Comparison of PCP Authentication Approaches

draft-wasserman-pcp-authentication-01.txt
draft-ohba-pcp-pana-00.txt

Dacheng Zhang
Huawei
Margaret Wasserman
Painless Security

PCP Authentication Status

- draft-wasserman-pcp-authentication-01.txt
  - Defines options to pass authentication information in PCP requests/responses
  - Define an in-band, PCP-specific key management method
  - Draft mentions open question about key management (in-band or separate?)
- draft-ohba-pcp-pana-00.txt
  - Defines a separate key management mechanism using PANA
  - Leverages same PCP options defined in previous draft

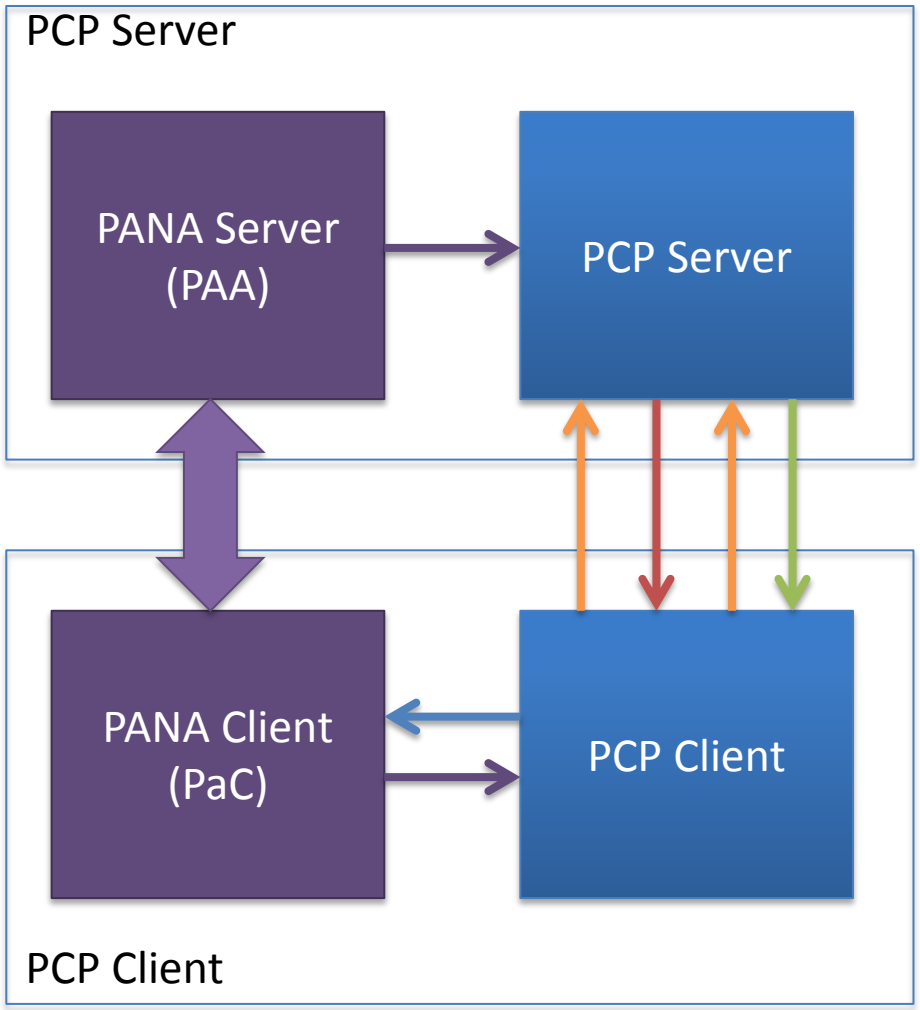
Separate vs. In-Band

- Separate approach uses a separate protocol (two separate sets of ports) for key management, and security credentials are passed from the key management client/server to the PCP client/server
  - Proposed mechanism uses PANA for key management
- In-band approach uses a single protocol (one set of ports) and the security exchange is an integral part of the PCP protocol
  - Proposed mechanism uses EAP for authentication
- Both approaches use the same PCP option to pass security credentials between the PCP Client and Server
- Both types of approaches have been used successfully in the past (e.g. TLS is in-band, IPsec and IKE are separate)
- In this case, both proposed mechanisms provide the same level and type of security (both ultimately based on EAP and same set of available EAP methods)

High-Level Points

- Both proposals are well-understood and will work
- Both proposals will provide the same level and type of security
  - Both are ultimately based on EAP and the same underlying EAP methods
- There are more similarities between these proposals than differences

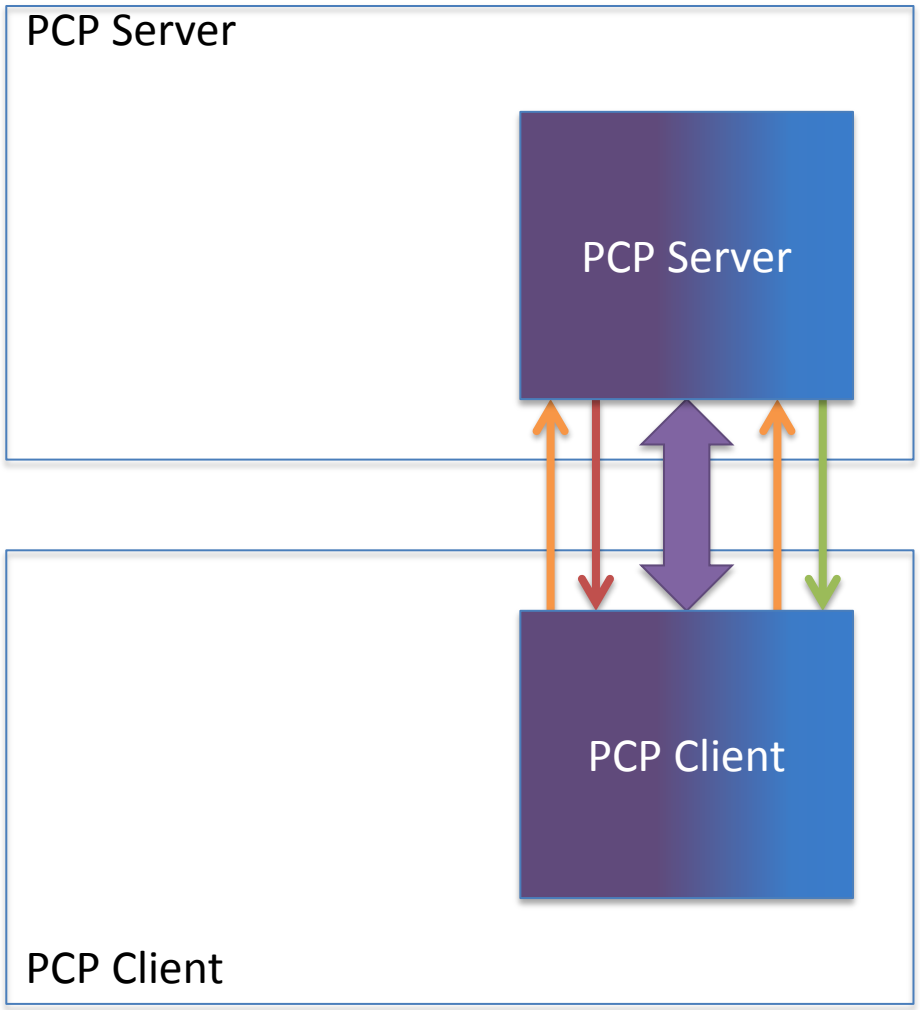
Separate Key Management



- PCP Client sends Request
- Error: AUTH REQUIRED
- PCP Client triggers PANA Client
- PANA Exchange (several msgs)
- PANA Client sends security association info to PCP Client
- PANA Server sends security association to PCP Server
- PCP Client sends Authenticated Request
- Success Response

(First two steps can be avoided, if Client is configured to use Authentication)

In-Band Management

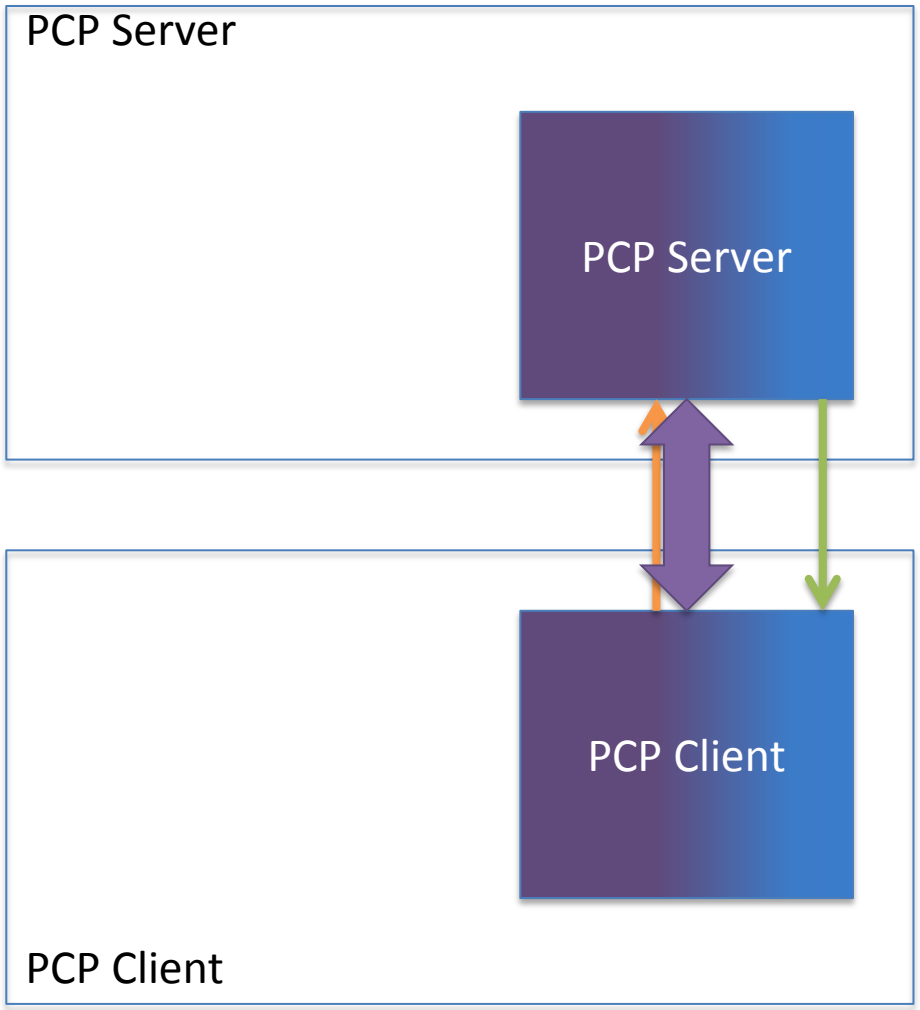


- PCP Client sends Request
- Error: AUTH REQUIRED
- Auth Exchange (several msgs)
- PCP Client sends Authenticated Request
- Success Response

(First two steps can be avoided, if Client is configured to use Authentication)

Additional PCP messages are used to transport EAP authentication instead of PANA messages

Possible In-Band Optimization



PCP Client sends Request with first step of Auth Exchange

Remainder of Auth Exchange (several msgs)

Success Response

Client can initiate authenticated session, and piggy-back first Step of Auth Exchange in the Request packet

Requires that client knows that Authentication is required for this request (or all requests).

Possible with in-band approach, not with separate approach.

Standardization/Specification Status

- Standardization Status
  - PANA has been a Proposed Standard since May 2008
- Specification Status
  - In-band approach is fully specified
  - PANA proposal requires further specification for PCP Authentication
    - Need to specify/describe interface between PANA and PCP elements
    - Need to specify how the PANA client finds the correct PANA Server for PCP Authentication (may be passed from PCP client?)

Running Code

- Multiple PANA implementations have existed for many years
  - Open source implementations are available, but would require modification for this purpose
  - PANA is not currently available in any major operating system distributions
- In-Band approach has not been implemented

Potential for Code Reuse

- Both approaches allow reuse of code for EAP and EAP methods across multiple EAP-based protocols
- If a system implements PANA for network access or other purposes, there is potential to reuse the PANA code in the separate approach

PCP-Specific Code Required

- Both approaches require implementation of PCP-specific security options
- In-band approach requires implementation of a PCP-specific security exchange
- Separate approach requires implementation of PCP Client/Server to PANA Client/Server communication (could be system-internal)

Operational Experience

- In-band approach uses one port (PCP)
- Separate approach uses two ports (PCP & PANA)
  - May introduce complexity for intermediate firewalls or other middleboxes
- Additional configuration/management complexity
  - Client needs to know what PANA Server to use, as well as what PCP Server to use
    - draft-ohba currently assumes PANA Server and PCP Server are co-located, so this would be a non-issue
  - If PANA is also used for Network Access or other purposes, the client system may need to express that it is using different PANA Servers for different purposes

Questions? Thoughts?

Any comments or discussion before we try to make a decision?

Decision Making Options

- We need to make a decision to move forward
  - We have two workable choices
  - They are similar in many ways
- Can we reach consensus on which approach to pursue?
  - In-Band Approach vs. Separate (PANA-based) Approach
- If not, can we reach consensus to let the majority to decide?