EMU
IETF 105

Chairs: Mohit Sethi, Joe Salowey

NOTE WELL

This is a reminder of IETF policies in effect on various topics such as patents or code of conduct. It is only meant to point you in the right direction. Exceptions may apply. The IETF's patent policy and the definition of an IETF "contribution" and "participation" are set forth in BCP 79; please read it carefully.

As a reminder:

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.

As a reminder:

- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam (https://www.ietf.org/contact/ombudsteam/) if you have questions or concerns about this.

Definitive information is in the documents listed below and other IETF BCPs. For advice, please talk to WG chairs or ADs:

- BCP 9 (Internet Standards Process),
- BCP 25 (Working Group processes),
- BCP 25 (Anti-Harassment Procedures),
- BCP 54 (Code of Conduct),
- BCP 78 (Copyright),
- BCP 79 (Patents, Participation),
- https://www.ietf.org/privacy-policy/ (Privacy Policy)

Agenda

05 min	Administrivia (Minutes, Jabber, BuleSheets)
20 min	WG Documents
	draft-ietf-emu-eap-tls13 draft-ms-emu-eaptlscert
	draft-ietf-emu-rfc5448bis draft-arkko-eap-aka-pfs
	draft-dekok-emu-eap-session-id
25 min	RFC 7170 (TEAP) Erata
5 min	draft-dekok-emu-tls-eap-types
30 min	Recharter discussion
15 min	draft-aura-eap-noob
10 min	draft-lear-eap-teap-brski
10 min	draft-friel-acme-integrations

draft-ietf-emu-eap-tls13

- Completed WGLC
- Issues raised by Jouni Malinen
  - Sending empty data record inconvenient for implementations, proposed send one byte 0x00 instead
  - Omitting NewSessionTicket causes similar problem, proposal to force new session ticket always
- Any other implementers out there?
- Any concern with the proposals
  - Confusion with sending encrypted data bytes in EAP-TLS
  - Always sending newSessionTIcket

draft-ms-emu-eaptlscert

- Any objections to adoption?

draft-dekok-emu-eap-session-id

- Any objections to adopting as a WG item and issuing WGLC?

draft-arkko-eap-aka-pfs

- Call for adoption had consensus
- IPR raised some objections
  - No alternatives proposed
  - General consensus that document is needed and should move forward
  - Similar IPR situation to EAP-AKA/EAP-AKA’
- Proposal: Accept document into working group as Information Document

draft-ietf-emu-rfc5448bis

- WGLC completed, new revision submitted
- Ready to move forward to IESG?

TEAP Errata (5127,5128)

- 5127, 5128
- Function Signature for TLS-PRF wrong

IMCK[j] = TLS-PRF(S-IMCK[j-1], "Inner Methods Compound Keys", IMSK[j], 60)
IMSK = First 32 octets of TLS-PRF(EMSK, "TEAPbindkey@ietf.org" | "\0" | 64)

- Should be

IMCK[j] = TLS-PRF(CK[j-1], "Inner Methods Compound Keys" | IMSK[j], 60)
IMSK = First 32 octets of TLS-PRF(EMSK, "TEAPbindkey@ietf.org" | "\0", 64)

- Proposed: Accept

TEAP Errata (5765)

- Change Authority-ID to be optional
  - Outer TLVs MUST be optional
- Proposal: Accept

TEAP Errata (5767)

Section 3.3.1 says:

EAP method messages are carried within EAP-Payload TLVs defined in Section 4.2.10. If more than one method is going to be executed in the tunnel, then upon method completion, the server MUST send an Intermediate-Result TLV indicating the result.

It should say:

EAP method messages are carried within EAP-Payload TLVs defined in Section 4.2.10. Upon completion of each EAP authentication method in the tunnel, the server MUST send an Intermediate-Result TL indicating the result.

Also clarify Authentication method text

- Proposal: Accept

TEAP Errata (5768)

- Compound MAC is fixed, bu calculation does not truncate
  - What to do?
  - Variable Length or Truncate
  - Implementation?
- Do not fix TLS version to 1.2
- Encoding of EAP-TYPE clarification

Proposal: DIscuss

TEAP Errata (5770)

- S-IMCK[j] derivation
  - Does this just need clarification?

TEAP Errata (5775)

What if there is not key generating method executed?

- WHat is CMK[0]

What do implementations do?

- Use 0s?
- Use Ssession_key_seed

Charter Update

- Several new drafts covering different topics:
  - Fixes based on errata or update of underlying technologies (TLS 1.3):
    - draft-dekok-emu-tls-eap-types
    - EAP-TEAP
  - OOB authentication method for EAP:
    - draft-aura-eap-noob
  - Using time or domain-limited credentials for creating longer term credentials
    - draft-lear-eap-teap-brski
    - EAP-Creds

Charter Update

The Extensible Authentication Protocol (EAP) [RFC 3748] is a network access authentication framework used, for instance, in VPN and mobile networks. EAP itself is a simple protocol and actual authentication happens in EAP methods. Several EAP methods have been developed at the IETF and support for EAP exists in a broad set of devices. Previous larger EAP-related efforts at the IETF included rewriting the base EAP protocol specification and the development of several standards track EAP methods.

EAP methods are generally based on existing security technologies such as TLS and SIM cards. Our understanding of security threats is continuously evolving. This has driven the evolution of several of these underlying technologies. As an example, IETF has standardized a new and improved version of TLS in RFC 8446. The group will therefore provide guidance and update EAP method specifications where necessary to enable the use of new versions of these underlying technologies.

At the same time, some new use cases for EAP have been identified. EAP is now more broadly in mobile network authentication. The group will update existing EAP methods such as EAP-AKA' to stay in sync with updates to the referenced 3GPP specifications. RFC 7258 notes that pervasive monitoring is an attack. Perfect Forward Secrecy (PFS) is an important security property for modern protocols to thwart pervasive monitoring. The group will therefore work on an extension to EAP-AKA' for providing Perfect Forward Secrecy (PFS).

Charter Update

Out-of-band (OOB) refers to a separate communication channel independent of the primary in-band channel over which the actual network communication takes place. OOB channels are now used for authentication in a variety of protocols and devices (draft-ietf-oauth-device-flow-13, WhatsApp Web, etc.). Many users are accustomed to tapping NFC or scanning QR codes. However, EAP currently does not have any standard methods that support authentication based on OOB channels. The group will therefore work on an EAP method where authentication is based on an out-of-band channel between the peer and the server.

EAP authentication is based on credentials available on the peer and the server. However, some EAP methods use credentials that are time or domain limited (such as EAP-POTP), and there may be a need for creating long term credentials for re-authenticating the peer in a more general context. The group will investigate minimal mechanisms with which limited-use EAP authentication credentials can be used for creating general-use long-term credentials.