PCP Authentication Methods

Yoshihiro Ohba
Yasuyuki Tanaka
Subir Das
Alper Yegin

Options

1. Using PANA (RFC 5191 – EAP-over-UDP)
   a. Side-by-side (i.e., PANA and PCP 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 several 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 not easy/fast
- 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”
- Complicates PCP implementation as now PCP implementation needs to act as an EAP-lower layer and support EAP-style messaging
- Each protocol in need of security keys designing its own EAP lower-layer is not a scalable approach for IETF
  - Re-use of independent key management provides modularity

PANA-based Approaches

- Side-by-side PANA
  - Pros
    - Separation of PANA and PCP over-the-wire giving 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