

Formal verification of the 5G EAP-TLS authentication protocol using Proverif

31-01-2023

Alessandro Zanatta

University of Pisa

Reference paper (DOI): [10.1109/ACCESS.2020.2969474](https://doi.org/10.1109/ACCESS.2020.2969474)

Proverif

- Symbolic verification tool:

Proverif

- Symbolic verification tool:
 - Attacker \rightarrow Dolev-Yao;

Proverif

- Symbolic verification tool:
 - Attacker \rightarrow Dolev-Yao;
 - Cryptographic primitives \rightarrow black-box;

Proverif

- Symbolic verification tool:
 - Attacker \rightarrow Dolev-Yao;
 - Cryptographic primitives \rightarrow black-box;
 - **Perfect cryptography** assumption:

Proverif

- Symbolic verification tool:
 - Attacker \rightarrow Dolev-Yao;
 - Cryptographic primitives \rightarrow black-box;
 - **Perfect cryptography** assumption:
 - e.g. can decrypt $\text{enc}(m, k) \iff k$ is known

Proverif

- Symbolic verification tool:
 - Attacker \rightarrow Dolev-Yao;
 - Cryptographic primitives \rightarrow black-box;
 - **Perfect cryptography** assumption:
 - e.g. can decrypt $\text{enc}(m, k) \iff k$ is known
- Based on **applied π -calculus**;

5G EAP-TLS protocol entities

- Home Network (HN):
 - Authentication Server Function (**AUSF**)
 - Certificate $CERT_{AUSF}$
 - Unified Data Management (**UDM**)
 - Authentication Credential Repository and Processing Function (**ARPF**)
 - Subscription Identifier De-concealing Function (**SIDF**)

5G EAP-TLS protocol entities

- Home Network (HN):
 - Authentication Server Function (**AUSF**)
 - Certificate $CERT_{AUSF}$
 - Unified Data Management (**UDM**)
 - Authentication Credential Repository and Processing Function (**ARPF**)
 - Subscription Identifier De-concealing Function (**SIDF**)
- User Equipment (UE):
 - Subscription Permanent Identifier (**SUPI**)
 - Public asymmetric key pk_{UDM}
 - Certificate $CERT_{UE}$

5G EAP-TLS protocol entities

- Home Network (HN):
 - Authentication Server Function (**AUSF**)
 - Certificate $CERT_{AUSF}$
 - Unified Data Management (**UDM**)
 - Authentication Credential Repository and Processing Function (**ARPF**)
 - Subscription Identifier De-concealing Function (**SIDF**)
- User Equipment (UE):
 - Subscription Permanent Identifier (**SUPI**)
 - Public asymmetric key pk_{UDM}
 - Certificate $CERT_{UE}$
- Serving Network (SN):
 - Security Anchor Function (**SEAF**)

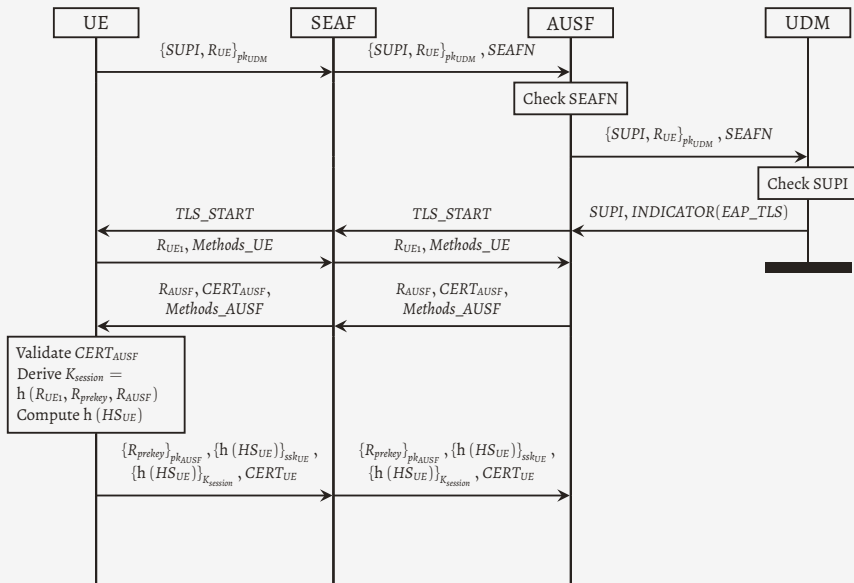
5G EAP-TLS protocol entities

- Home Network (HN):
 - Authentication Server Function (**AUSF**)
 - Certificate $CERT_{AUSF}$
 - Unified Data Management (**UDM**)
 - Authentication Credential Repository and Processing Function (**ARPF**)
 - Subscription Identifier De-concealing Function (**SIDF**)
- User Equipment (UE):
 - Subscription Permanent Identifier (**SUPI**)
 - Public asymmetric key pk_{UDM}
 - Certificate $CERT_{UE}$
- Serving Network (SN):
 - Security Anchor Function (**SEAF**)

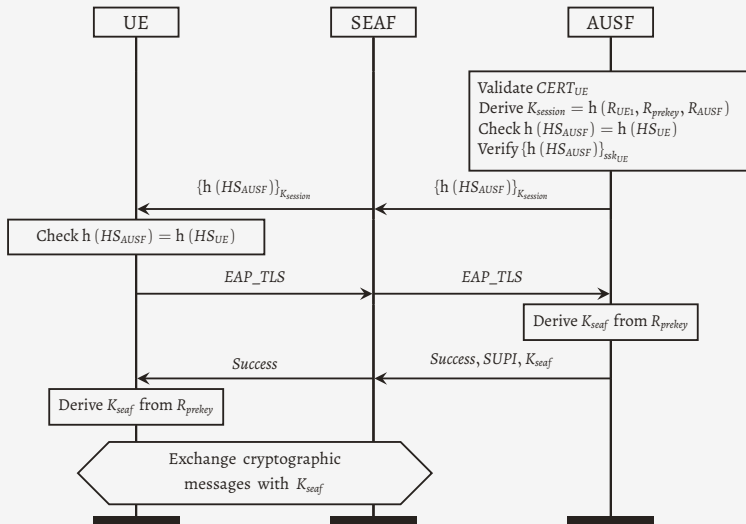
Assumptions:

- $HN \leftrightarrow SN$ communications are secure

5G EAP-TLS protocol execution I



5G EAP-TLS protocol execution II



Required security properties

Required security properties

- **Authentication properties:**

- A1. Both the home network and the subscriber should agree on the identity of each other after successful termination
- A2. Both the home network and the subscriber should agree on the pre-master key R_{prekey} after successful termination

Required security properties

- **Authentication properties:**

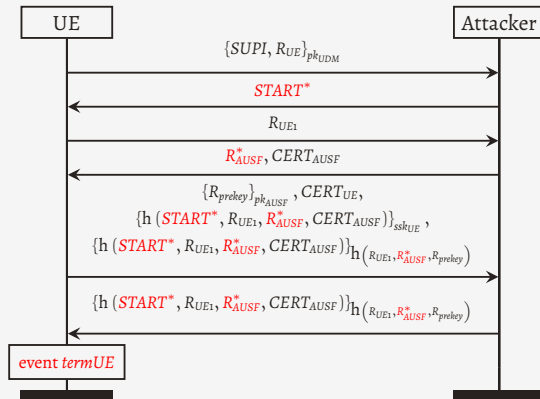
- A1. Both the home network and the subscriber should agree on the identity of each other after successful termination
- A2. Both the home network and the subscriber should agree on the pre-master key R_{prekey} after successful termination

- **Secrecy properties:**

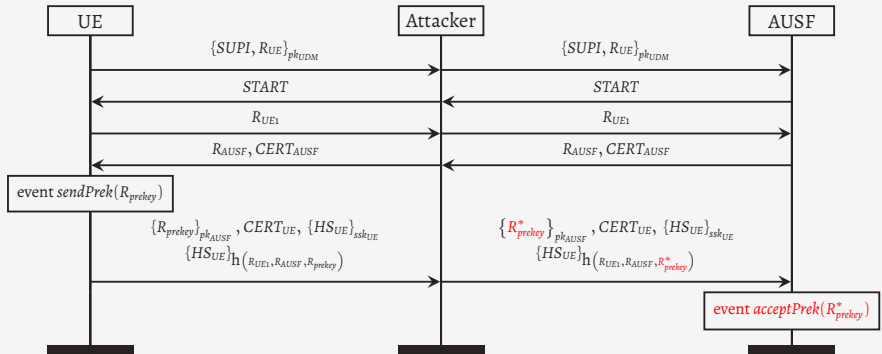
- S1. The attacker cannot obtain the identity $SUPI$ of an honest subscriber
- S2. The attacker cannot obtain the pre-master key R_{prekey} of an honest subscriber
- S3. The attacker cannot obtain the session key $K_{session}$ of an honest subscriber

It's **DEMO** time!!

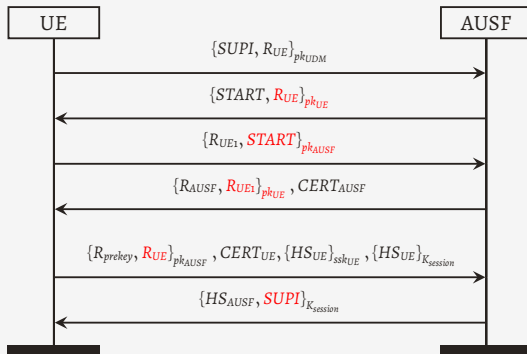
Counterexample for property A1



Counterexample for property A2



Fixing the protocol



THANKS
for your attention!!