NEA Working Group
IETF 83
March 28, 2012

nea[-request]@ietf.org

http://tools.ietf.org/wg/nea

Co-chairs: Steve Hanna shanna@juniper.net

Susan Thomson sethomso@cisco.com

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

1300 Administrivia
Jabber & Minute scribes
Agenda bashing

1305 WG Status

1310 NEA Reference Model

1315 Discuss and Resolve WGLC PT-TLS Comments

http://www.ietf.org/internet-drafts/draft-ietf-nea-pt-tls-02.txt

1350 Discuss and Resolve WGLC PT-EAP Issues

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

1425 Discuss next steps for NEA Asokan I-D

http://tools.ietf.org/id/draft-salowey-nea-asokan-01.txt

1450 Next Steps

1500 Adjourn

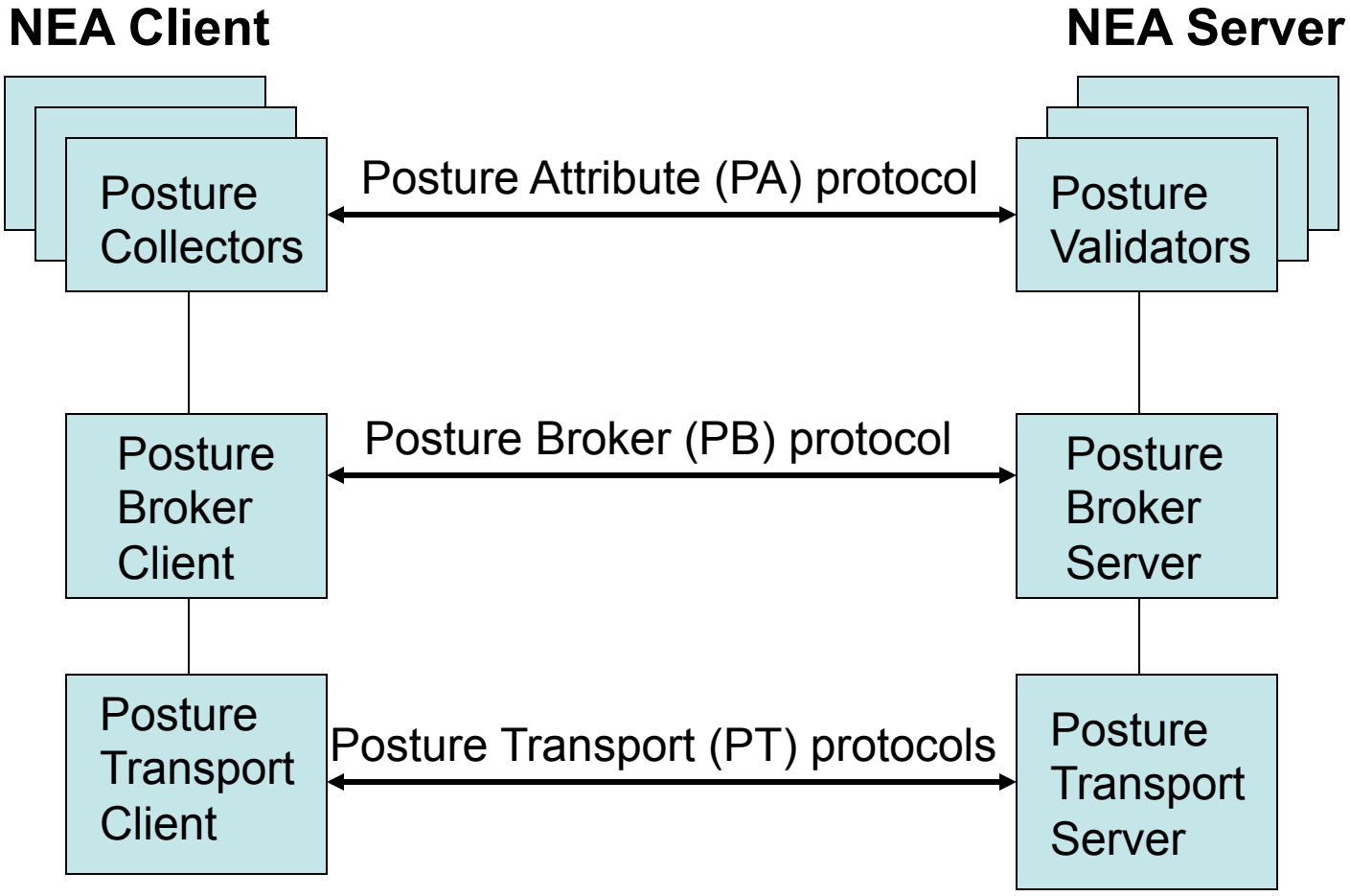
WG Status

- PT-TLS
  - Integrated Comments into PT-TLS -02 I-D
  - Ran Second WGLC
- PT-EAP
  - Integrated Comments into PT-EAP -01 I-D
  - Ran First WGLC
- NEA Asokan Attack
  - Decided to Not Generalize
  - Published NEA Asokan -01 I-D

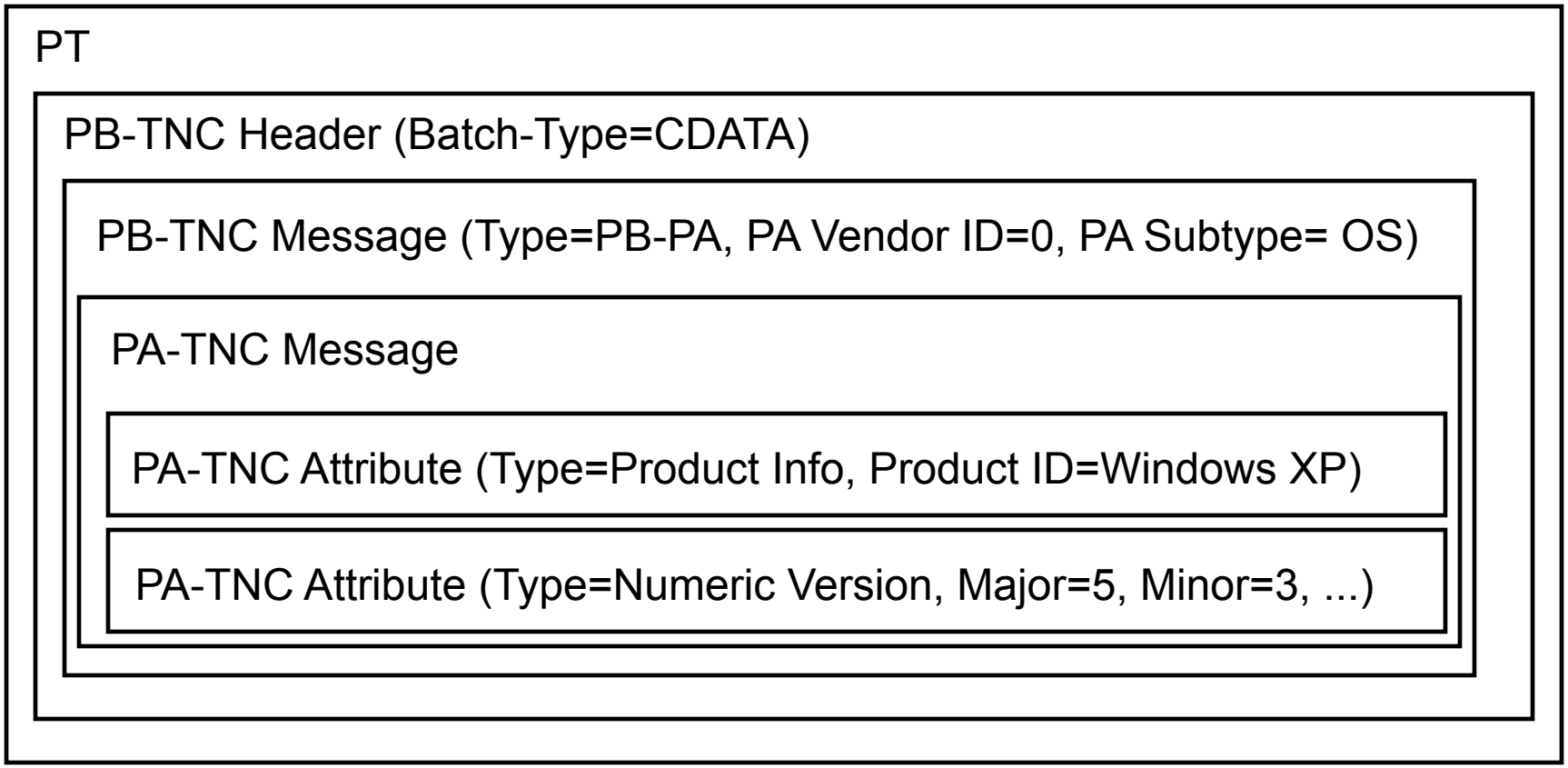
NEA Reference Model

NEA Reference Model

from RFC 5209



PA-TNC Within PB-TNC Within PT



Use Cases for PT-EAP

- NEA Assessment on 802.1X Network
  - Consider posture in network access decision
  - Isolate vulnerable endpoints during remediation
  - Block or quarantine infected endpoints

- NEA Assessment during IKEv2 Handshake
  - Assess posture before granting network access
  - Isolate vulnerable endpoints during remediation
  - Block or quarantine infected endpoints

Use Cases for PT-TLS

- NEA Assessment on Non-802.1X Network
  - Legacy Network
  - Remote Access
- Large Amount of Data in NEA Assessment
  - For example, Installed Packages
  - Unsuitable for EAP Transport
- Posture Re-assessment or Monitoring After 802.1X Assessment
- Application Server Needs to Perform NEA Assessment

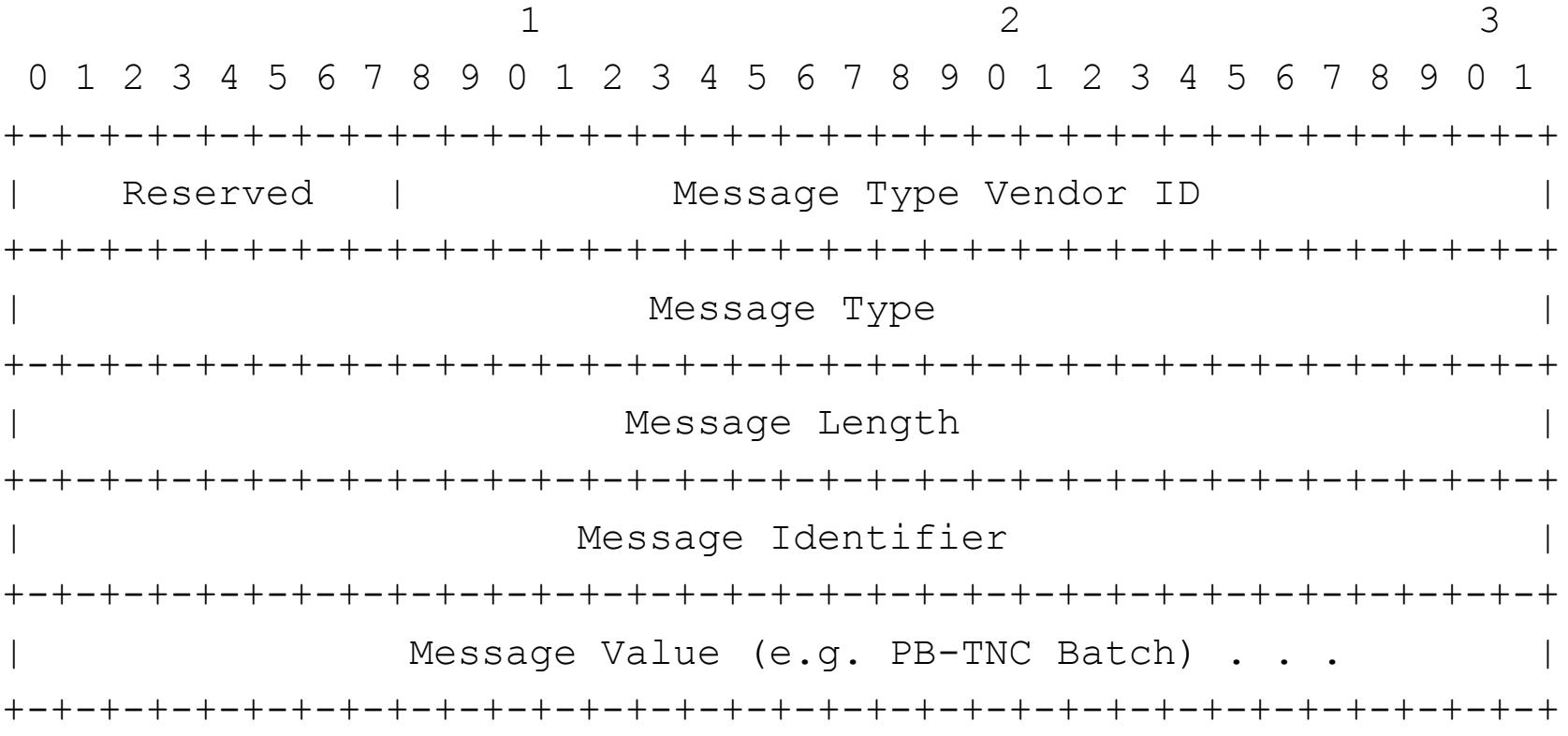
PT-TLS Update

Paul Sangster

Agenda

- PT-TLS Overview
- Summarize Changes in -02
  - NEA Server starts all SASL auths
  - Clarifications
  - Typos
- WGLC Comments
- Questions

PT-TLS Message Format



- Format matches PB-TNC Message header (plus Message Identifier)

Three Phases of PT-TLS

1. TLS Setup
   - Unmodified (includes TLS handshake)

2. PT-TLS Negotiation
   - Version negotiation
   - Optional SASL authentication of NEA Client

3. PT-TLS Data Transport
   - NEA assessments

SASL Client Authentication

- Four SASL oriented messages
  - SASL Mechanisms
  - SASL Mechanism Selection
  - SASL Authentication Data
  - SASL Result
- MUST support SASL mechanisms
  - PLAIN and EXTERNAL
- One mechanism at a time (multiple allowed)

PT-TLS -02 Changes

NEA Server Starts SASL

- NEA Server policy defines when client authentication required
- Removed ‘Request SASL Mechanisms’ client initiation message
- NEA Server initiates SASL using ‘SASL Mechanisms’ message
  - Empty SASL Mechanisms means no (further) client authentication required
- Removed race condition text (no more client initiation)

Clarifications

- Section 3.1.1 Server Initiated PT-TLS
  - NEA Client acts as TLS Server so uses X. 509 certificate
  - Client and Server perform path validation as per RFC 5280
  - SHOULD support TLS heartbeat (RFC 6520)
- Section 3.4.2 PT-TLS Phases
  - TLS session renegotiation only allowed during TLS Setup phase (not later)

Clarifications

- Section 3.4.2.1 TLS Setup Phase
  - NEA Client performs server certificate validation as per RFC 5280 and recommendations from RFC 6125
- Section 3.7 PT-TLS Version Negotiation
  - MUST NOT renegotiate PT-TLS protocol version after successful completion

WGLC Comments

- “Introduction: Same as with PT-EAP: it is mentioned that there is another PT protocol. Maybe it makes sense to reference PT-EAP?”

➢ Agreed, we will a mention of PT-EAP specifically in the introduction

WGLC Comments

- Section 3.5 PT-TLS Message Format

This field contains a value that uniquely identifies the PT-TLS message on a per message sender (Posture Transport Client or Server) basis. This value can be copied into the body of a response message to indicate which message was received and caused the response. For example, this field is included in the PT-TLS Error Message so the recipient can determine which message sent caused the error.

Make this a SHOULD?

WGLC Comments

- Section 3.5 PT-TLS Message Format

Change to:

“Message Identifier
This field contains a value that uniquely identifies the PT-TLS message on a per message sender (Posture Transport Client or Server) basis. This value is copied into the body of the PT-TLS Error Message, so the recipient can determine which message caused the error.”

AND

Section 3.9 Error Message

Copy of Original Message
This variable length value MUST contain a copy (up to 1024 bytes) of the original PT-TLS message that caused the error.

WGLC Comments

- Section 3.6 IETF Standard Message Types

3 (SASL Mechanisms)
Sent by the NEA Server to indicate what SASL mechanisms it is willing to use for authentication on this session. The NEA Client MUST send an Invalid Message error code in a PT-TLS Error message if a SASL Mechanisms message is received at another time.

Change to:

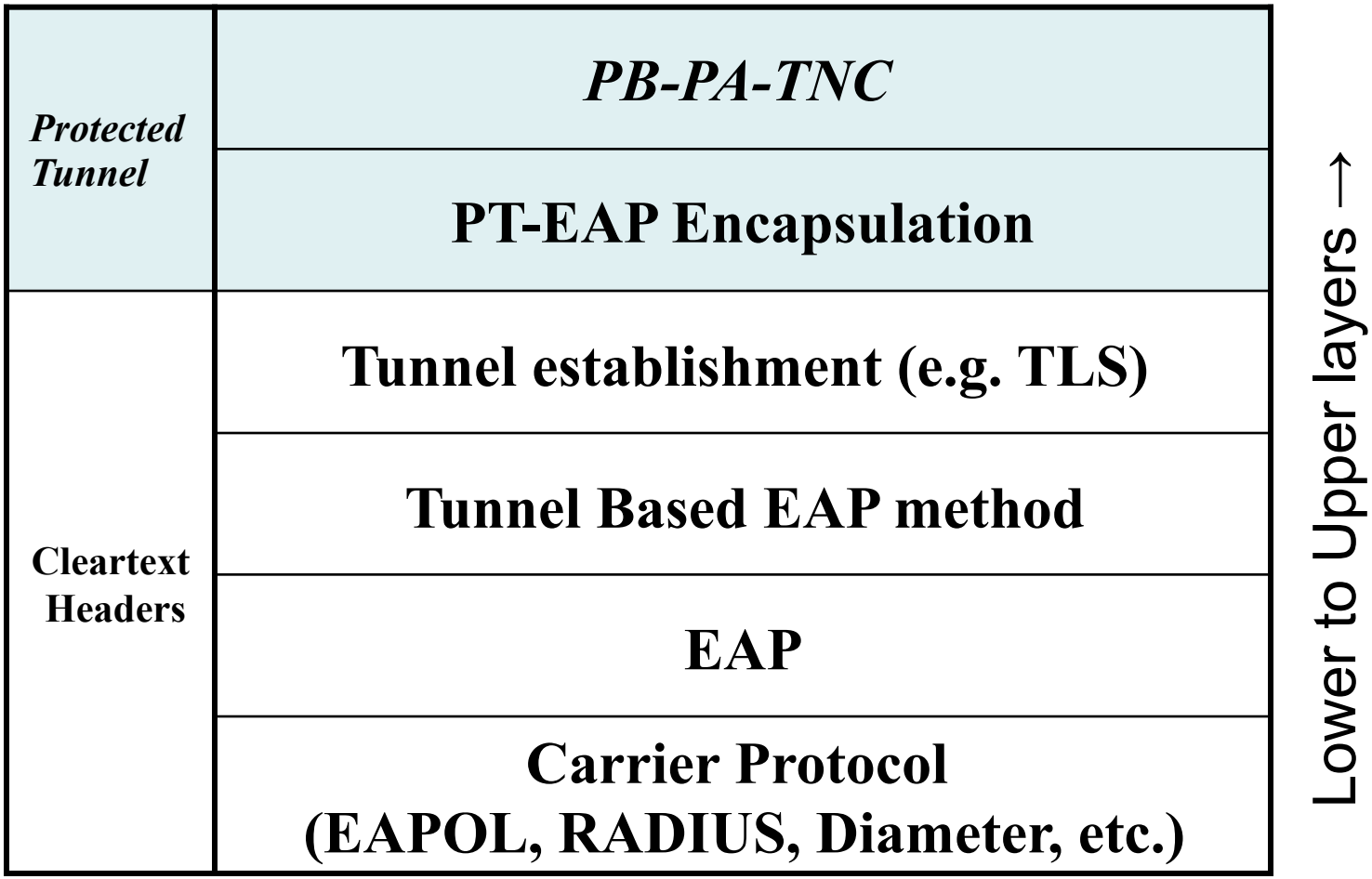
Sent by the NEA Server to indicate what SASL mechanisms it is willing to use for authentication on this session. This message type MUST only be sent by the NEA Server during the PT-TLS Negotiation phase. The NEA Client MUST send an Invalid Message error code in a PT-TLS Error message if a SASL Mechanisms message is received at another time.

Questions?

PT-EAP Update

Nancy Cam-Winget

EAP Tunnel Protocol Layers



PT-EAP Message Format

* Only when using fragmentation

Status

- draft-ietf-nea-pt-eap-01 submitted on March 2012
- Comments addressed

Remaining Issues

- Move EAP Tunnel requirements to “Security Requirements” vs. Security considerations
  - *In section 4.2.1, RFC2119 terms are used, this means they are requirements. Is that the case? If so, you may want to have a Security Requirements section prior to your Security Considerations Section and include items like these. It is starting to become a trend in drafts so that security requirements are not ignored by developers. This particular statement is high-level, so you may want to change it to use language not defined in RFC2119, but clearly point to the specification that provides the details of how the authentication and other security features are provided in the introduction.*
  - *Section 4.2.5 and 4.3 also contains an RFC2119 term. This is fine, just point it out as you decide how to handle considerations versus requirements with the current introductory remarks.*

Remaining Issues

- Kathleen suggests that we need explicit references for authentication options in 4.3
  - *Section 4.3: I think you need to be more specific and provide references to the acceptable authentication options to have interoperability between implementations.*

Comments on -01 by Steve Hanna

Comment	Proposed Update
Various editorial nits	Can be addressed by editor
There's no need for the L bit or the Data Length field since we have removed fragmentation. The recipient of a PT-EAP message can determine the length of that message by just looking at the EAP Length field.	Can remove both L bit and Data length fields.
In the last sentence on page 8, "match endpoint" should be "match and this is confirmed by the EMA". In order to prevent a NEA Asokan attack, the server needs to confirm that the EMA has the same tls-unique value. Another way to clarify this would be to change the words "NEA Client" where they first appear in that sentence to "EMA".	Can be addressed by editor

Comments on -01 by Steve Hanna

Comment	Proposed Update
In section 4.2.2, I think that "Similarly" should be "Therefore". This better explains the causality between hiding the PT-EAP method and increasing the difficulty for a passive MITM to tamper with the method. However, this argument is fairly weak since the PT-EAP method might always occur at the same offset in the exchange. Probably it would be better to just remove the last two sentences in this paragraph lest they give a false understanding of the protections that prevent a MITM from inserting falsified messages without detection. Those protections reside primarily in integrity protection and authentication not in encryption.	Can be addressed by editor
In section 4.5, the claim for Fragmentation should be "No" since that has been removed from this draft.	Can be addressed by editor

Comments on -01 by Carolin Latze

Comment	Proposed Update
Aseveral formatting and editorial nits provided	To be addressed by editor
Section 3.4: In the sections before, you said PT-EAP could run over a TLS-based tunnel or one with comparable features. However, the channel bindings solution is only for TLS, right? So maybe, we need another sentence there, mentioning how to do this for other tunnel methods	Can be addressed by editor: consensus needed as to whether to enforce EAP tunnel only or allow other tunnel mechanisms?

-01 Received Comments + Resolutions

Comments

Originator	Comment	Update
Nancy Cam-Winget	Minimize acronyms: use PT-EAP vs. PT-TNC/EAP-TNC	Update references and Abstract, introduction, “Trust relationships”, IANA Considerations
Nancy Cam-Winget	New EAP method	EAP type is now TBD
Stephen Farrell	Remove Appendix (requirements) as they are no longer needed	Done.
Susan Thomson	Fragmentation unnecessary	Removed section 3.3
Nancy Cam-Winget	Remove TCG reference	Include new TCG section for reference
Joe Salowey/Stefan Winter	Enforce the need for a protected tunnel	Update text to allow EAP tunnel preference but not rule out others

Comments by Carolin Latze

Comment	Response/Resolution
Section 3.2- "The NEA Client SHOULD choose the value sent by the NEA …" -> does this mean, the client is allowed to choose an older version even he supports the same version like the server. Wouldn't it be better to require the client to use the version the server requested if he supports it and only allow to use older versions if the client does not support the server's version?	That is the intent as the subsequent sentence parenthetically states that the client MAY only support a lesser version. If the client includes a lower version, it is up to the NEA Server's policy to then determine whether to accept a lesser version (as stated in the subsequent paragraph).
Section 4.2.1 2n paragraph: "In order to protect again NEA assessment message theft" -> against	Fixed.
Section 4.3 5th paragraph: "Whether the communication channel is established …." -> ok this can be my bad English, but I thought it is bound to at least the authentication of the NEA _server_, not the client since most of the tunnel protocols authenticate the server only. Did I just misunderstand this paragraph?	Yes, that is true so the paragraph has been updated to reflect this.
Section 4.4 4th paragraph: "Each of these methods employs at least a NEA Server authentication using an X.509 certificates" -> certificate (= only one)	Fixed.

Comments by Kathleen Moriarty

Comment	Response/Resolution
Section 3.1, could you include a diagram? I think that will help the reader to see the flow on first read. The text reads well, but not being familiar with the draft, I had to read it twice to make sure I had the background to continue reading. It would be useful to reference while reading section 3.2 as well.	Not sure what diagram is requested….a packet flow diagram? Given that we've now simplified the draft to just define PT-EAP, is the text now sufficient?
Section 3.3: Just a suggestion to reword the first paragraph:In most cases, EAP-TNC fragmentation will not be required. However, PB-TNC batches can be very long and EAP message length is sometimes tightly constrained. As a result, EAP-TNC includes a fragmentation mechanism to be used when a particular PB-TNC batch is too long to fit into a single EAP-TNC message.	Fragmentation has been removed by this draft as the EAP-Tunnel methods already define how to support fragmentation.
Section 3.3: Is there a reference that can be included to where one can find the 'variety of reasons' in the last paragraph?" However, a NEA Server or peer still MAY decide to terminate an EAP-TNC exchange at any time for a variety of reasons."	Fragmentation has been removed by this draft as the EAP-Tunnel methods already define how to support fragmentation.

Comments by Kathleen cont'd

Comments	Response/Resolution
Section 3.4: Type, I had the word please in a draft :) and someone recommended pulling it out and just directly making the request. You may want to do the same here.	IANA note has been removed.
Section 3.4 Data Length: Recommend adding a comma in the first sentence and removing two in the second: Data Length is an optional field, four octets in length. When present, it indicates the total length before fragmentation of a fragmented PB-TNC batch.	The text has been updated to reflect its new use given that fragmentation is no longer in PT-EAP
Section 3.5: Should 'SHOULD' be 'MUST' in the following sentence to protect against the attack? If this is not required of the protocol, then I suggest using non RFC2119 language, something like the following: To protect against NEA Asokan attacks, it is necessary for the Posture Broker on an EMA-equipped endpoint to pass the tls-unique channel binding [18] for PT-EAP's tunnel method to the EMA.	Updated as suggested.

Comments by Kathleen cont'd

Comments	Response/Resolution
Section 3.3: Is there a reference that can be included to where one can find the 'variety of reasons' in the last paragraph?"However, a NEA Server or peer still MAY decide to terminate an EAP-TNC exchange at any time for a variety of reasons."	There is no good reference, but the offending text is obviated by the removal of fragmentation.
I think the following sentence should be broken into two as follows (left in the page information so you can find it):This value can then be in the EMA's attestation and the Posture Validator responsible for communicating with the EMA. The EMA may then confirm that the value matches the tls-unique channel binding for its end of the tunnel.	Updated it to reflect intent: the tls-unique is included in the EMA's attestation so that the Posture Validator can check it.
Can you reword the following sentence (next one in this section)? It is a little tough for me to follow: "If the values match and the integrity of the endpoint is good, the posture sent by the EMA and NEA Client is from the same endpoint as the client side of the TLS connection (since the endpoint knows the tls- unique value) so no man-in-the-middle is forwarding posture."	Reworded to: *If the tls-unique values between the NEA Client and NEA Server match endpoint, then the posture sent by the EMA (and thus the NEA Client) is from the same endpoint as the client side of the TLS connection (since the endpoint knows the tls-unique value) so no man-in-the-middle is forwarding posture.*

Comments by Kathleen cont'd

Comments	Response/Resolution
Security Considerations: Could you reference the documents where the security requirements exist. I like that the introduction to this section clearly states that these are recommendations and not the requirements, but want to be sure the requirements are directly referenced.	RFC5209 has been included.
In section 4.2.1, RFC2119 terms are used, this means they are requirements. Is that the case? If so, you may want to have a Security Requirements section prior to your Security Considerations Section and include items like these. It is starting to become a trend in drafts so that security requirements are not ignored by developers. This particular statement is high-level, so you may want to change it to use language not defined in RFC2119, but clearly point to the specification that provides the details of how the authentication and other security features are provided in the introduction.	Open for discussion

Comments by Kathleen cont'd

Comments	Response/Resolution
Section 4.2.2, Consider breaking the last sentence into multiple sentences.	Presume it's the last sentence of last paragraph. This has now been split into 2 sentences.
Section 4.2.5 and 4.3 also contains an RFC2119 term. This is fine, just point it out as you decide how to handle considerations versus requirements with the current introductory remarks.	Open for discussion
Section 4.3: I think you need to be more specific and provide references to the acceptable authentication options to have interoperability between implementations.	Open for discussion
Section 4.4: I like seeing the reference to TLS, can you also include the references to EAP-FAST and EAP-TLS here so the reader has links to the RFCs when the document is published? It could help them figure out things like the necessary version of TLS to support, etc…	Done.

Comments by Kathleen cont'd

Comments	Response/Resolution
Section 4.4: Last paragraph, this goes into authentication, but doesn't provide a reference to the appropriate specs to follow either.	Updated 1st sentence of paragraph to include FAST and TTLS with references.
Section 4.5: It may only be me, but I had to read the introductory sentence a couple of times to get the context - to make sure I had it right. Can you add 'for this specification' or something like that to the sentence?	Done.
Section 6: I think you can make a direct statement requesting registration of the value. This text will live on in the document after the value is assigned. Maybe ask IANA, but in the draft make it more direct - Registers value 38…	It's actually TBD now and must be assigned by IANA; do text has been updated to reflect this.
Section 6.1 looks good - I just finished similar IANA requests.	Thanks!

Questions?

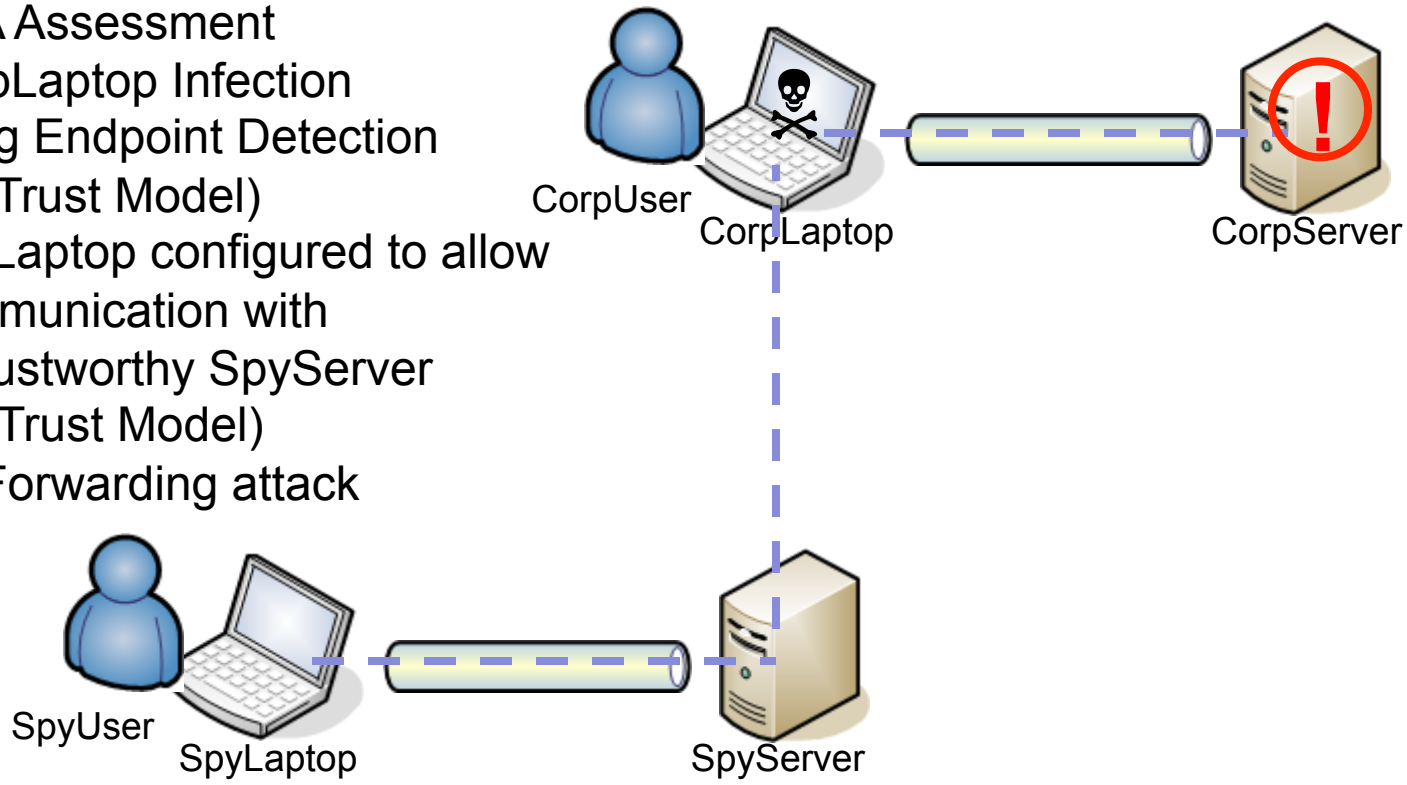
NEA Asokan Attack Analysis

Joe Salowey

Asokan Attack on NEA

Preconditions

1. NEA Assessment
2. CorpLaptop Infection
3. Lying Endpoint Detection (PA Trust Model)
4. SpyLaptop configured to allow communication with untrustworthy SpyServer (PT Trust Model)
5. PA Forwarding attack



External Measurement Agent

- The “Asokan Attack” is most significant when there is an independent entity that can collect and authenticate the assessments
- The draft refers to this entity as an “external measurement agent” or EMA
- If the tunnel and EMA authentication are not bound together then the system is vulnerable to the “Asokan Attack”

TLS-Unique Channel Binding

- Uses tls-unique Channel Binding defined in RFC 5929 to bind into EMA exchange
  - tls-unique is the contents of the first Finished message
  - Finished(PRF(master_secret, “client_finished”, hash(M1 || M2 || M3a || M3b)))
- Binds to a particular TLS connection
- Can be used with any cipher suite

Changes from -00 to -01

- Updated References to Transports
- Reflect decision to use ‘tls-unique’ channel binding

Next Steps

- Post Revision as Working Group Draft
- WGLC
- Send to IESG for Informational Status

NEA WG Next Steps

Next Steps

- PT-TLS
  - Update PT-TLS I-D to reflect WGLC comments
  - Send to IESG for Standards Track

- PT-EAP
  - Update PT-EAP I-D
  - Send to EMU WG for review, handle any comments
  - 2nd WGLC if needed
  - Send to IESG for Standards Track

- NEA Asokan Attack Analysis
  - Publish updated version as WG document
  - WGLC
  - Send to IESG for Informational

Milestones

Apr 2012	Publish -03 PT-TLS I-D
	Send PT-TLS to IESG for Standards Track
	Publish -02 PT-EAP I-D
	Send PT-EAP to EMU WG for Review
	Publish -00 WG I-D on NEA Asokan Attack
	WGLC on NEA Asokan Attack
May 2012	If Needed, Publish -03 PT-EAP I-D and 2nd WGLC
	Send PT-EAP to IESG for Standards Track
	Publish -01 WG I-D on NEA Asokan Attack
	Send NEA Asokan Attack Analysis to IESG for Info'l

… Wait for Feedback from IETF LC and IESG …

… Probably No Need for WG Meeting at IETF 84 or Beyond …

Adjourn