PCP Authentication Methods

Yoshihiro Ohba
Yasuyuki Tanaka
Subir Das
Alper Yegin
Tina Tsou

issue#60: Loosely coupled vs. tightly coupled authentication

- EAP session lifetime, EAP session keys lifetime, hence PCP SA (security association) lifetime are all driven by the AAA server.
- The state created by the execution of PCP (i.e., NAT mappings, firewall rules) may have a lifetime different than the PCP SA lifetime.
- (Note: whatever the deployment chooses, it can be supported by PANA and EAP-o-PCP)

issue#61: Unsolicited reauthentication

- If PCP SA is not maintained at all times, then an unsolicited PCP message from the server may need to trigger unsolicited re-authentication.

- RADIUS and Diameter support EAP re-authentication initiated by the AAA server. Unless we explicitly forbid that, they are there to be supported by any EAP lower-layer.

- (Note: PANA can be used w/o PAA-initiated re-auth as well).

issue#62: Client-driven or server-driven auth retransmissions

- EAP is a server-driven protocol. Not clear if a client-driven EAP lower-layer can work (see http://www.ietf.org/mail-archive/web/abfab/current/msg01746.html for a single packet stalling the protocol flow as an issue)

- What is the objective of client-driven rexmits?
  - State savings on the server? No, there’s still state.
  - Alignment with PCP? Not a worry if auth is offloaded to PANA.

Solution Options

1. Using PANA (RFC 5191 – EAP-over-UDP)
   a. Side-by-side (i.e., PANA and PCP executed over the same port) [draft-ohba-pcp-pana-03]
   b. Tunneled (i.e., PANA carried over PCP) [draft-ohba-pcp-pana-encap-00]

1. Defining a new EAP lower-layer (EAP-over-PCP/UDP) [draft-wasserman-pcp-authentication-02]

Why use PANA?

- An IETF standard (RFC 5191)
- Already adopted by other standards
  - Zigbee IP
  - ETSI M2M
  - ATIS IPTV
- There are two open-source implementations
- Multiple commercial implementations that have passed interop tests
- Fits the problem
  - Negligible amount of extra (15-20 lines of code for IP Reconfig and PANA Ping which are not needed for PCP)

EAP-over-PCP/UDP

- Currently incomplete
  - Missing EAP Reauthentication support
- Technically possible
  - But designing a security protocol is non-trivial/time-consuming
- Re-inventing the wheel (by even borrowing design from PANA)
  - Not clear why “re-creating PANA under the PCP hood” is a better approach than “re-using PANA”
- Imposes additional consideration on the PCP implementation as now PCP implementation needs to act as an EAP-lower layer and support EAP-style (server-driven req/rsp) messaging
- Each protocol in need of security keys designing its own EAP lower-layer is not a scalable approach for IETF
  - Re-use of a separate/independent protocol provides modularity

PANA-based Approaches

- Side-by-side PANA
  - Pros
    - Separation of PANA and PCP over-the-wire providing flexibility
  - Cons
    - One of the Reserved PANA bits needs to be allocated for supporting port-sharing operation
- Tunneled PANA
  - Pros
    - No bit allocation
  - Cons
    - Encapsulation overhead. 24 extra bytes per PANA packet