Authentication Mechanism for Port Control Protocol (PCP)

draft-wasserman-pcp-authentication-01.txt

Margaret Wasserman

Sam Hartman

Painless Security

Dacheng Zhang

Huawei

PCP Security Models

- PCP Base draft defines two threat models:
  - Simple Threat Model
    - Not concerned about spoofing by on-link attackers
    - Goal to be no _less_ secure than implicit mappings
    - Imposes limits on PCP operation
  - Advanced Threat Model
    - For use in all cases where the limitations of the simple threat model are not acceptable
    - Requires authentication and integrity protection
    - PCP Authentication draft proposes a security mechanism to address this threat model

Simple Threat Model

- A PCP Server is secure under this threat model if the PCP Server is constrained so that it does not configure any explicit mapping that it would not configure implicitly.
- Goal is to be secure against off-path attackers who cannot spoof a packet that appears to come from the internal network
  - Other nodes on the internal network are considered friendly/non-threats

Typical STM Limitations

- All internal hosts are within a single administrative domain, or can be securely partitioned by PCP Server
- Explicit mappings are created with the same lifetime as implicit mappings
- The PCP server does not support deleting or reducing the lifetime of existing mappings
- The PCP server does not support the THIRD_PARTY option
- MAP is supported only if the security policy on the device running the PCP Server would permit endpoint independent filtering of implicit mappings

Advanced Threat Model

- PCP Requests that do not meet the limitations of the Simple Threat Model must be authenticated and integrity protected
  - Includes all DELETE operations, THIRD_PARTY options, and mappings that would not be made implicitly
- A PCP client may send, and a server may accept, unauthenticated requests that match the Simple Threat Model _and_ authenticated requests that support the Advanced Threat Model

PCP Security Use Cases (1)

- Security infrastructure equipment (such as corporate firewalls) that does not create implicit mappings
- Equipment (such as CGNs or service provider firewalls) that serve multiple administrative domains and do not have a mechanism to securely partition traffic from those domains
- Any implementation that wants to be more permissive in authorizing explicit mappings than it is in authorizing implicit mappings
- Proxies or other implementations that support the THIRD_PARTY Option
- Implementations that wish to support any deployment scenario that does not meet the constraints described in the STM

PCP Security Goals

- Make simple things simple
  - Operations that fit within the Simple Threat Model don’t have to use PCP Authentication
- Make complex things possible
  - Operations that do _not_ meet the constraints of the STM can be performed using PCP Authentication

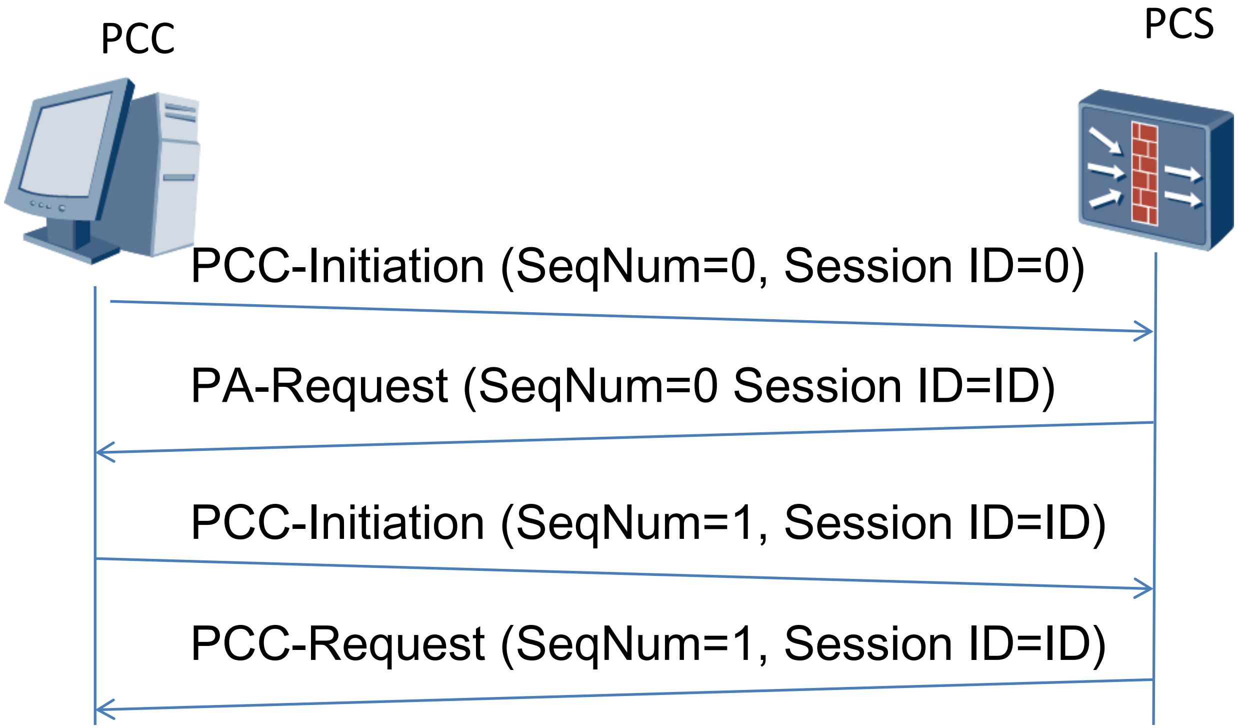
PCP Authentication Overview

- PCP Authentication relies on EAP for authentication and key derivation
  - Use of EAP is consistent with widely deployed enterprise security systems
  - Can also scale down to simple shared keys for a single proxy/PCP server combination
- Mechanism allows for both client-initiated and server-initiated security
  - Clients can choose to make secure requests
  - Servers can force authentication when needed
- Largely based on PANA (RFC 5191)

PA Messages

- In a PA session, **PA-Request** messages are sent from Servers to Clients, **PA-Answer** messages are sent from Clients to Servers.
- An EAP request message MUST be transported within a PA-Request message, and an EAP answer messages MUST be transported within a PA-Answer message.
- When a PCP device receives a PA- Request or a PA-Answer message from its partner and cannot generate a response within a pre-specified period, the PCP device will reply with a **PA-Acknowledge** message to indicate that the message has been received.

Session Initiated by PCC



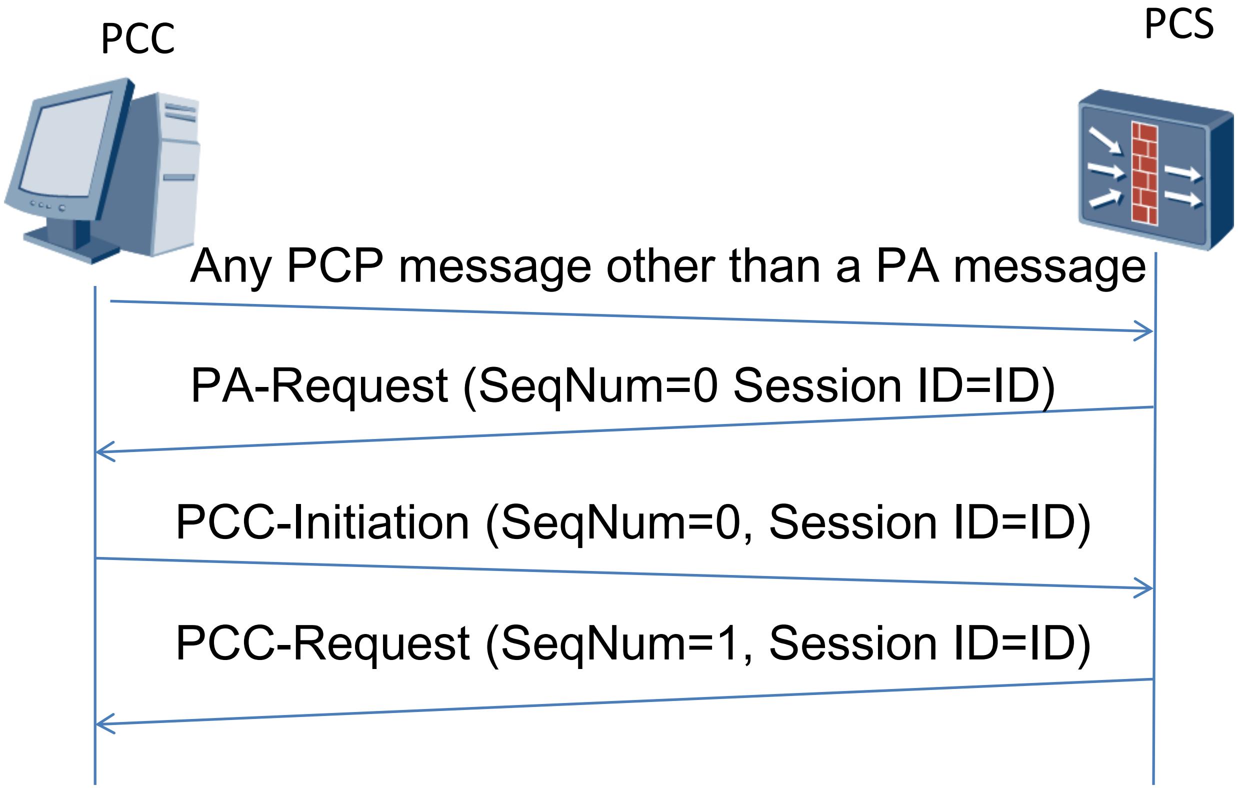
PCC-Initiation (SeqNum=0, Session ID=0)

PA-Request (SeqNum=0 Session ID=ID)

PCC-Initiation (SeqNum=1, Session ID=ID)

PCC-Request (SeqNum=1, Session ID=ID)

Session Initiated by PCS



PCC

PCS

Any PCP message other than a PA message

PA-Request (SeqNum=0 Session ID=ID)

PCC-Initiation (SeqNum=0, Session ID=ID)

PCC-Request (SeqNum=1, Session ID=ID)

Algorithm Agility

- Session partners agree on a Pseudo-Random Function (PRF) for the transport key derivation and a MAC algorithm to provide data origin authentication for subsequent PCP signaling packets.
  - The Server appends a set of PRF Options and MAC Algorithm Options to the initial PA-Request message
  - The Client selects a PRF and a MAC algorithm, and sends back a PA-Answer with a PRF Option and a MAC Algorithm Option for the selected algorithms.

Authentication Results

- The last PA-Request message transported within a PA session carries the EAP authentication and PCP authorization results.
- If the EAP authentication succeeds, the result code of the last PA- Request is **Authentication-Success**
- If the EAP authentication fails, the result code of the last PA-Request is **Authentication-Failed**
- If the EAP authentication succeeds but Authorization fails, the result code of the last PA-Request is **Authorization-Failed**

Session Termination

- A PA session can be explicitly terminated by sending a termination-indicating PA Acknowledge message from either session partner
- After receiving a termination-indicating message from the session partner, the other PCP device involved in the session MUST response with a termination-indicating PA Acknowledge message and remove the PA SA immediately
- When the session partner initiating the termination process receives the acknowledge message, it will remove the associated PA SA immediately

PA Security Association (1)

- IP address and UDP port number of the Client
- IP address and UDP port number of the Server
- Session Identifier
- Sequence number for the next outgoing PCP message
- Sequence number for the next incoming PCP message
- Last transmitted message payload
- Retransmission interval
- MSK

PA Security Association (2)

- MAC algorithm: The algorithm that the transport key should use to generate digests for PCP messages.
- Pseudo-random function: The pseudo random function negotiated in the initial PA-Request and PA-Answer exchange for the transport key derivation
- Transport key: the key derived from the MSK to provide integrity protection and data origin authentication for the messages in the PA session. The life time of the transport key SHOULD be identical to the life time of the session.

Sequence Number (1)

- Every PCP packet exchanged during EAP authentication must carries an monotonically increased sequence number.
- During a PA session, each PCP device needs to maintain two sequence numbers, one for incoming packets and one for outgoing packets.
- When generating an outgoing PCP packet, the device attaches the next outgoing sequence number to the packet
- After confirming that an incoming packet is valid, the device increments the incoming sequence number by 1

Sequence Number (2)

- However, the above rules are not applied to following conditions
  - When receiving or sending out a PA-Acknowledgement message, the device MUST not increase the correspondent sequence number.
  - Message retransmission

Any Questions?

Is the WG interested in adopting this document as a PCP WG Work Item?