Comparison of PCP Authentication Approaches

draft-ohba-pcp-pana-03.txt
draft-ohba-pcp-pana-encap-00.txt
draft-ietf-pcp-authentication-00.txt

PCP Interim Call, October 17, 2012

Margaret Wasserman
Painless Security

PCP Authentication Status

- Three proposals currently under discussion for key management in PCP
  - Two PANA proposals, both run PANA and PCP on the same port
    - Demultiplexed (side-by-side)
      Described in draft-ohba-pcp-pana-03.txt
    - Encapsulated
      Described in draft-ohba-pcp-pana-encap-00.txt
  - One PCP-Specific proposal
    - Described in draft-ietf-pcp-authentication-00.txt
- All proposals use EAP for authentication
- All proposals use the same option for carrying authentication information in PCP messages

What is the same?

- All three approaches use EAP (and EAP methods) for authentication
- All three approaches use the same PCP options to pass authentication information in PCP requests
  - Defined in draft-ietf-pcp-authentication-00.txt
- All three approaches use a similar technique to generate keys

- The only signficant difference between these approaches is whether we use PCP-Specific mechanism for key management, or whether we use PANA for key management (either side-by-side with PCP, or encapsulated in PCP messages).

What is PANA?

- RFC 5191: Protocol for Carrying Authentication for Network Access
- Three defined PANA entities:
  - PaC: PANA Client
    - Provides credentials to prove its identify for network access authentication
  - PAA: PANA Authentication Agent
    - Verifies credentials offered by PANA client, and authorizes network access
  - EP: Enforcement Point
    - Blocks all traffic (except PANA, ARP, ND, DHCP) to/from any unauthorized client

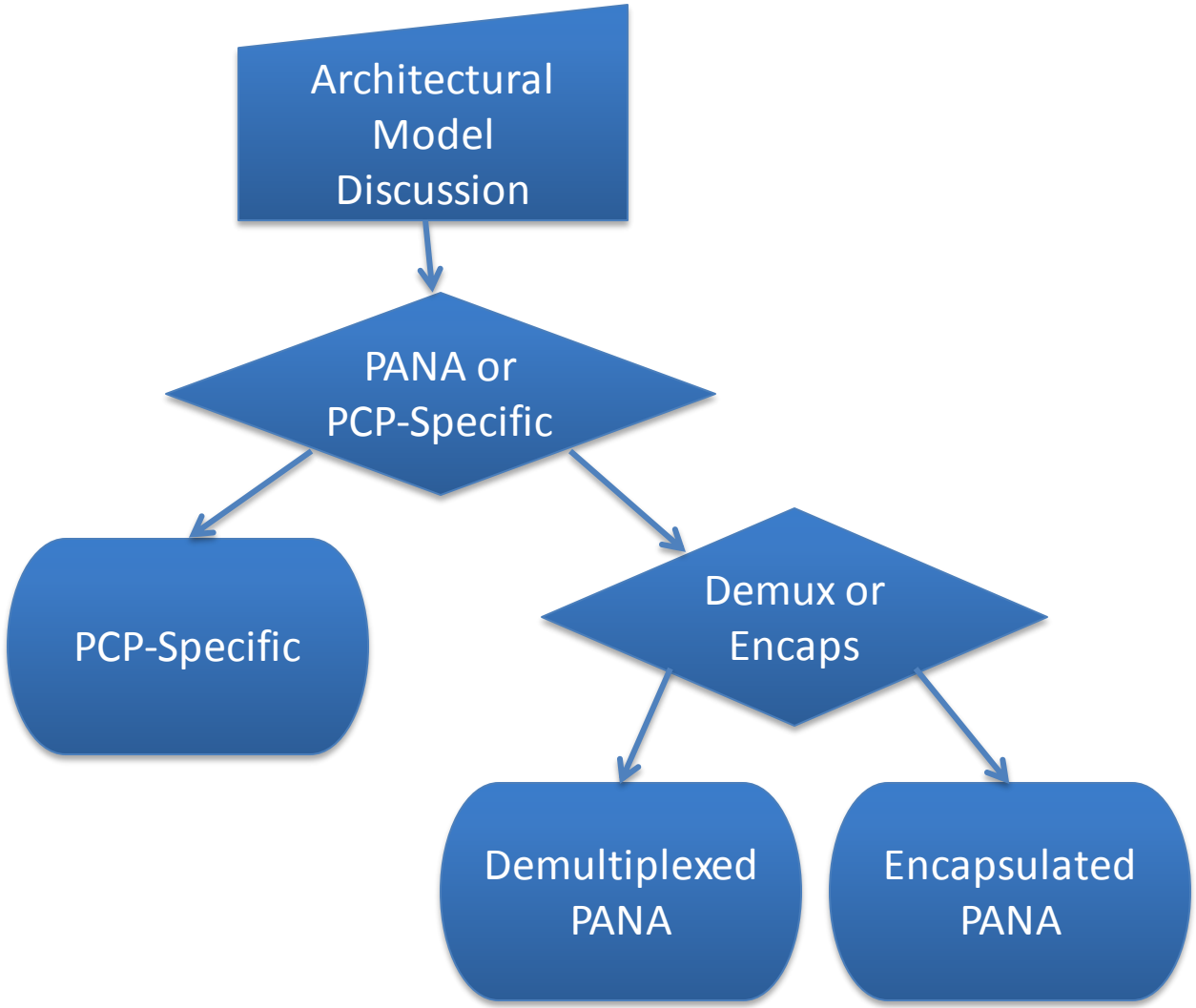
PANA Phases

- Authentication and authorization phase
  - A new PANA session is initiated and EAP is executed. Until authentication is complete, network access is blocked by the EP
- Access phase
  - Access device has access to the network
  - “Liveness Tests” may be performed by the client or server sent at any time during this phase
- Re-authentication phase
  - Sub-phase of access phase
  - Either side may initiate re-authentication to update the PANA session lifetime
- Termination phase
  - Either side may terminate, explicit termination message may be sent. After termination, network access is blocked by the EP.

PANA Properties

- Used to control network access
  - Potentially a continuous stream of packets between PANA client and arbitrary other nodes
    - Interruption of the stream could cause application failures
  - Accessing the service (network access) does not involve ongoing traffic between the PANA Client and the PANA Authentication Agent
- Authentication and authorization are tightly coupled
  - PANA client must be continually available for “liveness tests” or re-authentication, in order to retain network access

PCP Authentication Decision Tree



PCP Authentication/Authorization

- Loosely coupled:
  - Authentication needed only at the time of a request, to create/modify a mapping.
  - Authorization done separately, using the same mechanism as in non-authenticated PCP
    - Mappings are removed when authorization is revoked
  - Mapping lifetime is not tied to authentication lifetime
- Tightly coupled:
  - Authentication and authorization are performed using the same mechanism, or there is a link between them
  - Mapping lifetime is tied to authentication lifetime
    - Mappings are removed when keys expire OR authorization is revoked

Re-Authentication

- Would it be desirable to support unsolicited re-authentication?
  - May depend on previous answer – is there a need to renew authentication information when no requests are being issued?
- Or is it preferable to wait until a new mapping request is issued, and start a new authentication process then, if needed?

Operational Model

- PCP is a client-initiated request/response protocol with one-way notifications
  - Should authenticated PCP follow the same model?
  - Or is acceptable to use a different model for authenticated PCP?
- Should a client need to remain reachable in order to defend/retain it's mappings?

PCP-Specific Model

- PCP remains a client-initiated request/response protocol with notifications
  - No “liveness tests”
  - No unsolicited re-authentication or retransmission
  - In fact, no unsolicited messages that require a response
- Authentication and authorization are loosely coupled
  - Mappings survive key expiration, but are removed if authorization is revoked
  - Authorization mechanism same as unauthenticated PCP
- Clients do not need to remain reachable for mappings to remain active
- Simplified PANA-like mechanism, similar to gss-eap (currently in RFC Editor queue)

PANA Model

- Requires support for server-generated requests
  - To support server-initiated re-authentication or retransmissions
  - To support “liveness” detection [optional]
- Authentication and authorization tightly coupled
  - Supports ability to drop mappings immediately when authentication expires
- Clients need to remain active on the network to retain their mappings
  - Mappings are removed if the client goes away or fails to respond to re-authentication requests

Demux Approach

- Received packets are demultiplexed by overloading on three bits in the PCP version field
  - Zero bits (“000”) indicate that this is a PANA packet
    - Requires reserving these bits in PANA
  - Any other value is PCP (version 2 is “010”)
    - Requires reserving 1/8th of the PCP versions 0, 8, 16, 32, etc…
- Whole packet is handed to PANA for processing
- PCP entities that do not implement PCP Authentication will see these packets as having an unsupported version number
  - Errors will go back to PCP client in this case, not to PANA client

Encaps Approach

- Define a PCP opcode that indicates that the contents are a PANA packet
  - Packets received with this opcode are PANA packets, other PCP header fields can be ignored
  - All other opcodes indicate that this is a PCP packet
- PANA portion is handed to PANA for processing
  - All but the first 24 bytes of the packet
- PCP entities that do not implement PCP Authentication will report an unknown opcode

What is the Difference?

- In demux case, we overload the version field and hand the entire packet to PANA

- In encaps case, we have no overloading, and we have to add 24 bytes to the packet pointer before sending it to PANA

Discussion

- What criteria should we use to decide between the different approaches?
- Where do we go from here?