PANA threat analysis and security requirements

draft-ietf-pana-threats-eval-02.txt

Mohan Parthasarathy

Tahoe Networks

PANA threats update

- Removed Identity Protection from the list of threats after feedback from last IETF.
- Added a new threat “Device Identifier attack”
- Renamed “data protection” to “service theft”.
- Removed requirements on confidentiality.

PANA threats update

- Clarified the trust relationships between the various entities involved in the protocol.
- Added reference to threats in PAA-AS path.
- Rest are mostly editorial.

Service theft

- Most of the feedback essentially asked the question “How does PANA prevent service theft ?”
- Tried to clarify in the latest revision.
- If the link is not shared, ingress filtering should prevent service theft.
- If the link is shared, but link layer provides per-packet MIC, it prevents service theft.

Service theft

- If the link is shared, but link layer does not provide any protection, this threat is present.
- To avoid this threat, there needs to be an SA between PaC and EP that provides per-packet Message Integrity Check (MIC)
- How does PANA help establish this SA ?
  - PANA protocol establishes a trust relationship between PaC and PAA
  - Trust relationship can be further used to establish an SA to prevent service theft e.g. IPsec SA between client and EP