Public Comments on NIST Draft Special Publication 800-120

NIST received the following public comments on the draft Special Publication 800-120, "*Recommendation for EAP Methods Used in Wireless Network Access Authentication (December 2008)*".

The comments are ordered based on the dates they were received. Most comments were received in e-mail format. The line-breaks are deleted when copied to this file. The e-mail headers are removed to protect commenter's privacy. For the same reason, e-mail addresses, postal mailing addresses, and telephone numbers are also removed from the signatures.

Bernard Aboba

Overall Comments

Document Scope

The recommendations made in this document would appear to apply to wired as well as wireless Network Access Authentication. For example, IEEE 802.1X-REV is now considering wired authentication scenarios where data traffic could be accessed by an attacker. Therefore, it may be worth considering whether the scope of the document needs to be further clarified. For example, the document refers to applicability to "broadcast Ethernets".

In terms of applicability to IEEE 802.16, the scope may need to be clarified. The use of EAP with public IEEE 802.16 networks is defined by the WiMAX Forum (WMF). This includes requirements for EAP methods and key management, certificate profiles, and the architecture for international roaming. The use of a public WiMAX network is therefore somewhat different from the use of a private federal IEEE 802.16 network.

If the desire is to cover use of public WiMAX networks, then some updates may be needed. For example, the document might want to refer to the WMF specifications. Also, the statements made in Section 1 about the diversity of EAP methods do not necessarily apply to WiMAX, where EAP method use is highly restricted, since the methods may be implemented in firmware, and EAP authentication is required to terminate on a carrier AAA server due to the design of the certificate hierarchy. Thus, it is not clear that authentication could terminate on a federal AAA server which could then choose an EAP method as indicated in this document.

Key Management implications

Requirement SR-KE-7 may have implications beyond EAP method requirements, since EAP lower layers such as IEEE 802.16 derive session keys purely based on contributions from the authenticator.

Protocol Coverage

The document cites obsolete documentation for PEAP, and does not provide compliance checks for it. Given the prevalence of PEAP deployments, this might be worth addressing.

Ciphersuite support

As noted in RFC 5246 Section 9, TLS versions provide for mandatory-to-implement ciphersuites in the absence of application recommendations. This should be taken into account within the discussion of ciphersuite support within various TLS-based EAP methods.

Specific Comments

Section 1, page 8

IEEE 802.16 [3] does not support EAP. IEEE 802.16e-2005, while utilizing EAP, is not based on IEEE 802.1X or EAPoL. This was not possible since in IEEE 802.16e authentication occurs before data frames of any type can be transmitted.

IEEE 802.11i has been superceded by IEEE 802.11-2007, so you should refer to IEEE 802.11 and update reference [2] to refer to the latest version of the standard.

"wired broadcast Ethernets" should probably be replaced by "Shared media Ethernet".

Section 2

This section refers only to IEEE and IETF standards. The standards for EAP authentication within public IEEE 802.16 networks are defined by the WiMAX Forum.

So if the scope of this document includes public IEEE 802.16 networks, I would suggest that the WMF be added to the list of relevant SDOs.

Section 3

The definition of Transient EAP Key differs significantly from the one in RFC 5247. Note that the RFC 5247 definition does not require the TEKs to be derived from the master key, and that not all EAP methods have a readily identifiable master key.

Section 4.1

"Since the authenticator only acts as a pass-through device, no security requirements for authenticators are necessary and it is of no importance whether the authenticator is a federal or non-federal device."

This sentence could be rewritten to make the intent more clear. I believe that this sentence means to say that from the point of view of EAP method requirements, the authenticator is not important, not that authenticator security is unimportant in general. After all, authenticators still need to go through CMVP, and RFC 5247 Sections 2.3.1, 5.1, etc. emphasize the importance of authenticator security to the overall security of the system.

Section 4.2

"EAP consists of four different message types: request, response, success, and failure."

You might say "EAP as defined in RFC 3748 consists of..." since new message types have subsequently been defined in RFC 5296.

Figure 2 displays an EAP exchange in which the Type Code changes during execution. Some explanatory text should probably be included on page 18, since aside from use of EAP Notification, or EAP Identity, such a Type Code change is not permitted within the RFC 4137 state machine.

Section 4.4

"Inner authentication methods can be EAP methods or other authentication schemes encapsulated in EAP methods."

Some tunnel methods (such as EAP-TTLSv0) include native support for authentication schemes. These "native" authentication schemes do not involve encapsulation of EAP within the tunnel. It isn't clear whether the above text includes that possibility.

"Tunnel-based EAP methods were introduced for two reasons: first, and most importantly, tunnel-based EAP methods enable the use of legacy authentication methods for peers. Without tunneling, widely deployed but weak authentication methods (such as password

authentication) are insecure."

This sentence could be more clear. Does the term "legacy" refer to methods defined in RFC 3748, such as EAP GTC, OTP and MD5? It is not clear what the term "password authentication" is referring to here. Cleartext passwords are not supported within EAP, although challenge-response schemes (such as EAP-MD5) are.

"Secondly, tunnel-based EAP methods can enable privacy protection, because peer and, optionally, server identifiers can be exclusively exchanged in the tunnel and, thus, prevent an eavesdropper from identifying these entities."

Later on (Section 11.4) server identification is required, and so the term "privacy" only applies to peer identifies.

Server identities need to be exchanged within TLS, and so this cannot occur "in the tunnel" unless an anonymous exchange were to be done to establish the tunnel, which is prohibited elsewhere in the document.

"Note that the feature of executing several authentication methods within a protective tunnel can be useful if several layers of peer authentication are necessary, e.g. first authenticating the peer device, then authenticating the user operating the device."

Executing several authentication methods within a tunnel is not the only way to provide authentication for multiple credentials sets (e.g. user + machine). Such a scenario can also be handled via mutual authentication within TLS (e.g. peer machine certificate) plus an inner authentication (for authentication of peer user credentials).

Section 5.1

"Traffic analysis can be used to track mobile users, e.g. by correlating all EAP executions carrying the same peer identifier."

Since EAP privacy could address the "peer identifier" issue, you might want to point that out. Alternatively you might refer to correlation of a lower layer identifier (e.g. IEEE 802 MAC address), which cannot be addressed by an EAP method.

Section 5.2

It might be worth mentioning that the EAP method negotiation is unprotected, so that this negotiation is also vulnerable to attack. Presumably the recommendations made in this document can be used to restrict the methods that can be negotiated to those that have desirable security properties. This does not prevent a bidding down attack, though it does prevent negotiation of an insecure EAP method.

Section 5.3

"For example, commercial mobile wireless applications that provide wireless Internet access or International roaming make impersonating a legitimate subscriber or stealing service through attacking EAP more attractive to outsider attackers."

The international roaming issue is an important one, which I think needs to be brought up earlier. In particular, I don't think that this document will address security concerns in international roaming scenarios such as might occur with WiMAX.

Section 5.4

"The adversary uses a weak proprietary authentication mechanism (e.g. a password-based mechanism) and replays the peer's responses as its own responses to the authentication server through the tunnel. Hence, the adversary can successfully impersonate the peer to the authentication server."

The man-in-the-middle attack does not depend on use of a week inner authentication mechanism. It only depends on support for the use of a method both within the tunnel and outside it. For example, even a method such as EAP-TLS could be the successful object of a man-in-the-middle attack were it to be tunneled within EAP-FAST or EAP-TTLSv0 without cryptographic binding, as long as EAP-TLS was also permitted outside the tunnel.

Section 5.5

As pointed out in Section 4.1, where the authenticator operates in pass-through mode, authenticator security issues do not affect the EAP method requirements, while obviously they do affect the security of the system as a whole. This point might be better clarified if the material in this section were moved up earlier, perhaps into Section 4.

Section 7.2

"In that case the AAA protocol needs to provide all necessary security properties for protecting CL2."

Note that in practice Diameter clients and servers are frequently configured so as to provide no cryptographic protection (e.g. no TLS or IPsec support, just cleartext TCP).

Section 7.3

"In order to address threats by compromised or rogue authenticators and other intermediary entities (as described in Section 5.5),"

Section 5.5 doesn't really talk much about threats from intermediary entities. Also, EAP mutual authentication should deal with the rogue authenticator threat, no?

Section 8.3

"[SR-KE-7] A key establishment protocol should provide key control, i.e., the peer and the authentication server both contribute to the MK computation. This property prevents a single protocol participant from controlling the value of an established key."

Since IEEE 802.16e distributes keys based solely on input from the authenticator, this property cannot be satisfied by any IEEE 802.16 authenticator, regardless of the EAP method chosen.

Section 8.4

"An EAP peer is neither able to authenticate an authenticator nor verify the information received by it. As a result, EAP methods that do not support the exchange of additional service information are susceptible to the lying access point problem and other attacks by compromised or rogues authenticators (see Section 5.5)."

Does "received by it" refer to the authenticator or peer? Suggested change:

"An EAP peer is neither able to authenticate an authenticator nor verify the information received from it. As a result, EAP methods that do not support the exchange of additional service information are susceptible to the lying access point problem and other attacks by compromised or rogue authenticators (see Section 5.5)."

Section 9.1

"The second option is less favorable because the server policy that certain authentication methods can only to be executed within a protective tunnel must be enforced by the peers. Unlike authentication servers, peers might not be aware of their policy configurations and whether they are executing an EAP method inside or outside a protective tunnel. In addition, peers are more vulnerable to attacks that could change their configurations."

I'm not clear why peer enforcement is required. If the server can be configured not to offer non-key generating or vulnerable methods outside a tunnel, wouldn't this accomplish the goal without relying on the peer?

"The last option is the least favorable one because it completely relies on the peer to correctly enforce the policy."

Not clear why mitigation 3 relies completely on the peer. Can't the server be configured not to offer non-key establishing or vulnerable methods except inside a tunnel? Such policies are commonly supported today.

pp. 37

"[SR-TBEAP-4] In the case of the parallel execution of n inner"

This should be "serial execution".

Section 11

"Compliance checks are provided for a selection of widely known methods (namely EAP-GPSK [9], EAP-TLS [12], EAP-TTLSv0 [11] and EAP-FAST [15]) representing secret key-based, public key-based and tunneled EAP methods, respectively. However, this selection is purely illustrative and does not represent favorable methods for federal use."

You might consider adding compliance checks for PEAP based on the authoritative protocol documentation (see comments on reference [14] below).

Section 11.2

"EAP-TLS supports mutual authentication, server authentication, and no authentication."

RFC 5216 Section 2.1.1 states:

" If the EAP server is not resuming a previously established session, then it MUST include a TLS server_certificate handshake message, and a server_hello_done handshake message MUST be the last handshake message encapsulated in this EAP-Request packet. "

So an EAP-TLS server needs to provide a server certificate.

"EAP-TLS may support peer privacy which requires that the username is not transmitted in cleartext (instead, a NAI is used),"

This should probably say "(instead, a privacy NAI is used)" since an NAI could otherwise provide a username in the clear.

"EAP-TLS defines one ciphersuite that is mandatory-to-implement by both authentication servers and EAP peers:"

RFC 5216 mandates support for the RFC 4346 mandatory-to-implement ciphersuite. However, EAP-TLS implementations supporting TLS 1.2 are also required to support the RFC 5246 mandatory-to-implement ciphersuite:
TLS_RSA_WITH_AES_128_CBC_SHA

"This Recommendation follows the guidelines of NIST SP 800-57, Part 3 for ciphersuites defined in TLS v1.0, TLS v.1.1 and TLS v.1.2. Hence, only CS-TLS-1 complies and CS-TLS-2, CS-TLS-3, and CS-TLS-3 shall not be implemented."

CS-TLS-3 is mentioned twice in this sentence as well as in the list of requirements above it. Was the intent to refer to Cs-TLS-4?

Section 11.3

"Hence, none of the mandatory-to-implement ciphersuites are in compliance with this Recommendation."

The difference between the EAP-FAST and EAP-TLS mandatory ciphersuite is that EAP-FAST requires implementation of the RFC 5246 mandatory-to-implement ciphersuite vs. the RFC 4346 mandatory-to-implement ciphersuite for EAP-TLS. Strange that this should result in no ciphersuites complying with the recommendation.

pp. 45

"EAP-TLS does not enable the exchange of confidential information as part of the EAP execution. For this reason, EAP-TLS does not provide an encryption algorithm."

You might say "does not utilize an encryption algorithm" since EAP-TLS does negotiate such an algorithm.

Section 11.4

"There are no mandatory-to-implement ciphersuites defined in EAP-TTLSv0."

Wouldn't this imply that the mandatory-to-implement ciphersuites are determined based on the version of TLS that is negotiated?

"This type of privacy does not violate the security requirements in this Recommendation, as long as the privacy is unidirectional (i.e. server identifiers are exchanged as part of the tunnel protocol),"

Isn't server authentication (and thereby, server identification) also a requirement for EAP-TLS?

"EAP-FAST does not support the parallel execution of multiple inner authentications inside the TLS tunnel."

This probably should be "serial execution".

Appendix: References

[2] Should refer to IEEE 802.11-2007.

[3] Should refer to IEEE 802.16e-2005 (IEEE 802.16-2004 doesn't actually support EAP).
[13] This reference is now obsolete (should use an updated reference [2] instead).
[14] This reference is obsolete. It should be replaced by the following:
http://msdn.microsoft.com/en-us/library/cc209011(PROT.10).aspx
This represents the official MS-PEAP protocol documentation.
[16] This reference should be to RFC 5295. Reference [31] already refers to RFC 5247.

Mike Farley

Hello,

It is great to see NIST publishing specific recommendations regarding EAP Methods. My organization just recently engaged a consultant to evaluate this for us and this document probably would have saved us the cost of that.

We use the NIST Computer Security documents extensively when developing policies and configurations and I have read many of them. In the past I have found the documents to be very well written and easy to follow. However, this document seems to be a departure. This draft is difficult to follow and reads more like a legal document than a recommendation/guideline. I turned to this document specifically to research EAP-FAST and to get NIST's opinion on it. I found that I had to reread the section several times and I still don't know that I understand it. Page 46 seems to be particularly convoluted.

I would suggest NIST review this document and attempt to rewrite in a way that is much more approachable. I have a fairly technical background and I have had specific wireless security training from SANS, but I still find this difficult to follow. Many of my colleagues with less background on the subject would be completely lost if they tried to read this.

Thank you,

Mike Farley

Mike Farley
Vulnerability Management & Incident Response Team
KeyBank Corporate Information Security

John Streufert

Greetings,

Please find attached the following comment(s) by the U.S. Department of State.

Thank you.

John Streufert
IA Director

(The following is converted from the excel document.)

Section 1:

Technical Comment: The author states that, "EAP was originally designed and used to support user password authentication to Internet service providers for dial-up services using the Point to Point Protocol (PPP)."

Suggested Change: RFC 3748 states that, "EAP was designed for use in network access authentication, where IP layer connectivity may not be available. Use of EAP for other purposes, such as bulk data transport, is NOT RECOMMENDED. Since EAP does not require IP connectivity, it provides just enough support for the reliable transport of authentication protocols, and no more."

Section 3.1

Technical and Editorial Comment: Definitions are not in congruence with existing definitions published in NIST IR 7298, Glossary of Key Information Security Terms, and RFC 3748, Section 1.2, Terminology.

Suggested Change: Recommend that the author review the definitions published in IR 7298 and RFC 3748 and maybe even eliminate this section altogether in favor of using the IR and RFC as the standard glossary. Or as an alternate, wherever a term and definition is created or changed in the Draft SP 800-120, recommend that it be updated in the next revision of IR 7298.

Section 4

Technical and Editorial Comment: EAP is defined in RFC 3748.

Suggested Change: Recommend that the author review the definition of EAP as published in the RFC.

Section 4.1

Technical Comment: The illustration showing the EAP communication links and involved parties does not account for a pass-through authenticator to account for those sessions in which the authenticator acts as a pass-through to determine the outcome of the authentication based on the Accept/Reject indication sent by the backend authentication server.

Suggested Change: EAP communication links and involved parties should include a pass-through authenticator for sessions in which the authenticator acts as a pass-through where it MUST determine the outcome of the authentication solely based on the Accept/Reject indication sent by the backend authentication server; the outcome MUST NOT be determined by the contents of an EAP packet sent along with the Accept/Reject indication, or the absence of such an encapsulated EAP packet.

Pasi Eronen

Hi,

I have a small comment regarding draft 800-120, and the requirements for tunnel-based EAP methods.

The text on Page 35 describes one possible way to do cryptographic binding (basically, ensuring that EAP method runs can't be "copy-pasted" from outside the tunnel to the tunnel, or from one tunnel to another), by computing a compound key (called CTK here).

However, a compound key is not the only method to perform cryptographic binding.

While current tunnel methods mostly use compound keys, using EAP in IKEv2, for example, has a similar problem. To solve the problem, IKEv2 uses RFC5056-style "channel bindings" (note that in EAP documents, "channel bindings" has a completely different meaning, quite unrelated to the RFC5056 meaning) -- basically computing a MAC (with the inner MSK as key) over information uniquely identifying the "tunnel" (the IKE_SA).

While IKEv2 is not an EAP method (it just uses EAP), a similar approach would also work for tunnel-based EAP methods.

Thus, I think the requirements SR-TBEAP-1 and SR-TBEAP-2, which require using compound keys to solve the cryptographic binding problem, should be slightly rephrased: require cryptographic binding, but allow other ways to do it in addition to compound keys.

Best regards,
Pasi

Joseph Salowey

Hi Katrin and Lily,

I finally got my comments together on SP 800-120. I think the document is already in good shape. I put together a list of comments in somewhat of a priority order. The first 5 or so are somewhat significant. I ran out of time and some of the latter comments may be somewhat cryptic. Let me know if you have any questions, need more info or want to discuss anything

Thanks,

Joe

1. Negotiation of parameters

The document does identify the negotiation of ciphersuites as an issue that effects the security of EAP methods, however this is not the only parameter that affects the security of methods. For example, the security features and/or cryptographic algorithms used may depend upon the version of the protocol. The secure negotiation of parameters such as version allows for new security capabilities such as channel binding or crypto binding to be introduced in a backward compatible way. Without this, strict policy must be enforced which will often be incompatible with current deployments.

Document Modification Suggestions:

Section 4.6 - Discuss parameter negotiation in addition to ciphersuites. This would typically include version and security related parameters.

Section 5.2 - Discuss vulnerability associated with negotiation of other parameters. For example disabling channel bindings or improper selection of ciphersuites if bound to a version.

Section 6.2 - in list include negotiation of ciphersuites, version and other security related parameters. Discuss that other security related parameters may need to be negotiated. Also I did not see much of a discussion of backward compatibility in section 4.6.

Section 8 - I didn't see in the document where it discussed hard coded algorithms. While hard coded algorithms may be used it is best to provide some means of agility, even it if is through versioning.

Section 8.1 and 8.5 - Methods also should provide protected verification of other security related parameters. Perhaps an SCN-CN-3 should be added to cover this or the

requirement SR-MP-1 should point out that it is important to secure negotiation of parameters in addition to ciphersuites that are related to security, such as protocol version. Probably a discussion in section 8.5 is better since it seems the requirement is already there.

2. Tunnel Man-in-the-middle attack

A few observations on the tunnel man-in-the-middle attack material.

In section 9.1 the peer can also fall victim to the attack if it does not perform proper authentication of the server. This emphasizes the need for mutual authentication and the danger of anonymous connections.

In section 9.1 the protocol reflected to the peer does not have to be an EAP protocol, it just needs to use the same credentials in a vulnerable protocol. For example, if "single sign-on" is in use and the user name and password are used with unprotected web authentication then there still is a man-in-the-middle attack. This also applies to section 9.3, SR-TEAP-2 which should add something like "The same credentials shall not be used in weak unprotected authentication protocols outside of EAP".

The description of the attack in section 5.4 is not as clear as in section 9.1. Perhaps this section should just reference section 9.1. Also a weak method is weak whether it is proprietary or not.

3. Section 8 requirements applicability to tunnel methods (section 9)

It seems that most of the requirements in section 8 should apply to tunnel methods, but it seems that some are not included. Section 9.2 pulls in 8.3 and section 8.2. The other sections 8.1, 8.4 and 8.5 do not seem to be covered. Not all of these are necessarily taken care of by the tunnel. For example CB-1 and SR-MP-1 are not currently part of the TLS tunnel handshakes.

4. EAP Server location

The wording in section 4.1 is strange. The EAP server is usually located within a AAA server and accessed through AAA protocols. The EAP server is access through AAA protocols and not the other way around. It is true that an EAP server may have to validate credentials against a remote data store, but this can be any one of a wide variety of protocols such as LDAP, ODBC, etc.

5. Backend Authentication server, Full authentication and Local authentication

In general backend authentication services are not required by EAP. There are deployed systems that collocate the EAP-Server with the authenticator. This is especially useful with methods that use certificate based credentials such as EAP-TLS. It is not clear that only focusing on the backend case makes the document any simpler. It seems the

document can state that the EAP server may be collocated with the authenticator. There is a tradeoff between securing C2 and securing the EAP Server that can also be discussed.

In addition the terms full authentication and local authentication are introduced at the beginning of the document and not used later in the document. They are some what problematic in that it seems to indicate that local authentication is always based on temporary credentials and that full authentication always requires a back end. Since these terms are not used during the discussion of requirements perhaps they should be removed?

6. Result indications

The document does not have much discussions about result indications. These are desirable to make sure that the peer and server have the same notion of what has taken place. They are discussed in section 8.4. Should this also be discussed for the result of authentication and perhaps associated authorization?

7. Point of Attachment

Point of attachment may need to be better defined. Does it refer to a wireless AP? There are widely deployed wireless architectures, such as CAPWAP, in which the authenticator is not in the AP, but is in a Controller. Here the authenticator is often not at the edge of the network and greater physical security can be provided.

8. Role of EAP

The "authorization and authentication check of the authenticator by the authentication server" is not strictly in the scope of EAP. EAP itself is mode independent and doesn't take into account whether it is running in pass-through mode or not. EAP must have help from the rest of the system that knows this information and can make these decisions.

9. Authenticator as Federal device

In section 4.1 you mention it is of no importance whether the authenticator is a federal or non-federal device. I'm not really familiar with what it means to be a federal device, but it seems the authenticator is involved because it handles the MSK and does encryption and message protection with the supplicant. From an EAP perspective it may not matter as long as the EAP server is not collocated with the authenticator.

10. [SR-KD-4]

As you know this typically isn't done by methods today, its not clear what the identities are or how they make their way to the EAP methods. Is there any guidance here?

11. Information Needed in channel binding

I think as much detail as possible of channel bindings should be left to the channel bindings document. This section seems to indicate that all information is equally relevant. This seems misleading as not all information will be required in all cases.

12. CTK key confirmation

I found SR-TBEAP-1 a little confusing, perhaps the term "key confirmation" should be used in place of or in addition to authentication: "and how this key is used to perform mutual key confirmation"

13. EAP Identity Request, Success and Failure

These are not strictly required by EAP (the exchange can begin with a method and the success and failure can be lost). However, they are almost always present in practice.

14. EMSK Usage

In the EMSK definition you indicate that it is reserved for future use, however in section 4.5 you mention it is used. Perhaps the definition should be updated.

15. Client authentication in tunnel establishment

It might be worth noting that peer authentication may be executed in tunnel establishment.

16. Missing Annex A

Section 5.1 mentions Annex A which appears to be missing or named differently.

17. CS-TLS numbering

In section 11.2 CS-TLS 3 is used twice in the list and the following paragraph. It seems that one of these should be CS-TLS-4.

Jennifer Evans

The Financial Management Service, one of Treasury's Bureaus, has no comments to offer on this document.

Regards,

Jennifer Evans
Treasury, FMS, Mission Assurance Division

Anthony Leibovitz

TO WHOM IT MAY CONCERN:

Regarding NIST SP800-120, I respectfully request the addition of MS-PEAP and related modifications noted below to NIST SP800-120, “Recommendation for EAP Methods Used in Wireless Network Access Authentication”.

The basis for these requests is as follows:

1. MS-PEAP meets the requirements specified in NIST SP800-120, along with the other listed protocols such as EAP-FAST and EAP-TTLSv0. Specifically, MS-PEAP supports cryptobinding, identity privacy, protected ciphersuite negotiation, mutual authentication and other requirements outlined in the bulletin.
2. MS-PEAP is included and widely available on all modern versions of the Windows operating system (starting with Windows XP) and implementations are available for virtually all other operating systems in existence today – including Apple’s MacOS, Linux, etc.
3. MS-PEAP is broadly deployed; including deployment within the US Government, its agencies, contractors and affiliates.
4. There exists considerable customer interest in MS-PEAP vis-à-vis interest in Microsoft Network Access Protection which utilizes MS-PEAP. Consumers who are impacted by NIST SP800-120 should be informed that MS-PEAP meets the requirements as set out by the bulletin.
5. Factual correction of references to improve quality of the document.

The exclusion of MS-PEAP from NIST SP800-12 is both a significant and conspicuous missing element of the bulletin and its omission does not serve the public’s best interests in providing a “Recommendation for EAP Methods Used in Wireless Network Access Authentication.”

I am happy to assist with questions and/or clarifications to this request. Please feel free to contact me.

Thank-you,

Anthony Leibovitz
Senior Program Manager
Microsoft Corporation

Specific Requests:

Item	Request
1	Add **MS-PEAP: Protected Extensible Authentication Protocol (PEAP)** to section 11: “Discussion of Selected EAP Methods”, including a Compliance Check Table for MS-PEAP

2	Include appropriate parallel references to MS-PEAP throughout the special publication.
3	Please update the stale MS-PEAP reference in the document's appendix from "[14] IETF Personal draft, Vivek Kamath, Ashwin Palekar, Mark Wodrich, "Microsoft's PEAP version 0 (Implementation in Windows XP SP1)", draft-kamath-pppext-peapv0-00.txt, work in progress, October 2002" to http://download.microsoft.com/download/9/5/E/95EF66AF-9026-4BB0-A41D-A4F81802D92C/%5BMS-PEAP%5D.pdf

---

Hao Zhou

Katrin:

Here are my review comments. Very good document.

1. Section 3.1, I don't quite understand the statement: "Unlike the authentication server, the authenticator is typically not located in the protected (wired) network." This contradicts with Section 7.2.
2. Section 3.2, PMK might also have another definition, pairwise master key in 802.11i. Plus it is not used at all in the document. Suggest to remove it.
3. Should add AVP to the definition table.
4. Figure 2, the 4th message sent from the peer should be NAK. Otherwise, two different EAP types have been executed within a single EAP execution.
5. Section 4.4 "Inner authentication methods can be EAP methods or other authentication schemes encapsulated in EAP methods. ". Not quite true. The inner method could be non-EAP based, such as PAP, CHAP etc. run inside EAP-TTLS.
6. Section 5.1, it's worthwhile to point out that dictionary attack can also be done as part of the passive attacks.
7. Section 5.4, I would call the MITM attack mentioned in this section a different name, such as Compound MITM or Tunnel MITM, to be distinct from the normal MITM attack.
8. Section 6.1, could we add other EAP objectives, especially for EAP running on wireless, such as session resumption for roaming, handover, channel-binding, computationally lightweight and efficiency for low power and resource constrainted devices.
9. Section 6.2 and Section 8.1, could the ciphersuite negotiation be extended to include version negotiation an EAP type header negotiation as well? If we don't have secure version and EAP type header negotiation, attacker can play a downgrade attack.

10. Section 9, it helps to stress tunnel EAP method must also meet all requirements for non-tunneled EAP methods in Section 8. What is described in Section 9 are additional requirements for tunnel method. I see section 9 covers a couple of section 8 requirmeents, but not all of them.
11. Section 11.4, "As for EAP-FAST, with a recommended choice of TLS ciphersuites the tunnel protocol meets all requirements, " Is "EAP-FAST" supposed to be "EAP-TTLS"?

Yoshihiro Ohba

General comment: The document is very carefully written and covers all aspects of EAP key management. I have only minor comments as described below.

Specific comments:

In Section 3, PoA stands for "point of attachment", while it stands for "point of access" in Section 1. Consistent usage of the terms PoA, point of attachment and point of access is recommended.

In Page 12, Key derivation is defined as "The process that derives keys from another key or from the shared secret of a key agreement scheme." What is the definition of key agreement scheme? On the other hand, the definition of key derivation can be simplified as "The process that derives keys from another key." without mentioning key agreement scheme.

In Page 20, last paragraph, what is the definition of "legacy authentication methods"?

In Section 8.1, one specific method of comparing CS_offer and CS_offer' as well as CS_select and CS_select' is described. However, there are other ways of post-verification. One example is a mechanism that is similar to Finished message exchange in TLS. For this reason, it is recommended to revise the Section 8.1 that the post-verification method described in Section 8.1 is one example and there can be other mechanisms for post-verification.

In Page 36, difference between the 2nd and 3rd policies for mitigating man-in-the-middle attack on tunnel-based EAP methods is not clear. It is recommend to either clarify the difference or remove the 3rd policy.

Figure 9 can be enhanced to (i) add MK of tunneling-based EAP method above TK and connect the MK and TK, (ii) replace MK next to TK with MK_i (0<i<=n), and (iii) replace CK with CTK.

In Appendix, reference [2] should be updated to point to IEEE 802.11-2007.

Best Regards,
Yoshihiro Ohba, Ph.D
Research Director
Toshiba America Research, Inc.

Rafael Marin Lopez

Dear Sir/Madam

Please see below my comments on SP 800-120

"DRAFT Recommendation for EAP Methods Used in Wireless Network Access Authentication"

In general, the document is very well-written and pretty clear though some comments/clarifications are highlighted in the following:

beginning page 9

"..."and a back end EAP Authentication Server (AS)" I would suggest to say: "and EAP server located in a back end authentication server" After all it is the pass-through mode what it is used in mobile scenarios.

Page 11
Extensible Authentication Protocol (EAP) Authentication An authentication framework defined in IETF RFC 3748. The Extensible Authentication Protocol can support different authentication methods.

Note that RFC 5247 updates RFC 3748.

Page 16

"As specified in [1], EAP is a framework for two party authentication protocols that are executed between a peer and an authentication server (AS)...""

Actually, they are executed between the peer and EAP server. In pass-through mode, the EAP server is located in the authentication server (AS). I shall suggest to clarify that part.

Page 17

"Note that the server has access to an AAA server as well as a local database (DB), sometimes co-located with the server."

I am not sure why server (authentication server) is considered as a separated entity from AAA server. Usually, the authentication server IS a AAA server where the EAP server is located.

In page 18, authentication server definition also assumes that.

Page 19, Figure 2

According RFC 3748, not sure figure is correct, only one method (e.g. type T_1) is allowed between the EAP Identity exchange and EAP success.

2.1. Support for Sequences

An EAP conversation MAY utilize a sequence of methods. A common example of this is an Identity request followed by a single EAP authentication method such as an MD5-Challenge. However, the peer and authenticator MUST utilize only one authentication method (Type 4 or greater) within an EAP conversation, after which the authenticator MUST send a Success or Failure packet.

Page 28.

"In that case the AAA protocol needs to provide all necessary security properties for protecting CL2."

Note that even in that case, intermediate AAA proxies can observe and modify the information that pass through them (though AAA protocol provides integrity and confidentiality)

Reference section

Both [16] and [31] is RFC 5247. However, only [31] is RFC 5247. [16] is RFC 5295

My best regards.

Rafael Marin Lopez
Dept. Information and Communications Engineering (DIIC)
Faculty of Computer Science-University of Murcia

Gerald V. Burton

Greetings. CDC has no comments on the latest draft of SP 800-120. Please refer any questions to the undersigned.

Gerald V. Burton
IT Specialist (Infosec)
Office of the Chief Information Security Officer
Centers for Disease Control and Prevention

Jouni Malinen

I'm sorry about missing the deadline for the comment period for SP 800-120. If you are willing to consider additional comments at this point, I'm sending couple of my observations on the Dec 22, 2008 draft of SP 800-120:

1. Introduction

- IEEE 802.16 does not use IEEE 802.1X/EAPOL; it has its own encapsulation mechanism for EAP

4.6. EAP Ciphersuite Negotiation

- while EAP-AKA itself is an example of an EAP method that does not negotiate cryptographic algorithms and parameters, it may not be ideal example of such a method taken into account that EAP-AKA' is in the final steps of being published as an RFC and does introduce negotiation on top of EAP-AKA (though, by using another EAP method type)

11.2 EAP-TLS

- using CS-TLS-3 to refer to two different ciphersuites (RSA with AES-128-CBC with SHA-1 and RSA with RC4-128 with MD5) is a bit confusing; could the latter identifier be renamed to CS-TLS-4?

- is the first CS-TLS-3 (TLS_RSA_WITH_AES-128-CBC_SHA-1) really not compliant with NIST SP 800-57, Part 3? Doesn't it match with Table 4-1 entry TLS_RSA_WITH_AES_128_CBC_SHA [256]? Or am I interpreting the "[256]" part incorrectly (based on the description in 4.2.2, I read it to mean that both SHA-1 and SHA-256 are acceptable with TLS 1.0); it would be odd to allow 3DES-EDE-CBC to be used, but not AES-128-CBC..

11.3 EAP-FAST

- doesn't CS-FAST-2 and CS-FAST-3 match with NIST SP 800-56, Part 3 Table 4-1 entries TLS_RSA_WITH_AES_128_CBC_SHA [256] and TLS_DHE_RSA_WITH_AES_128_CBC_SHA [256] and as such, would comply with the requirements (i.e., no requirement to implement additional ciphersuites for TLS in EAP-FAST)

11.4 EAP-TTLSv0

- how can EAP-TTLSv0 be in compliance with SR-TBEAP-2 if it is not in compliance with SR-TBEAP-1 due to not supporting cryptographic bindings and not deriving CTK; MSK and EMSK are derived directly from TK in case of EAP-TTLSv0 and that does not sound like compliant design as far as SB-TBEAP-2 requirement is concerned

Appendix: References

- "IEEE Standard 802.11-1999" has been superseded by IEEE Std 802.11-2007 (and the 2007 version incorporates IEEE Std 802.11i-2004 that was mentioned earlier in the document)

--
Jouni Malinen