Discussion of PCP Authentication Approaches

IETF 85, Atlanta, November 2012
Margaret Wasserman
Painless Security
Three Drafts Under Discussion

• PCP Authentication Mechanism
  – Describes PCP authentication options used in all choices
  – Defines a lower layer to run EAP directly over PCP

• Two alternatives that use PANA for key exchange
  – Provisioning Message Authentication Key for PCP using PANA (Side-by-Side Approach)
  – Provisioning Message Authentication Key for PCP using PANA (Encapsulation Approach)
What is the same?

• All three approaches use EAP (and EAP methods) for key generation
• All three approaches use the same PA Security Association structure
  – As defined in draft-ietf-pcp-authentication-01.txt
• All three approaches use the same PCP Authentication option to pass authentication information in PCP requests, after keys are generated
  – As defined in draft-ietf-pcp-authentication-01.txt
What is Different?

• The only difference between these approaches is whether we use EAP directly over PCP for key management, or whether we use EAP over PANA for key management (either side-by-side with PCP on a single port, or encapsulated in PCP messages)

• In other words, the only difference is how we transport EAP messages
  – directly in PCP messages
  – in PANA messages encapsulated in PCP messages, or
  – in PANA messages sent side-by-side with PCP messages
Direct EAP-over-PCP Approach

• Defines a EAP lower layer
• EAP messages are sent directly in PCP messages
  – Defines PCP Authentication OpCode
• Key management is based on simplified version of PANA and GSS-EAP
• Mechanism allows for both client-initiated and server-initiated security
  – Clients can choose to make secure requests
  – Servers can require authentication when needed
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
Side-by-Side Approach

• Received packets are demultiplexed based on the first bit of the PCP version field
  – A value of “1” indicate that this is a PANA packet
    • Requires reserving this bit in PANA
  – Any other value is PCP
    • Limits PCP version numbers to < 128
• 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
  – An unspecified capability discovery mechanism is mandated to avoid this situation
Encapsulated 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
• 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 if they receive these messages
PCP Authentication Decision Tree

Architectural Model Discussion

PANA or EAP-over-PCP

EAP-over-PCP

PANA Demux or Encaps

Demultiplexed PANA

Encapsulated PANA
Issue #60: Coupling of Authentication & Authorization

• Loosely coupled:
  – Authentication needed only at the time of a request, to create/modify/query a mapping.
  – Authorization done separately, using the same mechanism as in non-authenticated PCP (implementation-specific)
  – Mapping lifetime is not limited to authentication lifetime
    • NAT/Firewall determines mapping lifetime
    • Mapping lifetime may or may not be dependent on key lifetime, may be shorter or longer than key lifetime

• Tightly coupled:
  – Authentication and authorization are both performed using AAA
  – Mapping lifetime is limited to authentication lifetime
    • PCP/PANA server removes mappings when keys expire
    • Mapping lifetime must be equal to or shorter than key lifetime
Issue #61: Re-Authentication

- **Server-Originated Re-Authentication Costs**
  - Requires nodes to stay awake or on the network to respond to re-authentication messages
    - In tightly-coupled authorization approach, nodes that do not stay reachable will lose their mappings
  - May result in unneeded key exchanges
    - Possibly many unneeded key exchanges for each time the keys are actually required in loosely-coupled authorization approach, as key lifetimes may be much shorter than mapping lifetimes

- **Server-Originated Re-Authentication Benefits**
  - Keeps keys current, so they don’t need to be exchanged when a subsequent PCP Request is initiated
    - Minor benefit, as cost to exchange keys at that time is low, and cost of repeated key exchange may be higher
Re-Authentication Timelines

Assumptions: Loosely coupled authentication/authorization, mapping lifetime is 24 hours, key lifetime is one hour.
Issue #62: Retransmissions

• Do we need support for server-generated retransmissions?
  – EAP can do retransmission from both sides
  – EAP also allows lower-layers to handle reliability and do their own retransmissions
  – GSS-EAP is an example of an EAP lower-layer that does not do server-generated retransmissions
Operational Model

• All of these issues could potentially affect the PCP 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?
    • Server-initiated re-authentication, and server-generated retransmissions
• Should a client need to remain reachable in order to defend/retain its mappings?
  – Tightly-coupled authentication/authorization with server-initiated re-authentication
PCP Authentication Decision Tree

Architectural Model Discussion

PANA or EAP-over-PCP

EAP-over-PCP

PANA Demux or Encaps

Demultiplexed PANA

Encapsulated PANA
Direct EAP-over-PCP Model

• PCP remains a client-initiated request/response protocol with notifications
  – No “liveness tests”
  – No unsolicited re-authentication or retransmission
  – In fact, no server-generated 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
PANA Model

• Requires support for server-generated requests
  – To support server-initiated re-authentication and retransmissions
  – To support “liveness” detection
  – Alternative is to update PANA to remove these things

• 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
PCP Authentication Decision Tree

Architectural Model Discussion

PANA or EAP-over-PCP

EAP-over-PCP

PANA Demux or Encaps

Demultiplexed PANA

Encapsulated PANA
Key Differences

• In demux case, we overload the first bit of 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
Conclusions?

• What decision should we reflect in the next version of the PCP Authentication document?