Computational Analysis of the UMTS and LTE Authentication and Key Agreement Protocols

Joe-Kai Tsay

Joint work with Stig F. Mjølsnes

8 May 2012, Finse

Context

- GSM & UMTS mobile networks are a worldwide success
  - with now about 6 billion subscriptions
- LTE is forerunner and a main candidate for 4G generation mobile communication system
  - LTE emphasizes the all-IP packet switching design
- The Authentication and Key Agreement (AKA) protocols of these systems arguably the most widely used security protocols

Our Contribution

- First analysis of LTE AKA
- First analysis of UMTS AKA in the computational model
- Analysis conducted with CryptoVerif tool
  - with semantics in the computational model
- Discovery of a flaw in the UMTS & LTE specs
  - Breaks authentication of user to serving network
  - Can be exploited by both an outside and an inside attacker
  - Reported flaw to 3GPP
  - Not known to us whether real-world systems are affected

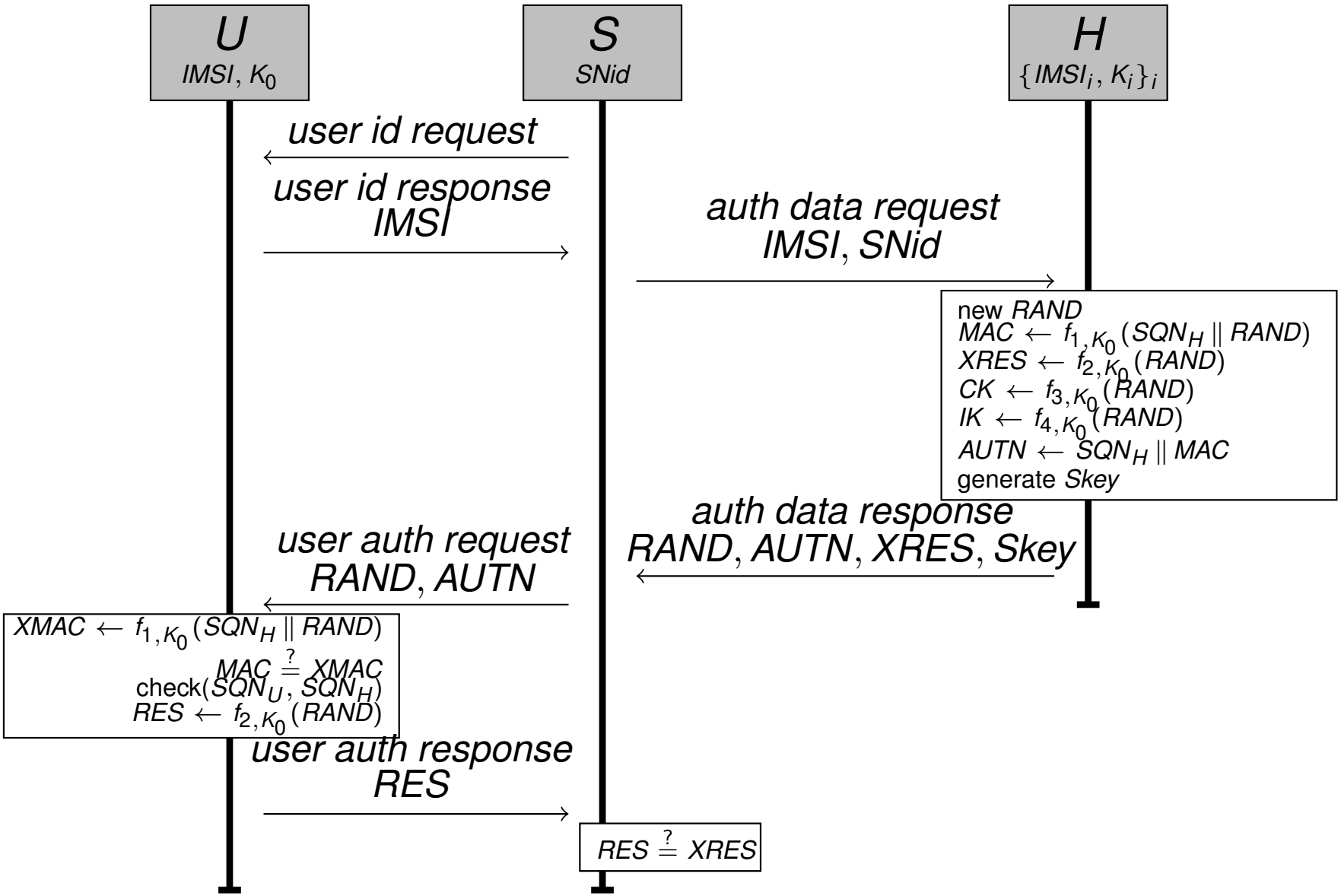
Related Work

- [3GPP TR 133.902] includes a formal analysis of the UMTS AKA protocol using a BAN logic variant.
  - Our flaw is not detected b/c too strong assumptions used
- [MeyerWetzel_Wise'04] shows interoperability of the GSM and UMTS systems permits an attack.
  - We ignore interoperability between LTE/UMTS/GSM.
- [ZhangFang_ IEEETransWirelComm'05] shows a redirection attack on the UMTS AKA
  - Possible b/c user can't verify identity of the *serving* network
    - LTE AKA designed to fix this and implicitly authenticate the serving network to the user.
- [Arapinis et al._arxiv2011] investigates privacy in UMTS
  - Formal analysis with ProVerif tool
  - Attacker can track a user using different error messages
  - They model UMTS AKA as a simplified two-party protocol.
    - This conceals the flaw we found.

UMTS & LTE AKA

- Mainly technical specs TS 33.102 and TS 33.401
- The AKA protocols executed between user U, visited serving network S and U's home network H
- U and H share the long-term key K_0 and a set of algorithms $f_1, \ldots, f_4$ and, in the case of LTE, also a key derivation function KDF
  - f_1, f_2 are so called *message authentication functions*
  - f_3, f_4 are so called *key generating functions*
- Moreover, U maintains a counter SQN_U and H a counter SQN_H for U.

UMTS & LTE AKA messages



Desired Security Properties

Informally, the AKAs should mainly achieve the following

- In UMTS:
  - Authentication of User to Serving Network
  - Agreement on session key $Skey \leftarrow CK \,||\, IK$
- In LTE:
  - Authentication of User to Serving Network
  - Agreement on session key
    $Skey \leftarrow KDF(SQN_H \,||\, CK \,||\, IK \,||\, SNid)$
  - Implicit Authentication of Serving Network to User
    - Session key is computed over S's name
    - $\exists$ session key confirmation step directly following AKA

Communication Protection in Core Network

- Obviously communication between *S* and *H* should be protected somehow
  - Otherwise session key(s) are sent in the clear
  - In GSM, security in core network entirely neglected
- Specs TS 33.210, TS 33.310 detail the protection of IP-based communication
  - distinction between inter-domain communication and *intra-domain* communication
  - Inter-domain connections: specs mandate IPsec.
  - Intra-domain connections: protection up to each operator.
- For UMTS, *S* and *H* can communicate over *global Signaling System No. 7 network*.
  - Specification TS 33.200 details the protection using *Mobile Application Part security* (MAPsec), on the application layer.

Flaw in the UMTS & LTE AKA Specs

- TS 33.210 and TS 33.200: IPsec and MAPsec should offer *data integrity, data origin authentication, anti-replay protection*, and *confidentiality*.
  - In addition, IPsec should offer *limited protection against traffic flow analysis*.
- However, specs not detailed enough w.r.t. to auth data resp from *H* to *S*
  - *S* can't verify for which user an auth data resp was generated
  - Although $\exists$ way of session handling using InvokeID/port numbers in IPsec/MAPsec that prevents attack
- Therefore, *session mix up attacks* are possible!
  - As often, concurrency not sufficiently accounted for
- Found flaw while assuming authenticated encryption between *S* and *H*

Outside Attack

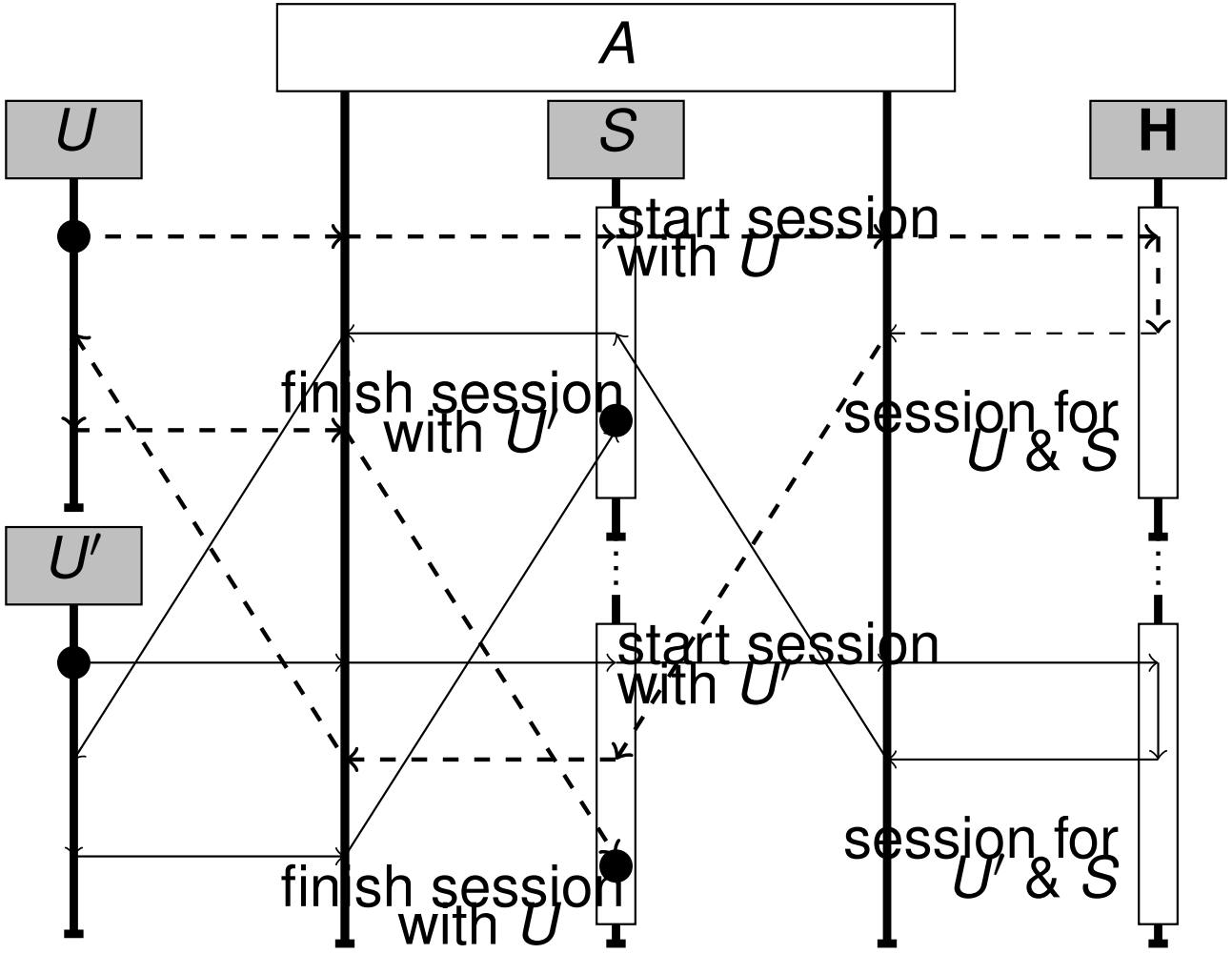


Figure: U is authenticated to S as U' and U' as U.

Inside Attack

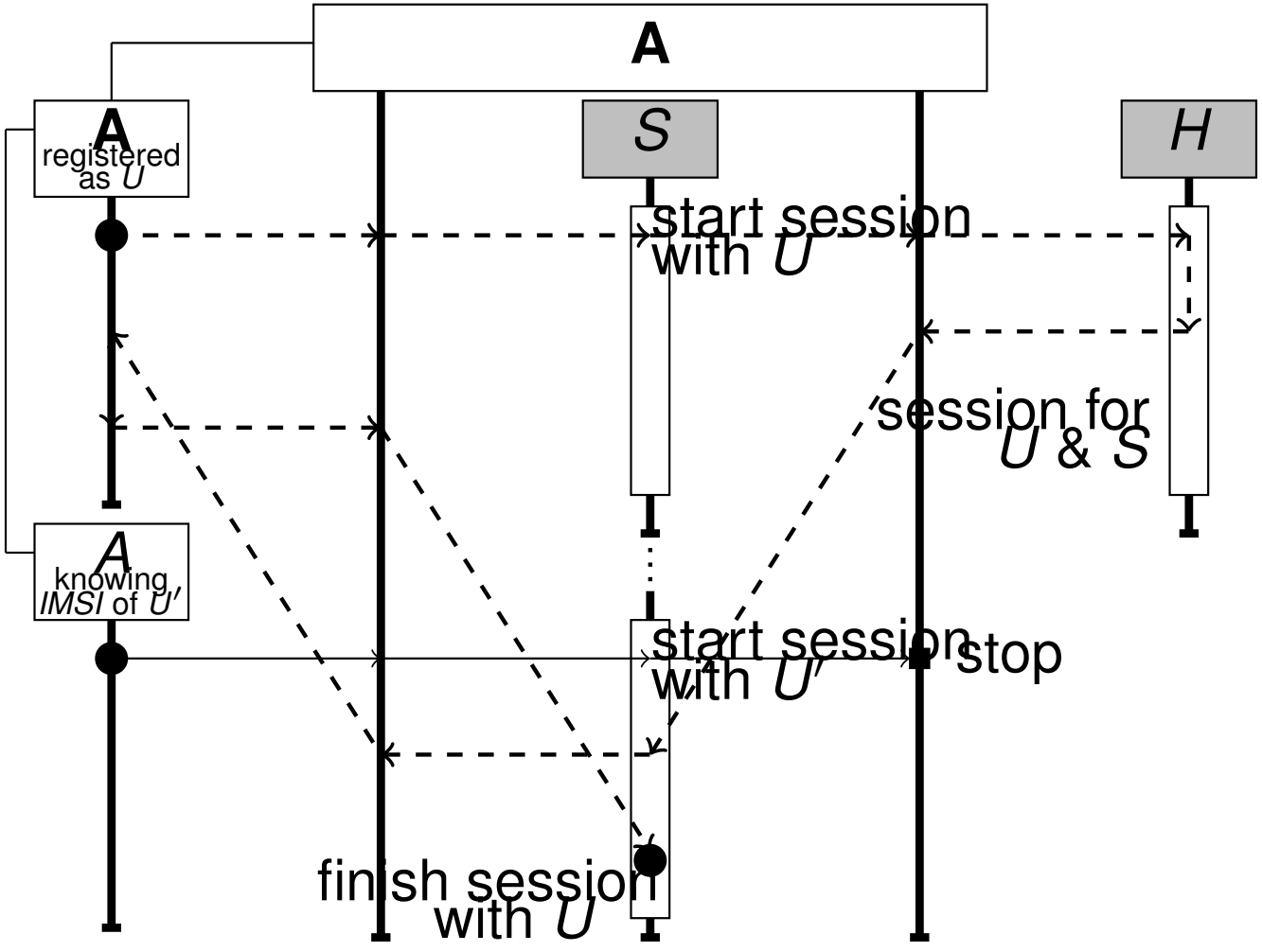


Figure: The attacker impersonates honest user U' to S and shares the session key(s) with S, without U' being involved.

Possible Corrections

Change exchange between S and H

- Adding user ID to data auth resp

$$S \longrightarrow H : IMSI, SNid$$

$$H \longrightarrow S : f(IMSI), RAND, AUTN, XRES, Skey$$

- Alternatively, use sessionID/nonce in challenge-response

$$S \longrightarrow H : n_S, IMSI, SNid$$

$$H \longrightarrow S : f(n_S), RAND, AUTN, XRES, Skey,$$

where n_S is fresh and $f(.)$ is some function computable by S with some injectivity properties (*e.g.* f may be identity or a hash)

CryptoVerif Overview

- Verified both corrected UMTS and LTE AKA using CryptoVerif (CV)
- CV developed by B. Blanchet (with the help of D. Pointcheval)
- CV proofs are sequences of games $Q_0, Q_1, \ldots, Q_n$
  - initial game Q_0 formalizes the protocol for which one wants to prove certain security properties.
  - two consecutive games Q_j and Q_{j+1} are *observationally equivalent*, i.e. computationally indistinguishable for the adversary.
  - in last game Q_n desired security properties are 'obvious'
- CV transforms games by applying the security definition of a cryptographic primitive or by applying syntactic transform's.
- input language is a applied pi calculus variant

CryptoVerif Overview cont'd

- CV can prove secrecy properties and correspondence assertions (i.e authentication properties)
- Given security parameter η, CV proofs are valid for a number of protocol sessions polynomial in η, in the presence of an active adversary
- CV sound but not complete
- CV operates in two modes: a fully automatic and an interactive mode
  - The interactive mode: CV user inputs commands that indicate the main game transformations CV should perform
  - Occasionally, conclude a proof manually by inspecting the last game

Cryptographic Assumptions

- $f_1, \ldots, f_4$ are all based on a single pseudo-random permutation block cipher (as in MILENAGE)
- all f_i in the same run will use the same long-term key (shared betw U and H) but each f_i also uses a constant c_i.
- S shares with H a long-term symmetric encryption key and a long-term message authentication key
  - IPsec and MAPsec must support pre-shared keys, and security associations are assumed static.
  - encrypt-then-mac scheme, with IND-CPA secure enc and WUF-CMA secure mac (this implies INT-PTXT).

Cryptographic Assumptions cont'd

- sequence number is constant and user checks equality.
  - i.e. the protocol in our model lacks replay-attack protection.
- In LTE AKA, the key derivation function is a pseudo-random function which outputs a key seed to generate a message authentication key.
  - This key seed is then used to generate the session key

Summary of Results

- We verified key secrecy and authentication properties for UMTS, LTE and LTE with the additional key confirmation exchange
  - Indistinguishability from random of the UMTS and LTE session keys that *S* holds
  - Entity Authentication of User to *S* in UMTS and LTE
  - Entity Authentication of *S* to User for LTE with additional key confirm. exchange
    - but lose key secrecy property
- Proofs mostly using CV interactive mode, and often concluded by inspection of the last CV game

Key Secrecy

Theorem (Key Secrecy in UMTS/LTE AKA)

Let Q_{UMTS} (Q_{LTE}) be the game in CryptoVerifs process calculus formalizing the corrected UMTS AKA (corrected LTE AKA). Furthermore, let keyS1 and keyS2 (keyS) denote in Q_{UMTS} (Q_{LTE}) the confidentiality key CK and, respectively, the integrity key IK (the session key K_{ASME}) that are (is) received by an honest serving network from the home network and generated by the home network for the use between the serving network and an honest user. Then Q_{UMTS} (Q_{LTE}) preserves the one-session secrecy of keyS1 and keyS2 (keyS).

Theorem (Entity Authentication of User to Serving Network)

In the corrected UMTS and LTE AKA, if there is an instance of

- *an honest serving network S completing a run of the corrected UMTS/LTE AKA with honest user equipment U and home network H*
- *in which S received a value $RAND'$ as nonce and a value $XRES'$ as expected response from H in a authentication data response*
- *and in which S received a value RES' in a user authentication response that equals $XRES'$*

then, with overwhelming probability, there is an instance of

- *H completing a data authentication transfer with S*
- *in which H generated a nonce RAND and an expected response XRES for the use between S and U, where $RAND'$ equals RAND and $XRES'$ equals XRES*

and an instance of

- *U completing a run of the corrected UMTS/LTE AKA*
- *in which U received a value $RAND''$ as nonce in a user authentication request that is equal to $RAND'$*
- *and in which U sent a response RES'' that equals $XRES'$.*

Conclusions

- First analysis of UMTS and LTE AKA in the computational model
- Discovered new flaw in UMTS and LTE AKA specs!
  - It's a logical flaw (i.e. on the symbolic level)
- Not clear yet, if current real systems are affected.
  - we are currently trying to find out
- Protocol specs need to be corrected
- We provide security proofs with CryptoVerif tool for corrected protocols

Thanks!