Automated Protocol Verification

Computer Security and Networks

Eike Ritter

University of Birmingham

The material in this lecture is not relevant for the exam

The Applied Pi Calculus

Want formal languages to model security protocols so that automatic verification can be done

Here: use Applied Pi-Calculus, a suitable adaptation of process calculi

Intuition:

Processes correspond to agents (Alice, Bob, Mallory etc.)

Sending messages modelled as communication in process calculus

Attacker modelled as arbitrary process which runs in parallel with processes modelling Alice and Bob

Applied pi calculus: Grammar

Terms

$$
\begin{array}{ll}
M, N ::= & \\
\quad a, b, c, k, m, n, s, t, r, \ldots & \text{name} \\
\quad x, y, z & \text{variable} \\
\quad g(M_1, \ldots, M_l) & \text{function}
\end{array}
$$

Equational theory

$$
\begin{array}{rcl}
\mathrm{adec}(\mathrm{aenc}(x, pk(y)), y) & = & x \\
\mathrm{fst}((x, y)) & = & x \\
\mathrm{snd}((x, y)) & = & y
\end{array}
$$

Applied pi calculus: Grammar

Processes

$P, Q, R ::=$	processes
0	null process
$P \mid Q$	parallel comp.
$!P$	replication
$\text{new } n.P$	name restriction
$\text{in}(u, x).P$	message input
$\text{out}(u, M).P$	message output
$\text{if } M = N \text{ then } P \text{ else } Q$	cond'nl

Proverif

Several tools available for automated verification

Consider a tool called Proverif (Blanchet 2001)

Capabilities of ProVerif:

- Reachability properties: Is a certain event reachable (eg leaking secret keys to the attacker)
- Correspondence assertions: If event e has been executed, then event e' has been previously been executed
- Observational equivalences: The attacker cannot identify which one of two processes has been executed

  Example:

  Process 1: Voter A chooses option 1, voter B chooses option 2

  Process 2: Voter A chooses option 2, voter B chooses option 1

Demo

Privacy in Mobile Telephony Systems

Based on a paper in Network and Distributed Systems Symposium 2014 by Arapinis, Mancini, Ritter and Ryan

Mobile phone communication

- Mobile phones are carried by large parts of the population most of the time
- Wireless communication always on
- Emitting their identity
- Answer without agreement of their bearers

Previous work on security of mobile phones

Content security, Integrity and Authentication

- Weaknesses in cryptographic algorithms used (Biryutov et al. 2000)
- Eavesdropping on mobile communication (Nohl et al. 2010)
- Weaknesses in the authentication and key agreement protocol (Ahamdian et al. 2009, Arapinis et al. 2012)

Privacy

- use paging procedure to locate mobile phone users (Foo Kune et al. 2012)
- IMSI-catchers: force mobile phone to reveal identity (recognised weakness in the standard)

Mobile phone privacy

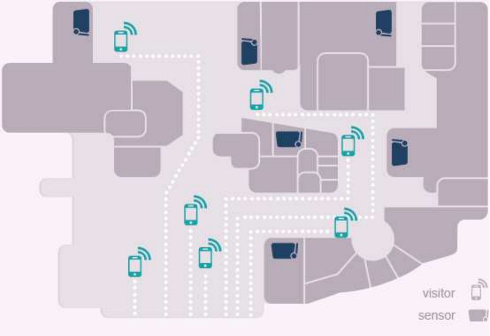
Privacy is explicit goal of UMTS standard:

UMTS specification [3GPP TS 33.102 V9.3.0 (2010-10)]

An intruder cannot deduce whether different services are delivered to the same user.

Tracking via mobile phones

- Tracking of mobile phone user done in reality
- Example: Market research companies use signal strength to track customers (eg. Smart Flow)



- anonymous, but linkable.
- No consent of mobile phone owner.

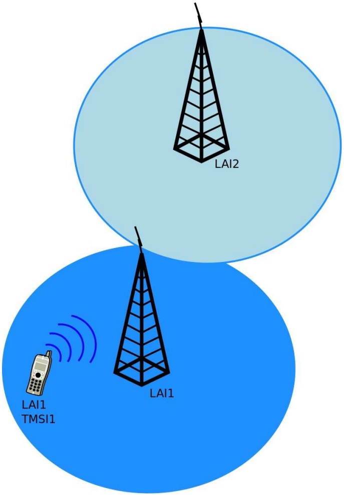
Mobile phone identifiers

- Every phone has unique identifier (IMSI)
- If IMSI appears in cleartext, identification of mobile phone user would be easily possible
- Problem recognised in the UMTS standard
- temporary identifiers (TMSI) used which should be changed periodically

Talk is about correct usage of TMSIs.

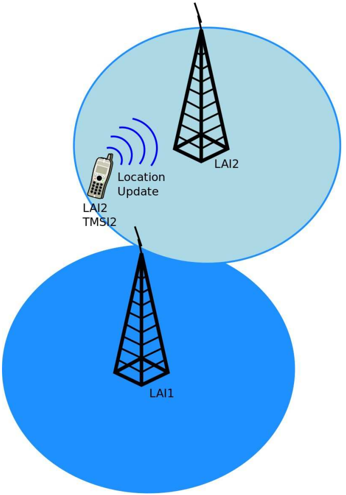
TMSI reallocation

- Initiated by the MS to update its location
- MS unique identity stored in the SIM card: IMSI
- The network assigns a temporary identity TMSI
- A new TMSI is assigned during the location update



TMSI reallocation

- Initiated by the MS to update its location
- MS unique identity stored in the SIM card: IMSI
- The network assigns a temporary identity TMSI
- A new TMSI is assigned during the location update



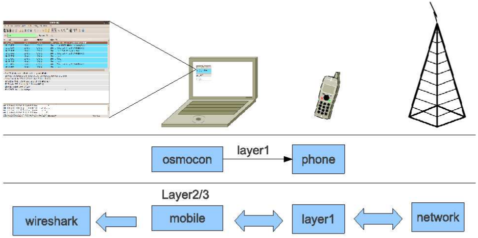
Problems with TMSI reallocation

1. TMSI reallocation rarely executed:
   Experimentally verified
2. Old keys for encrypting traffic are reused after TMSI-reallocation
   Gives rise to protocol attack

Both issues make it possible to track mobile phone users

Experimental Setup

- Osmocom-BB project implements GSM mobile station controlled by host
- Radio communication executed via flashed firmware on mobile phone
- Can use wireshark to analyse the communication



Experimental Setup, continued

Experimental results

TMSI reallocation procedure rarely executed:
Same TMSI allocated for hours and even days
Observed for major operators in UK, France, Italy and Greece

No.	Time	Source	Destination	Protocol	Info
1	2012-03-22 09:11:11.56498300	127.0.(	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
2	2012-03-22 09:11:12.02491000	127.0.(	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
3	2012-03-22 09:11:12.26095700	127.0.(	127.0.0.1	LAPDm	I, N(R)=0, N(S)=0(DTAP) (MM) Authentication Request
4	2012-03-22 09:11:12.64896900	127.0.(	127.0.0.1	LAPDm	I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Response
5	2012-03-22 09:11:13.43687500	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) TMSI Reallocation Command
6	2012-03-22 09:11:13.43692200	127.0.(	127.0.0.1	LAPDm	I, N(R)=3, N(S)=2(DTAP) (MM) TMSI Reallocation Complete
7	2012-03-22 09:11:14.14486500	127.0.(	127.0.0.1	LAPDm	I, N(R)=3, N(S)=3(DTAP) (MM) Location Updating Accept

```
▼ GSM A-I/F DTAP - TMSI Reallocation Command
  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..01 1010 = DTAP Mobility Management Message Type: TMSI Reallocation Command (0x1a)
  ▶ Location Area Identification (LAI)
  ▶ Mobile Identity - TMSI/P-TMSI (0xb42c2fdd)
```

No.	Time	Source	Destination	Protocol	Info
118	2012-03-25 10:24:17.50371100	127.0.(	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
119	2012-03-25 10:24:17.73977300	127.0.(	127.0.0.1	LAPDm	I, N(R)=0, N(S)=0(DTAP) (MM) Authentication Request
120	2012-03-25 10:24:18.14352900	127.0.(	127.0.0.1	LAPDm	I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Response
121	2012-03-25 10:24:18.91581700	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept

```
▶ Link Access Procedure, Channel Dm (LAPDm)
▼ GSM A-I/F DTAP - Location Updating Request
  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..00 1000 = DTAP Mobility Management Message Type: Location Updating Request (0x08)
  ▶ Ciphering Key Sequence Number
  ▶ Location Updating Type - IMSI attach
  ▶ Location Area Identification (LAI)
  ▶ Mobile Station Classmark 1
  ▶ Mobile Identity - TMSI/P-TMSI (0xb42c2fdd)
```

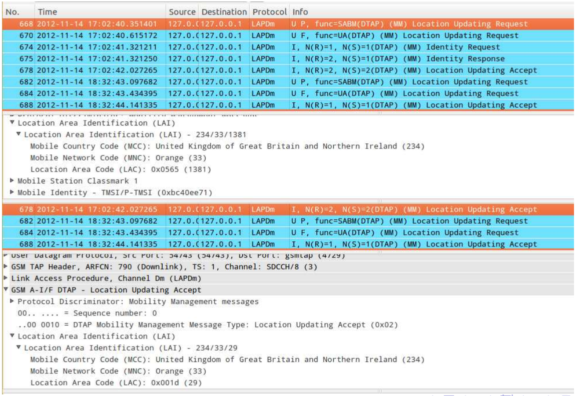
Experimental results, continued

Change of location area does not imply a change of TMSI

Example: couch journey between different cities in the UK

- First new TMSI assigned after about 45 min (53km)
- Second new TMSI assigned after about 60 min (70km)

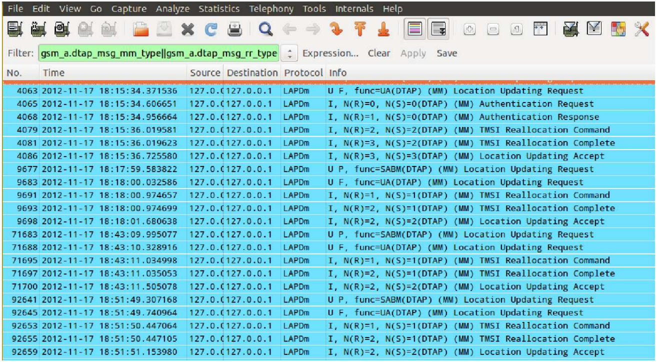
However: location update procedure performed every 5 min (3km)



Reuse of previous ciphering keys

Previously established keys are used for the TMSI reallocation procedure

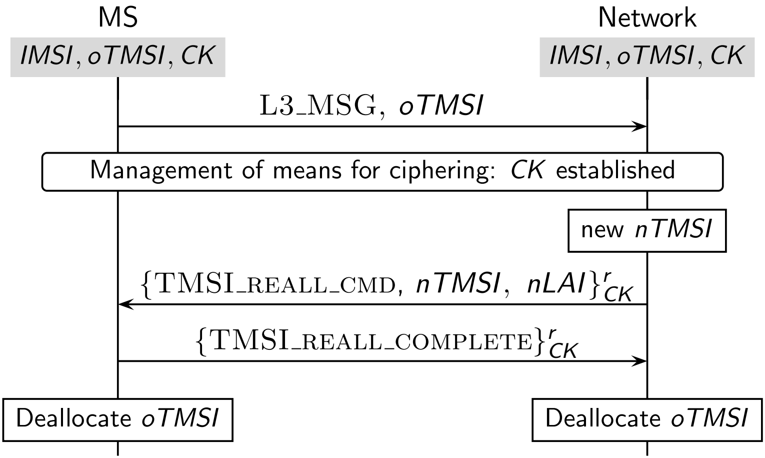
Observed for major UK and Italian network operators



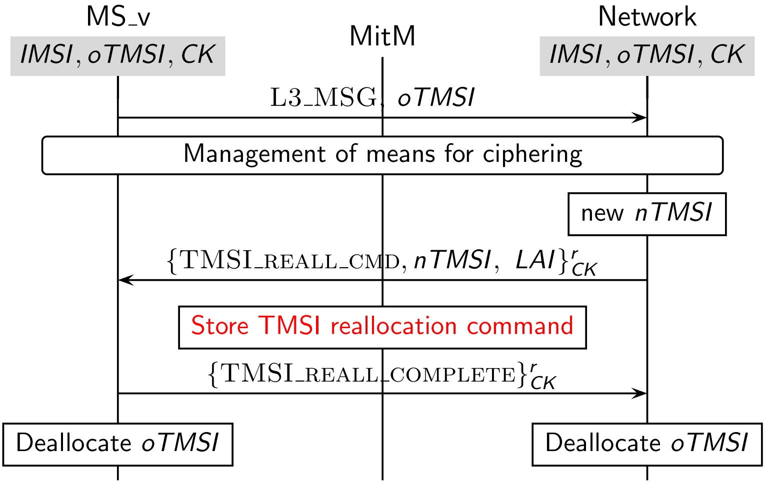
No.	Time	Source	Destination	Protocol	Info
4063	2012-11-17 18:15:34.371536	127.0.(	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
4065	2012-11-17 18:15:34.606651	127.0.(	127.0.0.1	LAPDm	I, N(R)=0, N(S)=0(DTAP) (MM) Authentication Request
4068	2012-11-17 18:15:34.956664	127.0.(	127.0.0.1	LAPDm	I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Response
4079	2012-11-17 18:15:36.019581	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) TMSI Reallocation Command
4081	2012-11-17 18:15:36.019623	127.0.(	127.0.0.1	LAPDm	I, N(R)=3, N(S)=2(DTAP) (MM) TMSI Reallocation Complete
4086	2012-11-17 18:15:36.725580	127.0.(	127.0.0.1	LAPDm	I, N(R)=3, N(S)=3(DTAP) (MM) Location Updating Accept
9677	2012-11-17 18:17:59.583822	127.0.(	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
9683	2012-11-17 18:18:00.032586	127.0.(	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
9691	2012-11-17 18:18:00.974657	127.0.(	127.0.0.1	LAPDm	I, N(R)=1, N(S)=1(DTAP) (MM) TMSI Reallocation Command
9693	2012-11-17 18:18:00.974699	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=1(DTAP) (MM) TMSI Reallocation Complete
9698	2012-11-17 18:18:01.680638	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept
71683	2012-11-17 18:43:09.995077	127.0.(	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
71688	2012-11-17 18:43:10.328916	127.0.(	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
71695	2012-11-17 18:43:11.034998	127.0.(	127.0.0.1	LAPDm	I, N(R)=1, N(S)=1(DTAP) (MM) TMSI Reallocation Command
71697	2012-11-17 18:43:11.035053	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=1(DTAP) (MM) TMSI Reallocation Complete
71700	2012-11-17 18:43:11.505078	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept
92641	2012-11-17 18:51:49.307168	127.0.(	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
92645	2012-11-17 18:51:49.740964	127.0.(	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
92653	2012-11-17 18:51:50.447064	127.0.(	127.0.0.1	LAPDm	I, N(R)=1, N(S)=1(DTAP) (MM) TMSI Reallocation Command
92655	2012-11-17 18:51:50.447105	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=1(DTAP) (MM) TMSI Reallocation Complete
92659	2012-11-17 18:51:51.153980	127.0.(	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept

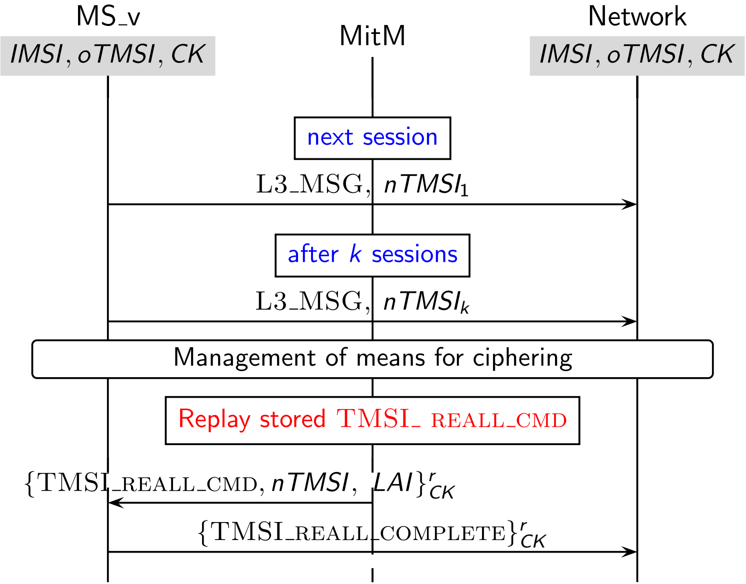
Gives rise to replay attack

TMSI reallocation protocol

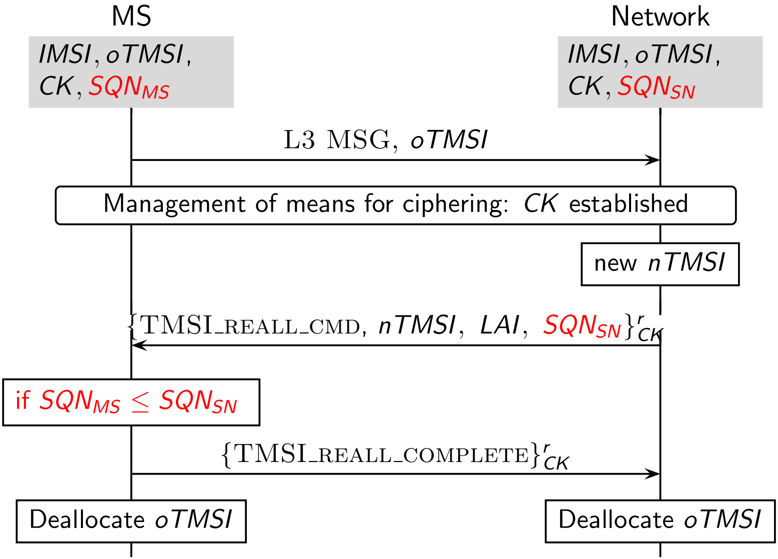


Replay Attack




MS_v
IMSI, oTMSI, CK
MitM
Network
IMSI, oTMSI, CK
next session
L3_MSG, nTMSI_1
after k sessions
L3_MSG, nTMSI_k
Management of means for ciphering
Replay stored TMSI_REALL_CMD
{TMSI_REALL_CMD, nTMSI, LAI}^r_CK
{TMSI_REALL_COMPLETE}^r_CK

Fix for replay attack

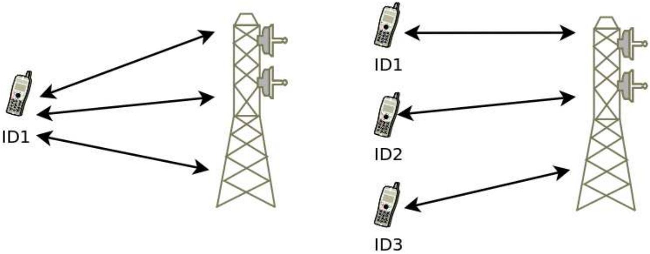


Privacy properties of fix

Have formally specified and verified privacy properties of fix
Applied π-calculus used for formalisation

- Agents modelled as processes
- communication between agents modelled as messages on channels
- have terms and reduction rules corresponding to cryptographic primitives
- nonces and private keys modelled by scope restriction of identifiers

Desired privacy property formalised as unlinkability: Attacker cannot distinguish two scenarios



Formally:

$$\nu dck.(!(Init|MS)|!SN) \approx \nu dck.(!(Init|!MS)|!SN)$$

Have automated tool (Proverif) to verify such equivalences

Modelling TMSI

Issue: How to handle TMSI (stored in phone memory)?

- Instance of global mutable state
- Encoding of state in applied π-calculus leads to large amount of false positives in Proverif

Solution: add mutalbe global state as primitive
Leads to StatVerif

Have shown following theorem

Theorem

$$\nu dck.(!(Init|MS)|!SN) \approx \nu dck.(!(Init|!MS)|!SN)$$

Proof works by constructing suitable bisimulation
Key point: multiple sessions of same mobile phone can be simulated by multiple phones executing one session each

Conclusions

Temporary identifiers used by mobile phones are used incorrectly

- changed rarely
- old ciphering keys are reused

Weaknesses make it possible to track mobile phone users

Second problem can be fixed by not reusing keys