Privacy through Pseudonymity in Mobile Telephony Systems

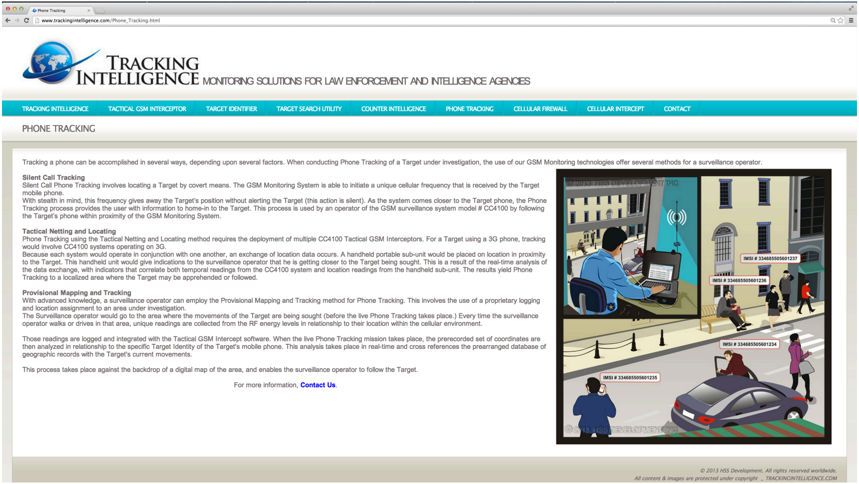
Myrto Arapinis [1] Loretta Mancini [2] Eike Ritter [2] Mark Ryan [2]

[1]School of Informatics, University of Edinburgh
[2]School of Computer Science, University of Birmingham

NDSS 2014

Context

Law enforcement agencies track individuals



PHONE TRACKING

Tracking a phone can be accomplished in several ways, depending upon several factors. When conducting Phone Tracking of a Target under investigation, the use of our GSM Monitoring technologies offer several methods for a surveillance operator.

Silent Call Tracking
Silent Call Phone Tracking involves locating a Target by covert means. The GSM Monitoring System is able to initiate a unique cellular frequency that is received by the Target mobile phone.
With stealth in mind, this frequency gives away the Target's position without alerting the Target (this action is silent). As the system comes closer to the Target phone, the Phone Tracking process provides the user with information to home-in to the Target. This process is used by an operator of the GSM surveillance system model # CC4100 by following the Target's phone within proximity of the GSM Monitoring System.

Tactical Netting and Locating
Phone Tracking using the Tactical Netting and Locating method requires the deployment of multiple CC4100 Tactical GSM Interceptors. For a Target using a 3G phone, tracking would involve CC4100 systems operating on 3G.
Because each system would operate in conjunction with one another, an exchange of location data occurs. A handheld portable sub-unit would be placed on location in proximity to the Target. This handheld unit would give indications to the surveillance operator that he is getting closer to the Target being sought. This is a result of the real-time analysis of the data exchange, with indicators that correlate both temporal readings from the CC4100 system and location readings from the handheld sub-unit. The results yield Phone Tracking to a localized area where the Target may be apprehended or followed.

Provisional Mapping and Tracking
With advanced knowledge, a surveillance operator can employ the Provisional Mapping and Tracking method for Phone Tracking. This involves the use of a proprietary logging and location assignment to an area under investigation.
The Surveillance operator would go to the area where the movements of the Target are being sought (before the live Phone Tracking takes place.) Every time the surveillance operator walks or drives in that area, unique readings are collected from the RF energy levels in relationship to their location within the cellular environment.

Those readings are logged and integrated with the Tactical GSM Intercept software. When the live Phone Tracking mission takes place, the prerecorded set of coordinates are then analyzed in relationship to the specific Target Identity of the Target's mobile phone. This analysis takes place in real-time and cross references the prearranged database of geographic records with the Target's current movements.

This process takes place against the backdrop of a digital map of the area, and enables the surveillance operator to follow the Target.

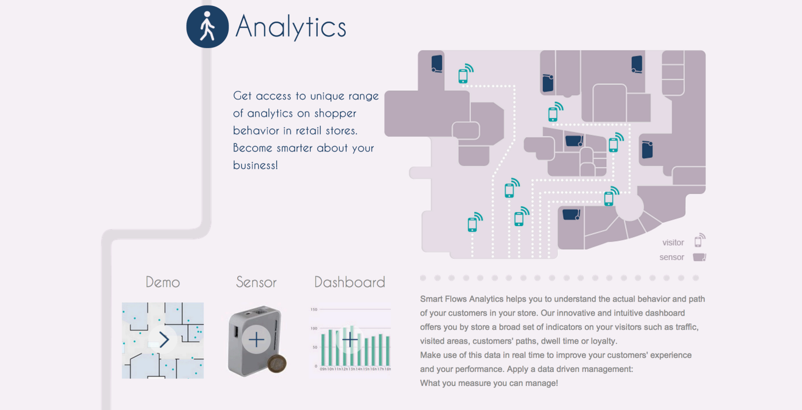
For more information, **Contact Us**.

But also...

- private detectives, jealous partners, abusive bosses, nosy neighbors, . . .

But also...

- private detectives, jealous partners, abusive bosses, nosy neighbors, . . .
- retailers, shopping malls, airports, railway stations, museums, public areas, . . .



Analytics

Get access to unique range of analytics on shopper behavior in retail stores. Become smarter about your business!

Smart Flows Analytics helps you to understand the actual behavior and path of your customers in your store. Our innovative and intuitive dashboard offers you by store a broad set of indicators on your visitors such as traffic, visited areas, customers' paths, dwell time or loyalty.
Make use of this data in real time to improve your customers' experience and your performance. Apply a data driven management:
What you measure you can manage!

Privacy and the GSM/UMTS standards

Privacy is an explicit goal of GSM/UMTS

GSM/UMTS aim at providing user untraceability from third parties

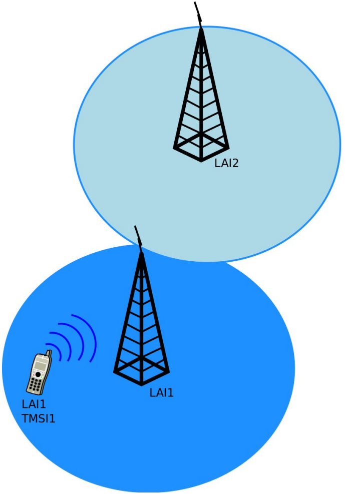
GSM/UMTS specification [3GPP TS 33.102 V9.3.0 (2010-10)]

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

⟶ the user is identified by a **pseudonym/temporary identity (TMSI)** which should be **periodically updated**.

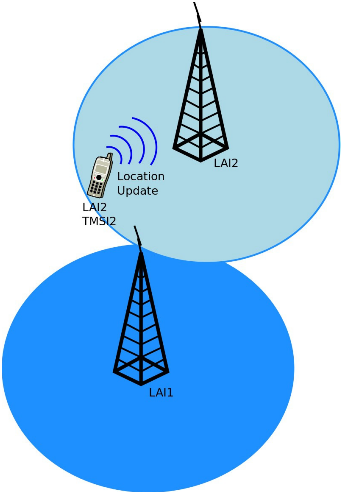
TMSI reallocation in the GSM/UMTS standards

- 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 should be assigned at each change of location



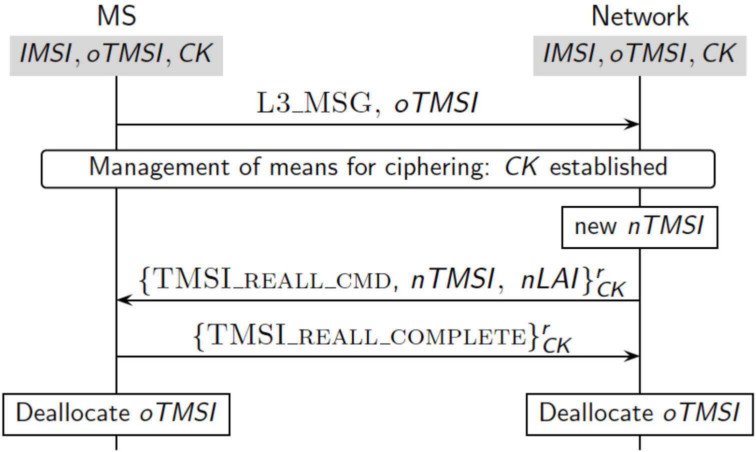
TMSI reallocation in the GSM/UMTS standards

- 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 should be assigned at each change of location



Analysis of TMSI reallocation

TMSI reallocation procedure



MS

$IMSI, oTMSI, CK$

Network

$IMSI, oTMSI, CK$

$\mathrm{L3\_MSG},\ oTMSI$

Management of means for ciphering: CK established

new $nTMSI$

$\{\mathrm{TMSI\_\textsc{reall\_cmd}},\ nTMSI,\ nLAI\}^{r}_{CK}$

$\{\mathrm{TMSI\_\textsc{reall\_complete}}\}^{r}_{CK}$

Deallocate $oTMSI$

Deallocate $oTMSI$

Our focus: correct usage of TMSIs

Does TMSI reallocation really achieve privacy?

Our focus: correct usage of TMSIs

Does TMSI reallocation really achieve privacy?

- What does periodically mean?

Our focus: correct usage of TMSIs

Does TMSI reallocation really achieve privacy?

- What does periodically mean?
- Is a new TMSI assigned at each change of location as the standard specifies?

Our focus: correct usage of TMSIs

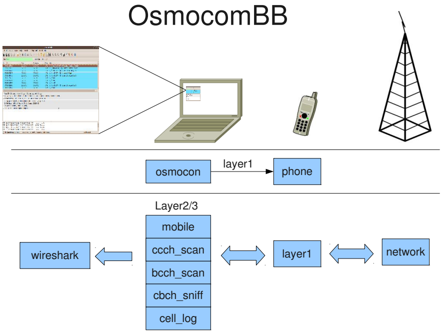
Does TMSI reallocation really achieve privacy?

- What does periodically mean?
- Is a new TMSI assigned at each change of location as the standard specifies?
- Are session keys reused?

Experimental setup

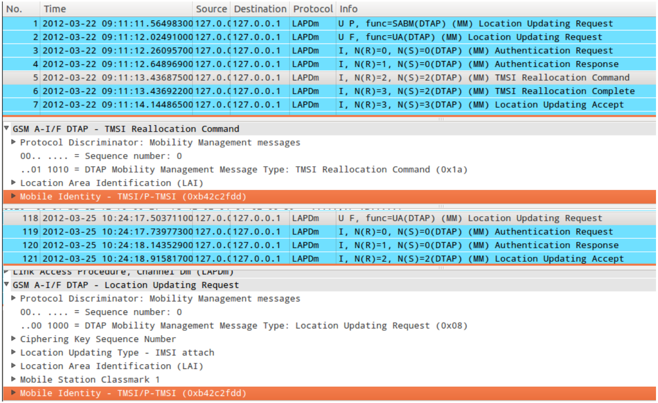
Experimental setup

- 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



TMSI reallocation procedure rarely executed

- same TMSI allocated for hours and even days,
- independently of MS activity



```
No.  Time                          Source   Destination  Protocol  Info
  1  2012-03-22 09:11:11.56498300  127.0.0  127.0.0.1    LAPDm     U P, func=SABM(DTAP) (MM) Location Updating Request
  2  2012-03-22 09:11:12.02491000  127.0.0  127.0.0.1    LAPDm     U F, func=UA(DTAP) (MM) Location Updating Request
  3  2012-03-22 09:11:12.26095700  127.0.0  127.0.0.1    LAPDm     I, N(R)=0, N(S)=0(DTAP) (MM) Authentication Request
  4  2012-03-22 09:11:12.64896900  127.0.0  127.0.0.1    LAPDm     I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Response
  5  2012-03-22 09:11:13.43687500  127.0.0  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  127.0.0  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  127.0.0  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)

118  2012-03-25 10:24:17.50371100  127.0.0  127.0.0.1    LAPDm     U F, func=UA(DTAP) (MM) Location Updating Request
119  2012-03-25 10:24:17.73977300  127.0.0  127.0.0.1    LAPDm     I, N(R)=0, N(S)=0(DTAP) (MM) Authentication Request
120  2012-03-25 10:24:18.14352900  127.0.0  127.0.0.1    LAPDm     I, N(R)=1, N(S)=0(DTAP) (MM) Authentication Response
121  2012-03-25 10:24:18.91581700  127.0.0  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)
```

Observed for major operators in UK, France, Italy and Greece

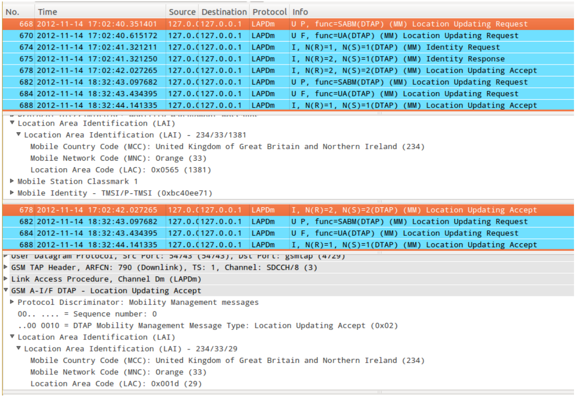
Change of location without TMSI reallocation

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)



No.	Time	Source	Destination	Protocol	Info
668	2012-11-14 17:02:40.351401	127.0.0	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
670	2012-11-14 17:02:40.615172	127.0.0	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
674	2012-11-14 17:02:41.321211	127.0.0	127.0.0.1	LAPDm	I, N(R)=1, N(S)=1(DTAP) (MM) Identity Request
675	2012-11-14 17:02:41.321250	127.0.0	127.0.0.1	LAPDm	I, N(R)=2, N(S)=1(DTAP) (MM) Identity Response
678	2012-11-14 17:02:42.027265	127.0.0	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept
682	2012-11-14 18:32:43.097682	127.0.0	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
684	2012-11-14 18:32:43.434395	127.0.0	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
688	2012-11-14 18:32:44.141335	127.0.0	127.0.0.1	LAPDm	I, N(R)=1, N(S)=1(DTAP) (MM) Location Updating Accept

```
▼ Location Area Identification (LAI)
  ▼ Location Area Identification (LAI) - 234/33/1381
      Mobile Country Code (MCC): United Kingdom of Great Britain and Northern Ireland (234)
      Mobile Network Code (MNC): Orange (33)
      Location Area Code (LAC): 0x0565 (1381)
▶ Mobile Station Classmark 1
▶ Mobile Identity - TMSI/P-TMSI (0xbc40ee71)
```

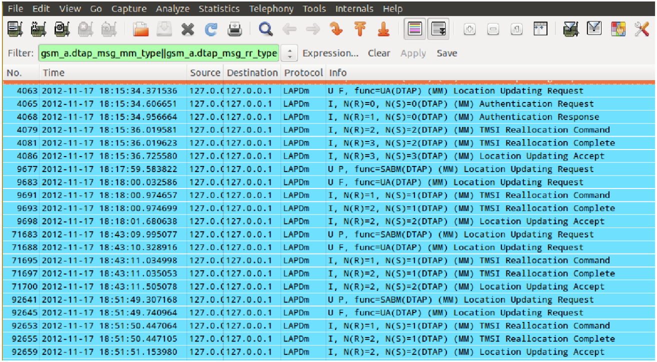
678	2012-11-14 17:02:42.027265	127.0.0	127.0.0.1	LAPDm	I, N(R)=2, N(S)=2(DTAP) (MM) Location Updating Accept
682	2012-11-14 18:32:43.097682	127.0.0	127.0.0.1	LAPDm	U P, func=SABM(DTAP) (MM) Location Updating Request
684	2012-11-14 18:32:43.434395	127.0.0	127.0.0.1	LAPDm	U F, func=UA(DTAP) (MM) Location Updating Request
688	2012-11-14 18:32:44.141335	127.0.0	127.0.0.1	LAPDm	I, N(R)=1, N(S)=1(DTAP) (MM) Location Updating Accept

```
▶ User Datagram Protocol, Src Port: 54743 (54743), Dst Port: gsmtap (4729)
▶ GSM TAP Header, ARFCN: 790 (Downlink), TS: 1, Channel: SDCCH/8 (3)
▶ Link Access Procedure, Channel Dm (LAPDm)
▼ GSM A-I/F DTAP - Location Updating Accept
  ▶ Protocol Discriminator: Mobility Management messages
    00.. .... = Sequence number: 0
    ..00 0010 = DTAP Mobility Management Message Type: Location Updating Accept (0x02)
  ▼ Location Area Identification (LAI)
    ▼ Location Area Identification (LAI) - 234/33/29
        Mobile Country Code (MCC): United Kingdom of Great Britain and Northern Ireland (234)
        Mobile Network Code (MNC): Orange (33)
        Location Area Code (LAC): 0x001d (29)
```

Reuse of previous ciphering keys

Previously established keys are reused for TMSI reallocation

Observed for major UK and Italian network operators

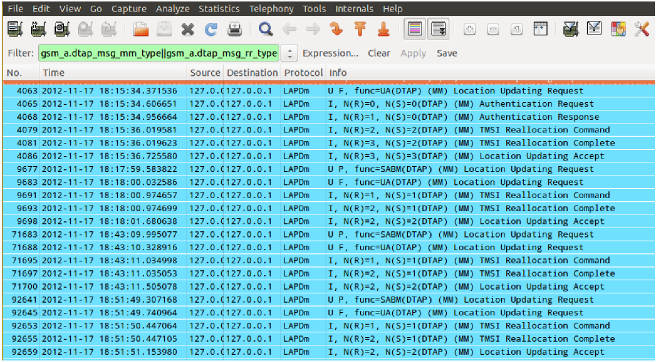


Filter: gsm_a.dtap_msg_mm_type||gsm_a.dtap_msg_rr_type

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

Reuse of previous ciphering keys

Previously established keys are reused for TMSI reallocation
Observed for major UK and Italian network operators



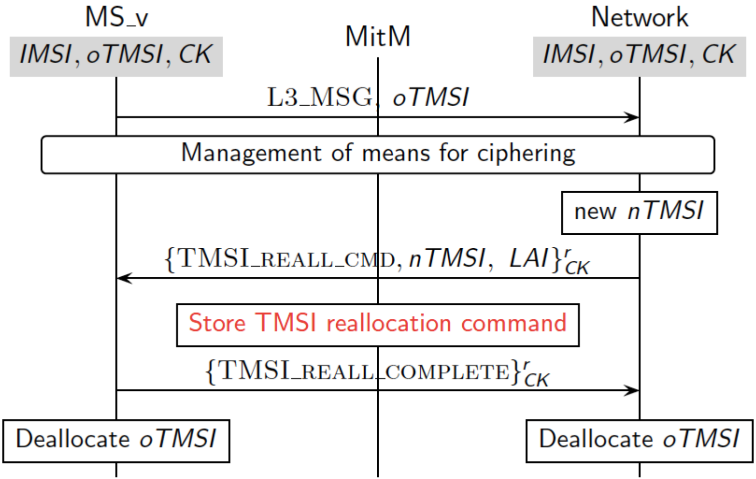
Filter: gsm_a.dtap_msg_mm_type||gsm_a.dtap_msg_rr_type

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

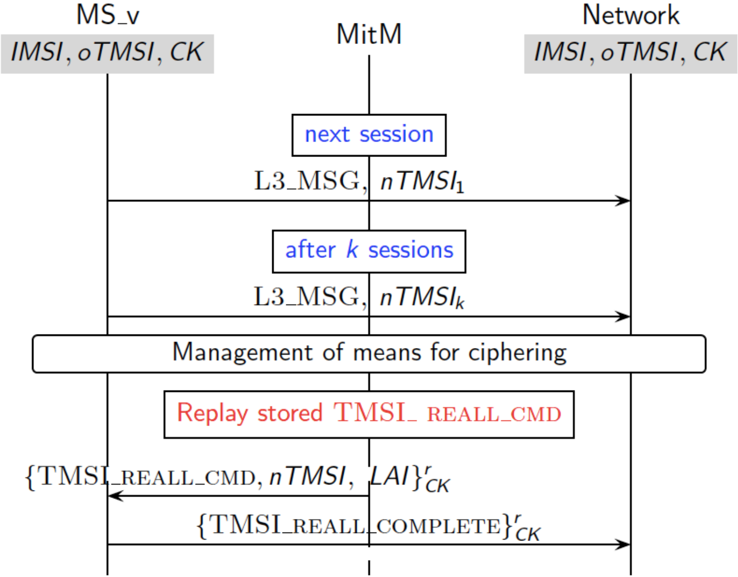
⇒ Gives rise to replay attack

Replay attack and fix

TMSI reallocation replay attack (1)


MS_v
$IMSI, oTMSI, CK$
MitM
Network
$IMSI, oTMSI, CK$
$\text{L3\_MSG}, oTMSI$
Management of means for ciphering
new $nTMSI$
$\{\text{TMSI\_REALL\_CMD}, nTMSI, LAI\}^r_{CK}$
Store TMSI reallocation command
$\{\text{TMSI\_REALL\_COMPLETE}\}^r_{CK}$
Deallocate $oTMSI$
Deallocate $oTMSI$

TMSI reallocation replay attack (2)



MS_v

$IMSI, oTMSI, CK$

MitM

Network

$IMSI, oTMSI, CK$

next session

$\mathrm{L3\_MSG}, nTMSI_1$

after k sessions

$\mathrm{L3\_MSG}, nTMSI_k$

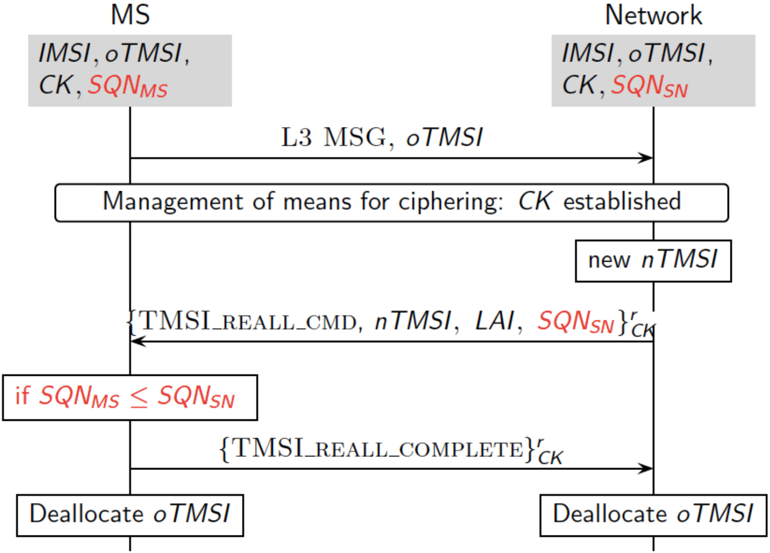
Management of means for ciphering

Replay stored $\mathrm{TMSI\_}$ $\textsc{reall\_cmd}$

$\{\mathrm{TMSI\_}\textsc{reall\_cmd}, nTMSI, LAI\}^r_{CK}$

$\{\mathrm{TMSI\_}\textsc{reall\_complete}\}^r_{CK}$

Fix for replay attack



MS

$IMSI, oTMSI,$
CK, SQN_{MS}

Network

$IMSI, oTMSI,$
CK, SQN_{SN}

L3 MSG, $oTMSI$

Management of means for ciphering: CK established

new $nTMSI$

$\{\text{TMSI\_REALL\_CMD}, nTMSI, LAI, SQN_{SN}\}^{r}_{CK}$

if $SQN_{MS} \leq SQN_{SN}$

$\{\text{TMSI\_REALL\_COMPLETE}\}^{r}_{CK}$

Deallocate $oTMSI$

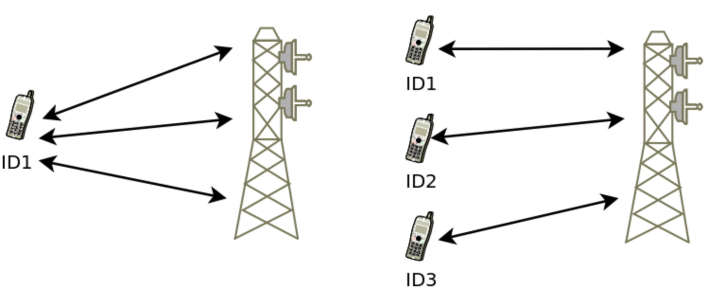
Deallocate $oTMSI$

Unlinkability

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

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

An attacker cannot distinguish two scenarios



Fixed TMSI reallocation satisfies unlinkability

- **Formal model of fixed TMSI reallocation procedure** in the applied pi calculus

- **Formal proof of unlinkability**

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

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

Conclusion

Summary of our results

- What does periodically mean?

- Is a new TMSI assigned at each change of location as the standard specifies?

- Are session keys reused?

[1]

Summary of our results

- What does periodically mean? RARELY
  ⇒ locate a victim by paging it[1]

- Is a new TMSI assigned at each change of location as the standard specifies?

- Are session keys reused?

[1] D. F. Kune et al. *Location leaks over the GSM air interface*, NDSS, 2012. K. Nohl and S. Munaut, *Wideband gsm sniffing*, 27C3, 2010.

Summary of our results

- What does periodically mean? RARELY

  ⇒ locate a victim by paging it[1]

  ⇒ TMSI reallocation should be activity dependent

- Is a new TMSI assigned at each change of location as the standard specifies?

- Are session keys reused?

[1] D. F. Kune et al. *Location leaks over the GSM air interface*, NDSS, 2012.
K. Nohl and S. Munaut, *Wideband gsm sniffing*, 27C3, 2010.

Summary of our results

- What does periodically mean? RARELY

  ⇒ locate a victim by paging it[1]

  ⇒ TMSI reallocation should be activity dependent

- Is a new TMSI assigned at each change of location as the standard specifies? NO

  ⇒ tracking across different locations by passively sniffing

- Are session keys reused?

[1] D. F. Kune et al. *Location leaks over the GSM air interface*, NDSS, 2012.
K. Nohl and S. Munaut, *Wideband gsm sniffing*, 27C3, 2010.

Summary of our results

- What does periodically mean? RARELY

  ⇒ locate a victim by paging it[1]

  ⇒ TMSI reallocation should be activity dependent

- Is a new TMSI assigned at each change of location as the standard specifies? NO

  ⇒ tracking across different locations by passively sniffing

  ⇒ TMSI reallocation should be executed at each change of location

- Are session keys reused?

[1] D. F. Kune et al. *Location leaks over the GSM air interface*, NDSS, 2012.
K. Nohl and S. Munaut, *Wideband gsm sniffing*, 27C3, 2010.

Summary of our results

- What does periodically mean? RARELY

  ⇒ locate a victim by paging it[1]

  ⇒ TMSI reallocation should be activity dependent

- Is a new TMSI assigned at each change of location as the standard specifies? NO

  ⇒ tracking across different locations by passively sniffing

  ⇒ TMSI reallocation should be executed at each change of location

- Are session keys reused? YES

  ⇒ replay attacks allowing phone tracking

[1] D. F. Kune et al. *Location leaks over the GSM air interface*, NDSS, 2012.
K. Nohl and S. Munaut, *Wideband gsm sniffing*, 27C3, 2010.

Summary of our results

- What does periodically mean? RARELY

  ⇒ locate a victim by paging it[1]

  ⇒ TMSI reallocation should be activity dependent

- Is a new TMSI assigned at each change of location as the standard specifies? NO

  ⇒ tracking across different locations by passively sniffing

  ⇒ TMSI reallocation should be executed at each change of location

- Are session keys reused? YES

  ⇒ replay attacks allowing phone tracking

  ⇒ replay attacks can be avoided using a simple counter, or by forbidding the reuse of session keys

[1] D. F. Kune et al. *Location leaks over the GSM air interface*, NDSS, 2012.
K. Nohl and S. Munaut, *Wideband gsm sniffing*, 27C3, 2010.

Thank you!