Secure Systems Group, Aalto University

Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, Tuomas Aura

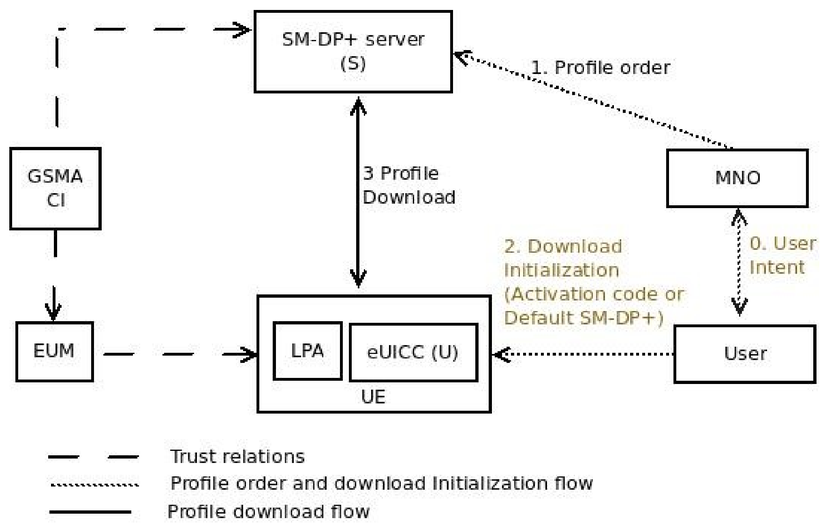
Formal Analysis of the Consumer Remote SIM Provisioning (RSP) Protocol

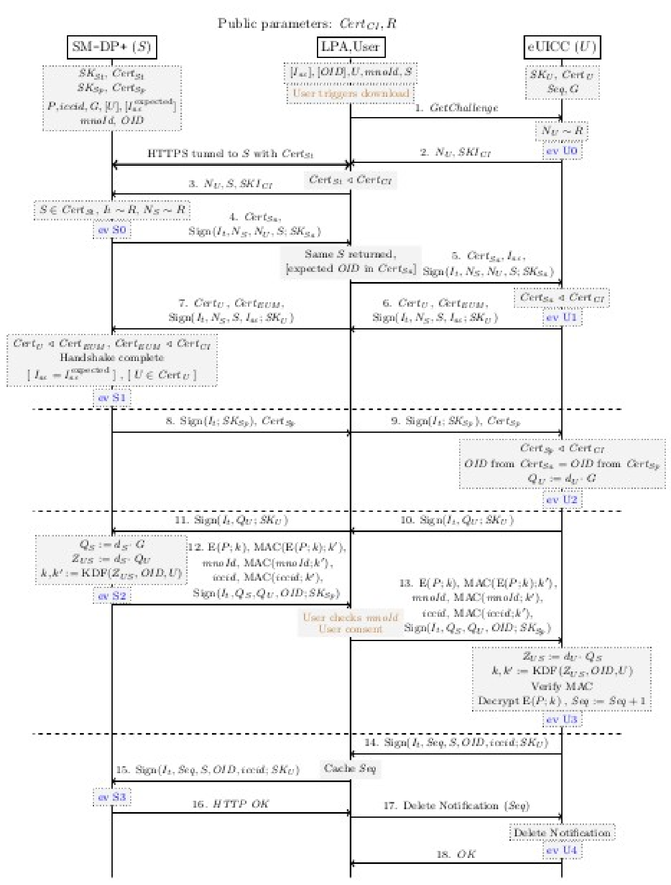
Goal

- Formally verify security goals of the Consumer RSP protocol
- Increase confidence for the protocol provided security
- Recommendations to improve security of the protocol for both the existing deployments and future releases

Consumer RSP

- SIM card is evolving from the physical form (FF) factor to the embedded (eSIM) form
- eSIM enables remote provisioning of SIM profiles
- eSIM devices such as Mobile phones use Consumer RSP protocol for download of SIM profiles to the eUICC of a mobile device





Formal Analysis

- ProVerif is a tool for modelling and automatic verification of security goals for cryptographic protocols
- It is symbolic, fully automatic, and supports many cryptographic primitives
- We use model checking technique with ProVerif to verify the expected security goals
- Verified security goals for both ideal and compromised scenarios
- When a security goal fails, we provide provable recommendations to fix it

Achievement

- Model checking for a widely deployed practical security protocol
- Identified several attacks that breaks the expected security goals
- Provable recommendations to improve security of the consumer RSP protocol

Aalto University