EAP-AKA’ Updates

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

draft-arkko-eap-rfc5448bis-01.txt
draft-arkko-eap-aka-pfs-01.txt

Background

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 small update of EAP-AKA’
- Updates are bugs in the current specification, missed items, or specifying behaviour for new situations introduced in 5G
- Changes in -01: upon deeper inspection, realised that there are two other issues beyond the one in -00
- Could also update security considerations, but not add new functionality

rfc5448bis updates

1. 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

2. Specify how EAP-AKA' uses identifiers in 5G, as there will be multiple to choose from; important that both sides use the same

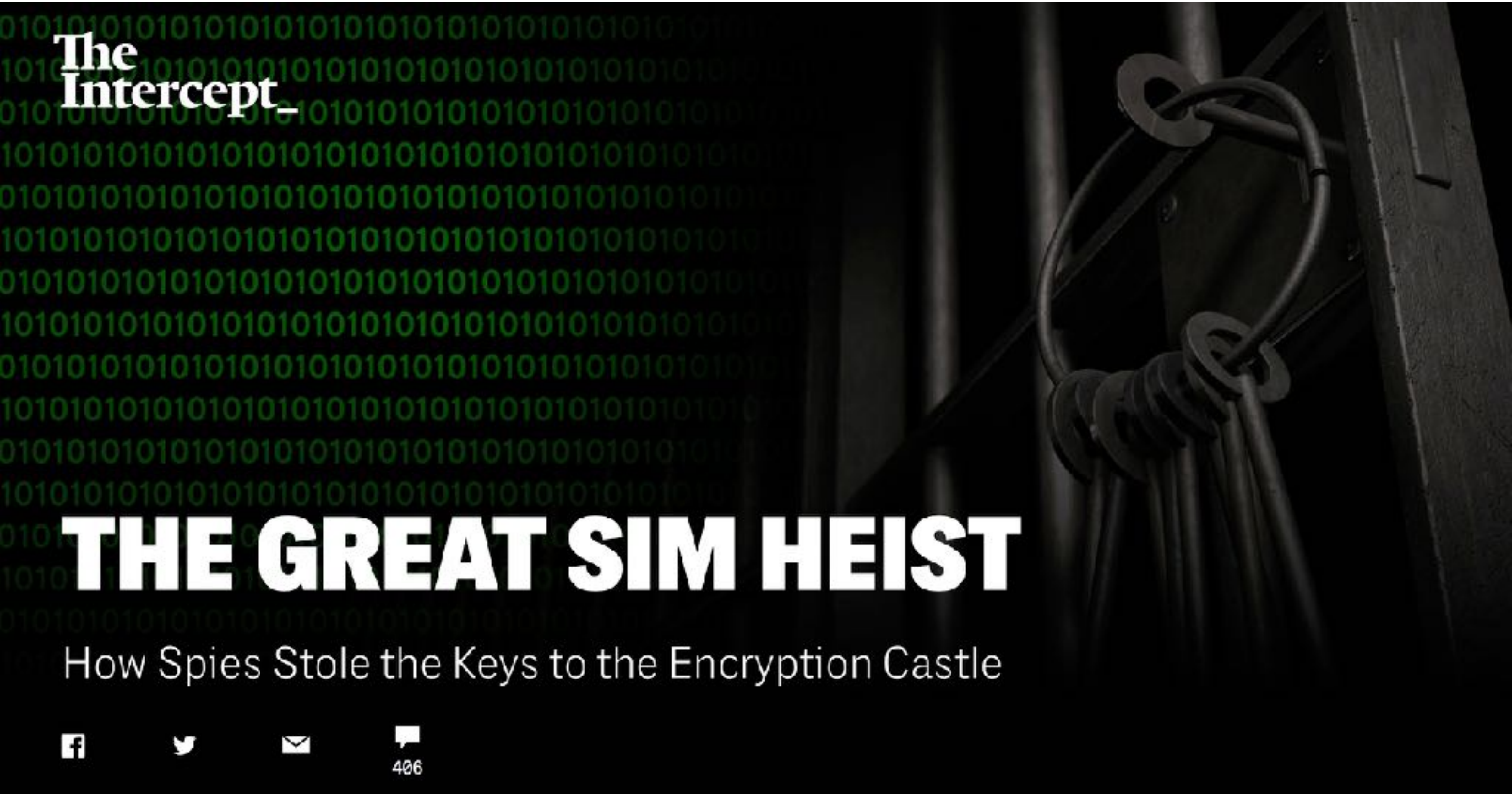
   - Use the actually sent identifier in key calculation, the temporary id, or the long-term identifier? Unclear if RFC 5448 were to be used in 5G…

3. Specify session identifiers and other exported parameters, as those were not specified in RFC 5448 despite requirements set forward in RFC 5247

rfc5448bis Next Steps

- Give us feedback & discuss!
- What other things did we miss?
- Note: coordination between IETF and 3GPP in EAP space is needed (and is ongoing; please contribute)

draft-arkko-eap-aka-pfs



The Intercept_

THE GREAT SIM HEIST

How Spies Stole the Keys to the Encryption Castle

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 protects against passive attackers (or forces active attack)

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

- Support for perfect forward secrecy is in the plans for the 2nd phase of 5G specifications

*) Has an IPR notice

Next Steps

- Need to enhance our protocols to match current pervasive surveillance and other threats
- There seems to be demand for PFS in the industry
- Send us feedback & discuss!
- Again, coordination with 3GPP is important and discussions are ongoing