HOKEY WG Meeting Minutes
IETF 71, Philadelphia

Agenda
Document status
Problem statement - approved
ERX - discuss open from Jari
EMSK - Key Hierarchy - Last Call

Key Management Discussion

** Chairs' Presentation

HOKEY KDE (Yoshihiro Obha)

Yoshi's Presentation

- addressed some open issues on message for mat and security
- other changes use cases, transport , automated key management, timestamp,
- Protocol format uses ASN.1 uses PER (Packed Encoding Rules)
- Hop-by-Hop supported with null encryption and integrity algorithms.
- Automated key management required for KIts and KCts (N2) problems, Kerberos used.
- Timestamp no longer used for freshness, nonce used instead.
- KDE can be carried in ERP to distribute keys. Can be used to distribute multiple keys in parallel KDE messages.
- KDE and also operate over UDP only.

Discussion

- Charles: Self contained protocol with own cryptographic protections, few transport mechanisms (ERX/AAA and UDP).

AAA support for ERP (Laksminath)

Lakshminath's Presentation:

- Reuse and rely on RADIUS key wrap
- Transport uses AAA messages (protected with RADIUS key wrap)
- Key Wrap for request
- Multiple keys can be carried in different attributes

Discussion

- Charles: Peer is out of the loop for this exchange
- Laksminath: Channel bindings and identity are provided by the peer

- CC: Two approach in front of the working group. Own message protection or a RADEXT based solution
- Bernard A: If you don't encrypt you can use the same encryption with Diameter or RADIUS
- CC: Timeline
- BA: works over security used today (IPSEC, Diameter, TLS)
- CC: Interop issues?
- BA: Server and client must support the same one on a hop - by hop basis
- CC: Concern, the peer doesn't know what the backed is doing with the key
- BA: always a concern
- GZ: only one Key with MPPE Keys
- BA: you need a new attribute
- JS: use existing key wrap to carry keys
- David Nelson: Have a key container attribute
- CC: Transport within RADIUS and DIameter should attribute provide its own protection?
- DN: Would rather see closer to RADIUS guidelines
- CC: RADIUS key wrap closer to RADIUS guidelines
- CC: do we want to support over other transports such as UDP?
- LD: what is the motivation for other transports? Do we want to redo that? doesn't think we should.
- Tim Polk: Need a good reason to redo work. Short timeline, redoing the work is probably not in your best interest.
- BA: Is this doing something new?
- CC: KDE is new messages over UDP, Yes
- GZ: yes new protocol
- Pasi: What is the difference between KDE0 and KDE1 and ERX
- CC: Different parties involved in back end network.
- PE: ?
- CC: ERX - Peer auth and home, KDE binds to visited server and ?
- CC: Do people understand these approaches?

Consensus Questions

- Q1: Should HOKEY rely on AAA transport security?
    - HUM if you think we should rely on AAA?
    - HUM if we should use our own?
    - Loud consensus for AAA transport security
- Q2: Interest in supporting non-AAA transports?
    - Hum if we should only consider AAA?
    - Hum for non-AAA transports?

    - About 50-50

Discussion

- LD: does not have objection to non-AAA, but seems like research project
- TP: what are we going to accomplish of non AAA transports. Seems like an enlargement of AAA.
- GZ: Nont sure if it is an enlargement of charter, but not sure it is going to accomplish anything.
- LD: cites from charter. If AAA doesn't work then charter allows it
- GZ: what are the objectives. Is there is a use case where AAA does not work
- Yoshihiro: Do we need 3 party key distribution? Key wrap is two party key distribution. Research papers on key distribution protocols point out no peer consent on 2 party protocol. Key can be requested without peers consent.
- GZ: what is the real security objective. I don't know that the channel binding help. Using ERX indicates desire to use keys.
- SH: Maybe multiple services in the domain, Channel bindings is important, but not required here.
- CC: So don's solve channel bindings here.
- SH: Leave space for it, don't solve the problem here.
- JS: This should be coordinated with what happens in RADEXT
- BA: new attribute can be made
- SH: Do it right in one place.
- YO: remove keys from KDE document?
- CC: Do we want to support the peer consent property? MAC needed in initial message
- CC: Do we want peer consent in protocol?
- TP: There is some level of peer consent. There is an aspect of peer consent.
- CC: Authenticated request
- Katrin: Active involvement of the peer not necessary at this point.
- BA: some consent necessary or anyone can ask.
- PE: Not sure that peer consent is needed for delivering keys. Would be good to have indication that keys used to prevent fraud.
- BA: ERX is vulnerable to Fraud
- GZ: How does ERX modify RADIUS accounting?
- BA: anyone can request a key and initiate billing. You don't proof that they were there
- GZ: I don't think that actually true. An not distributed to anyone.
- LD: There are business agreements in place.
- BA: had some proof, had some link of accounting to auth
- GZ: when you move to new domain you do EAP. HOKEY and ERX are within one admin domain, not between domains. Auth
- Alan(Jabber): this is an issue with proxy today Username and password.
- SH: from the client side of ERX there is nothing that limits it to one domain.
- CC: ERX handoff between key management domain not admin domain.
- SH: Problem exists unless domain is limited

- LD: In AKA triplets are sent to visited domain. Fraud could be perpetrated here. The market doesn't need this solution.
- CC [two options]
- JS: What does domain mean?
- GZ: permits authentication across domain this is wrong
- CC: two solutions:
  - Option 1: authenticated peer consent
  - Option 2: security considerations
- CC: remove crypto from key management document.
- JS: general RADIUS key delivery attribute would be better.
- BA: Better to use a attribute to specific to HOKEY to prevent interoperability problems
- DN: design your own and see if it is generally useful.
- GZ: Doesn't see how it affects interop
- TP: only need to satisfy hokey requirements
- Katrin: Can remove messages from KDE document
- CC: all except 2 and 3
- GZ: doesn't this get rid of KDE?
- In favor of proposal to move forward as on Charles' slide? HUM is favor?
- LD: can I be an author?
- CC: yes

Pre-Authentication (Yoshi)

- No discussion, positive or negative. Proceed with WGLC.