluated carefully with regard to the processing burden they may impose, since deployment may be impeded if network operators perceive that a solution will impose a processing burden which either:

* provokes substantial capital expense, or
* threatens to destabilize routers.

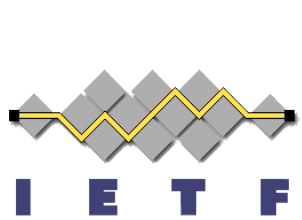
- Akin to #15 – “convergence times should not be materially affected.” Same thing?
- Formatting issue -

Req #25 (will be #23)

The new authentication and security mechanisms should not rely on systems external to the routing system (the equipment that is performing forwarding). In order to ensure the rapid initialization and/or return to service of failed nodes it is important to reduce reliance on these external systems to the greatest extent possible. Therefore, proposed solutions SHOULD NOT require connections to external systems, beyond those directly involved in peering relationships, in order to return to full service. It is however acceptable for the proposed

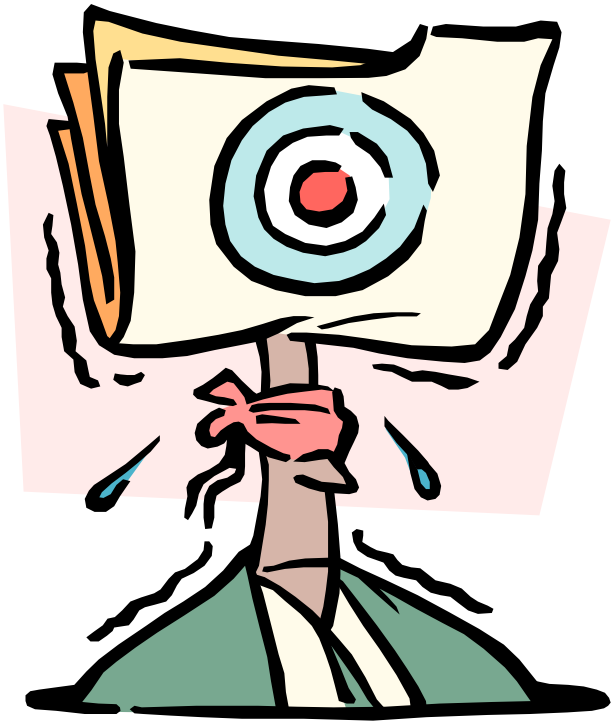
- Late entry. Clarify? Agreement?

Next Steps



- Clean up known items
- More reviews
- Start design teams

Feedback?



draft-ietf-karp-threats-reqs-00