EAP Usage in 5G

Jari Arkko, Vesa Lehtovirta, Karl Norrman, Vesa Torvinen
Ericsson Research

In early 2000s, IETF worked on the Extensible Authentication Protocol (EAP, RFC 3748) framework

We also defined authentication methods in the EAP and EMU WGs, including ones relating to GSM and 3/4G authentication mechanisms:

- EAP-SIM (RFC 4186)
- EAP-AKA (RFC 4187), revised in EAP-AKA' (RFC 5448)

Very widely implemented, somewhat widely used for WLAN access authentication (2/3/4G access uses native SIM card and AKA, not EAP)

5G access authentication introduces the use of EAP for 5G access

draft-arkko-eap-rfc5448bis

- A tiny update of EAP-AKA’
- EAP-AKA’ binds the context of authentication to the produced keys (context = authentication to WLAN, etc)
- Part of the binding context is defined in 3GPP TS 24.302 Table 8.1.1.2 (2008 version) — for 5G, “5G” added to table
- Reference version change seems like a small reason to update an RFC… but it is on a key part
- Could also update security considerations, but not a place for new functionality

draft-arkko-eap-aka-pfs

draft-arkko-eap-aka-pfs

- The 2015 revelations lead to SIM card manufacturers, the operators, and GSMA reconsider their processes & much improvements have been made … but vulnerabilities cannot be ruled out

- Backwards-compatible extension that adds Diffie-Hellman exchange to EAP-AKA'; output keys from EAP will now provide Perfect Forward Secrecy

- If there is a compromise of smart card long-term keys, the use of EAP AKA' PFS requires protects against passive attackers (or forces active attack)

- Details… look at the draft / can probably be done in different ways

- No current official requirements for this, but I think prudent design

Next Steps

- Feedback on these drafts very welcome!
- Coordination between IETF and 3GPP in EAP space would be useful — there are topics beyond what I talked about here
- I'd like to keep existing RFCs up-to-date whenever there are updates, even if small — how to pursue?
- I believe we should consider enhancing our protocols to match current pervasive surveillance and other threats — more substantial work than the above
  - FYI: also other potential documents in EAP method space, e.g., draft-mattsson-eap-tls13