NEA Working Group IETF meeting

Nov 17, 2011

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda Review

0900 Administrivia
- Jabber & Minute scribes
- Agenda bashing

0905 WG Status

0910 NEA Reference Model

0915 Discuss and Resolve WGLC PT-TLS Comments

http://www.ietf.org/internet-drafts/draft-ietf-nea-pt-tls-01.txt

1000 Discuss and Resolve PT-EAP Issues

http://www.ietf.org/internet-drafts/draft-ietf-nea-pt-eap-00.txt

1100 Discuss next steps for NEA Asokan I-D

http://tools.ietf.org/id/draft-salowey-nea-asokan-00.txt

1115 Next Steps

1130 Adjourn

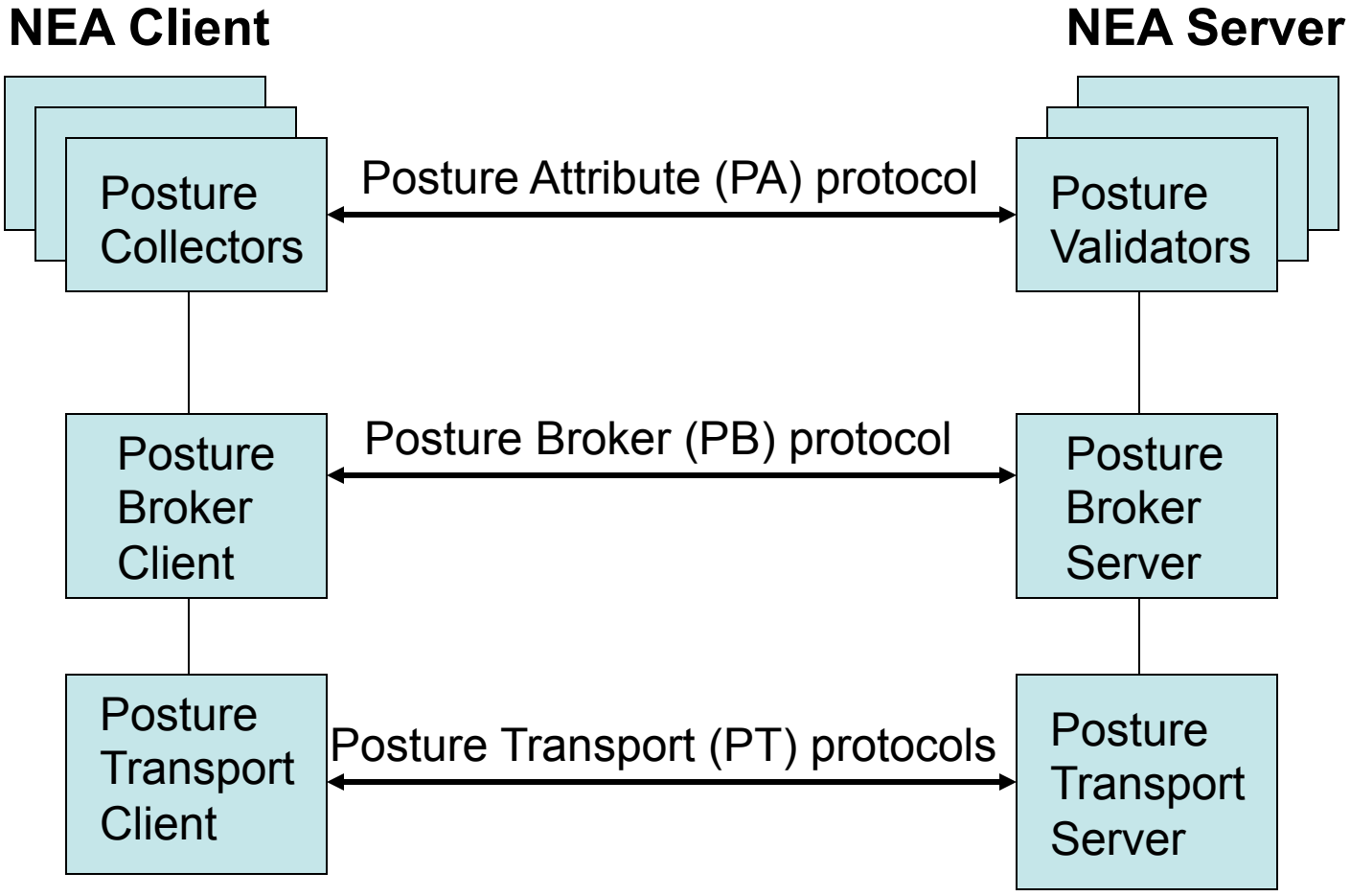
WG Status

- TLS-based Posture Transport
  - WGLC on PT-TLS -01 I-D
- EAP-based Posture Transport
  - PT-EAP selected as basis for WG document
  - PT-EAP published as -00 I-D

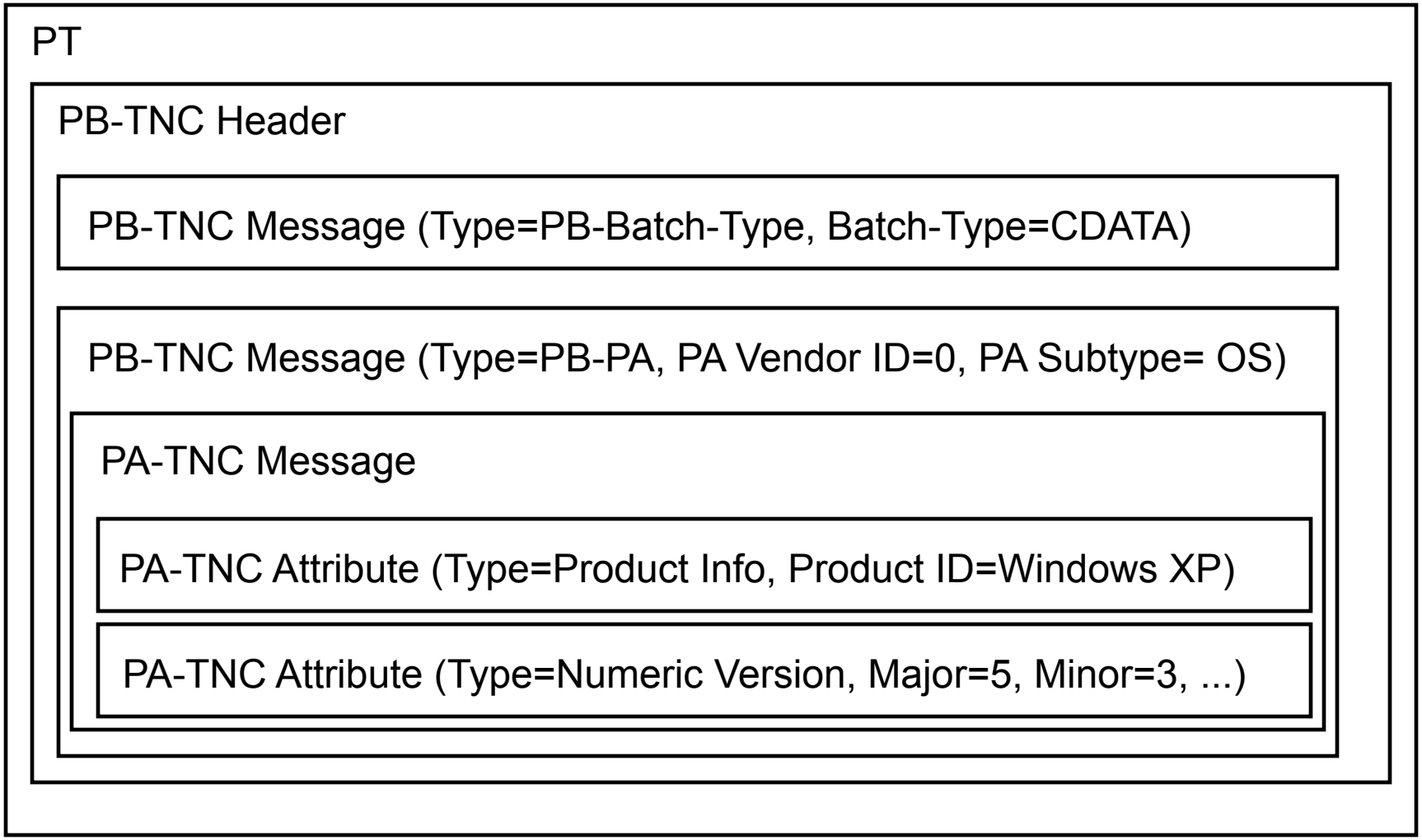
NEA Reference Model

NEA Reference Model

from RFC 5209



PA-TNC Within PB-TNC Within PT



PT-TLS WGLC Issues

Paul Sangster
Nancy Cam-Winget
Joseph Salowey

PT-TLS

- Working Group Last Call completed
  - Some open issues with proposed resolutions

TLS Keepalive

- TLS Heartbeat provides mechanism to keep TLS session up
  - draft-ietf-tls-dtls-heartbeat
  - Should be completed before PT-TLS
- Proposed Resolution: revise PT-TLS draft to include optional support for TLS heartbeat

Version Negotiation

“Subsequent assessments on the same session MUST use the negotiated version number and therefore SHOULD NOT send additional version negotiation messages.”

Proposed Resolution: Change SHOULD NOT to MUST NOT

SASL initiation

- Who initiates the SASL exchange? TLS client or server

- Proposed Resolution: Identify use cases to be supported and expected behavior. Update draft to ensure specified operation is unambiguous .

PT Client as TLS server

- If PT client is the TLS server, how does it authenticate the PT server?

- Proposed Resolution: Require TLS mutual authentication when PT client is acting as TLS server.

Channel Bindings

- Would be good to bind authentication to TLS tunnel when possible
  - SASL GS2 mechanism provides this capability
- Proposed Resolution: Add text describing usage of Channel Bindings between TLS and SASL

PT-EAP Issues

Nancy Cam-Winget
Paul Sangster

Status

- draft-ietf-nea-pt-eap-00 submitted on Aug 30, 2011
- A few comments posted by one of the editors
- Need more reviews!

Received Comment Summary

- Minimize acronyms, use PT-EAP for all instances of EAP-TNC and PT-TNC
  - Comments include proposed updates to achieve this throughout the draft
- New EAP method: NEA has defined new behavior
- *Section 1.1 remove TNC reference (e.g. the last sentence of the paragraph)*

Use PT-EAP only

Comment: PT-EAP defines the standalone method for carrying NEA data and specifies its bounds and usage to an EAP tunnel method. As such, I recommend that the draft stick to naming this method PT-EAP (vs. The use of both PT-EAP, EAP-TNC, and PT-TNC)

Proposal: Update draft to use PT-EAP only

Abstract simplification

- Update the abstract to:

  This document specifies PT-EAP, an EAP based Posture Transport (PT) protocol designed to be used only inside an EAP tunnel method. As such, the document also describes the intended applicability of PT-EAP as well as the evaluation against the requirements defined in the NEA Requirements and PB-TNC specifications.

Proposal: Update draft as suggested above

Introduction simplification

- Update 1st sentence of Introduction to:

  This document specifies PT-EAP, an EAP based Posture Transport (PT) protocol protected by a TLS based tunnel established by an EAP tunnel method.

Proposal: Update but with Steve's suggestion to:

This document specifies PT-EAP, an EAP based Posture Transport (PT) protocol protected by an outer TLS tunnel or equivalent protection.

Introduction simplification

- Update 2nd paragraph of Introduction to:

  The PT protocol in the NEA architecture is responsible for transporting PB-TNC batches (often containing PA-TNC [3] attributes) across the network between the NEA Client and NEA Server. The PT protocol must be protected by an outer TLS-based tunnel to ensure the exchanged messages are protected from a variety of threats from hostile intermediaries.

Proposal: adopt changes in next draft

Introduction simplification

- To be consistent with a single reference of the inner method, my suggestion is to remove the 5th and 6th paragraph and replace the entire 4th paragraph with:

  PT-EAP is an inner EAP method designed to be used under a protected tunnel such as EAP-FAST and EAP-TTLS.

Proposal: adopt changes in next draft

Remove TNC reference

- *Section 1.1 remove TNC reference (e.g. the last sentence of the paragraph)*

Proposal: adopt change in next draft. If TNC needs to be noted, include in the acknowledgement “N.B. The Trusted Computing Group will also be referencing the protocol as defined in this document at the time of completion.”

Clarification on 3.1

- Section 3.1: 4th paragraph, 2nd sentence seems to be a non sequitur, suggest to remove it (e.g. the sentence reading:

  ”Some EAP tunnel methods may provide explicit confirmation of inner method success; others may not. This is out of scope for the EAP-TNC method.”)

Proposal: can discuss on the list to either clarify the sentence/paragraph or adopt above update

New EAP method

- *Section 3.4: as NEA has changed the behavior of the method, it merits its own type and thus should be a TBD.*

Proposal: update in the next draft

Enforce use of EAP tunnel

- Section 4: language to enforce use within protected tunnel should be used, suggest wording to: *“is designed and MUST run inside an EAP tunnel method”*

Proposal: adopt change in the next draft

Questions?

Disposition of NEA Asokan I-D

Disposition of NEA Asokan I-D

- I-D provides analysis and recommendations for dealing with NEA Asokan attack
- Referenced by PT-TLS and PT-EAP I-Ds (Informative)
- Consensus to make WG document with goal to publish as Informational RFC?

Next Steps

- PT-TLS:
  - Update PT-TLS I-D after resolving WGLC issues
  - Issue 2nd WGLC
- PT-EAP:
  - More WG Comments Please!
  - Update PT-EAP I-D and issue WGLC
- NEA Asokan I-D:
  - Publish updated version as WG document

Milestones

Nov 2011	Resolve issues from PT-TLS WGLC at IETF 82
	Resolve open issues with PT-EAP at IETF 82
Dec 2011	Publish -02 PT-TLS I-D and issue 2nd WGLC
	Publish -01 PT-EAP I-D and issue WGLC
	Publish -00 WG I-D on NEA Asokan attack
Jan 2012	Send PT-TLS I-D to IESG
	Resolve WGLC issues on PT-EAP
	Resolve issues with NEA Asokan I-D
Feb 2012	Publish -02 PT-EAP I-D
	Publish -01 NEA Asokan I-D and issue WGLC
Mar 2012	Resolve IETF LC issues with PT-TLS I-D
	Resolve WGLC issues with PT-EAP and Asokan I-D

Adjourn