RFC 5448bis post-WGLC update

Jari Arkko, Vesa Lehtovirta, Vesa Torvinen
Ericsson Research
(+ RFC 5448 author Pasi Eronen)

draft-ietf-emu-rfc5448bis-04.txt

http://www.arkko.com/ietf/eap/
draft-ietf-emu-rfc5448bis-from-rfc5448.diff.html

Reminder of why -bis was needed

- Identifier usage is special for 5G
- Network name bindings changed for 5G
- Definition of exported parameters is required by RFC 5247
- Security, privacy, and pervasive monitoring considerations
- Document vulnerabilities
- Requirements on the generation of pseudonym and fast re-authentication identifiers
- References need updates

Comments and Questions

Form

- Clarification of updates/obsoletes language (Daniel Migault)

Editorial:

- Protocol name, extra spaces, missing “.”, … etc (per John Mattsson and Daniel Migault)

5G related:

- The permanent identifier (SUPI) is fed to the KDF in 5G. There’s a new question about this format (Marcus Wong)

Clarifications:

- Notation [n..m] is inclusive? Yes (Daniel Migault)
- Attribute length field calculation rules? Refer to RFC 4187 (Daniel Migault)
- Hex/dec in session id definitions (John Mattsson)
- EAP-AKA’ refers to RFC 4187 for many parts; can these parts use the references from that RFC (old) or if new ones are needed? (Daniel Migault)
- …

Security considerations:

- Can vs. SHOULD in “… refuse to send the cleartext permanent identity if it believes … should be able to recognize the pseudonym” (Daniel Migault)
- New underlying AKA attacks since last update

SUPI and KDF

- SUPIs are never sent on the wire, but used by KDF
- SUPIs can be either IMSIs or free-form NAIs
- There’s a discrepancy between TS 23.003 Section 2.2A and draft Section 5.3.1.1:
    - Draft represents everything as NAIs, as IMSIs can be NAIs (123456789@nai.5gc.mnc456.mcc123.3gppnetwork.org)
    - TS specifies a concept of a SUPI type followed by the SUPI value itself, but does not specify the actual format of the type

New Attacks

- AKA and mobile network security are a frequent target of analysis by academic community; possible new attacks appear at times
- Most recently, some news coverage of https://eprint.iacr.org/2018/1175.pdf
- I think our (IETF & EAP) principle should be the use of algorithms and procedures, and documenting their security properties
    - When or if changes to underlying algorithms are needed, that should be the task of who defined the algorithm (3GPP in this case)

=> add an overview of the impacts of this attack to Security Considerations

Next Steps

- Fixes during IETF week
    - Including E-mail discussion with 3GPP SA3 folk
- Resubmit and do IETF last call