ROYAL HOLLOWAY UNIVERSITY OF LONDON

Addressing user privacy issues in mobile telephony

Chris Mitchell

www.chrismitchell.net

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Acknowledgement

- This talk describes joint work with my PhD student Mohammed **Shafi**ul Alam Khan.
- Actually, Shafi did the work – I just made annoying suggestions.
- Of course, the errors in the talk are down to me …

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

GSM – the foundation

- GSM, the European and subsequently global 2G standard contains a suite of security (and to a lesser extent privacy) features.
- These have been extended and improved in both 3G and then 4G, but the basic idea remains the same.
- All based on a secret key shared by the subscriber identity module (*SIM*) and the issuing network (*home network*).
- Allows security to be provided even when a phone accesses a different network (*visited network*).

GSM – authentication

- GSM uses a challenge-response authenticated key establishment (AKE) protocol.
- Uses symmetric cryptography and a secret key shared by home network and SIM.
- Secret session key established is used to provide channel confidentiality using symmetric encryption.
- Design of AKE allows SIM issuer (home network) to keep control of AKE algorithms, and not divulge long-term key shared with SIM to visited network.

3G security

- In GSM the authentication was one-way and only one session key was established.
- In 3G:
  - mutual authentication added;
  - 2 session keys established: for encryption of channel data & for MACing channel commands;
  - USIM replaces SIM;
  - structure of protocol (AKE) unchanged, i.e. home network retains control of key and algorithms.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

3G privacy

- GSM, 3G and 4G all have essentially the same privacy feature (called *user identity confidentiality*).
- Every (U)SIM has a permanent identifier – the IMSI.
- Routine use of this across the radio link (air interface) would enable users to be easily tracked.
- So instead the visited network generates a temporary identity (TMSI) for every phone – a kind of pseudonym.
- TMSI changes regularly and is sent to mobile encrypted (so new/old TMSIs cannot be linked).

3G AKA – overview

- The 3G AKA protocol involves two messages:
  - one containing a challenge from the network to the mobile, and
  - a response from the mobile to the network.
- Both messages are computed as a function of the long-term secret key *K* shared by the USIM and the home network.
- We focus here on 3G, but 4G is very similar.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

3G AKA – message 1

- The first message contains *RAND* and *AUTN* (both 128 bits long):
  - *RAND* is a random challenge;
  - *AUTN* is made up of three sub-fields:
    - $SQN \oplus AK$ (48 bits) – where *SQN* is a sequence number used to enable the mobile to distinguish fresh from replayed challenges, and *AK* is stream cipher keystream generated as a function of *K* and *RAND*.
    - *AMF* (16 bits) – out of scope for this talk;
    - *MAC* (64 bits) – a MAC computed as a function of *K*, *RAND*, $SQN \oplus AK$ and *AMF*.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

3G AKA – processing message 1

- The USIM performs the following steps:
  - checks *MAC* using its stored key *K*;
  - decrypts (using *K*) & checks *SQN* (and updates its stored sequence number) – authentication is now complete;
  - computes two session keys: *IK* (integrity key) and *CK* (confidentiality key) from *K* and *RAND*;
  - computes a response *RES* as a function of *K* and *RAND* and sends it back to the network.
- All these computations are performed inside the USIM (*K* never leaves the USIM), although *CK* and *IK* are exported to the phone.

3G AKA – generating challenges

- Visited network doesn't know *K* or the current sequence #, so cannot generate challenges.
- The home network generates *RAND* and all the dependent values (*AUTN*, *CK*, *IK* and *RES*) using *K* and its stored sequence number.
- It sends 5-tuples (*RAND*, *AUTN*, *CK*, *IK*, *RES*) to visited networks 'on request'.
- In fact it sends small 'batches', elements of which must be used in the right order.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

Range of issues

- Despite use of the TMSI, there are a number of ways in which an attacker can track individual phones.
- We outline some of these …

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Newly arrived phones

- When a phone arrives in a network, e.g. as a subscriber moves from one country to another, the new network may have no way of knowing the TMSI allocated by the previously visited network.
- Thus the network needs a way of requesting a phone to send its IMSI across the air interface.
- This request is not authenticated (no way to know which key to use), and hence can be spoofed.
- This issue has been documented from the early days of GSM.

Paging message attack

- In 3G, the IMSI *Paging* message allows a network to try to work out whether a phone is present in a particular area.
- The message can contain an IMSI or TMSI, and is not authenticated.
- If a phone detects a message with its IMSI or TMSI it sends a response (containing its current TMSI).
- This allows an IMSI to be linked to a TMSI.

AKA threats I

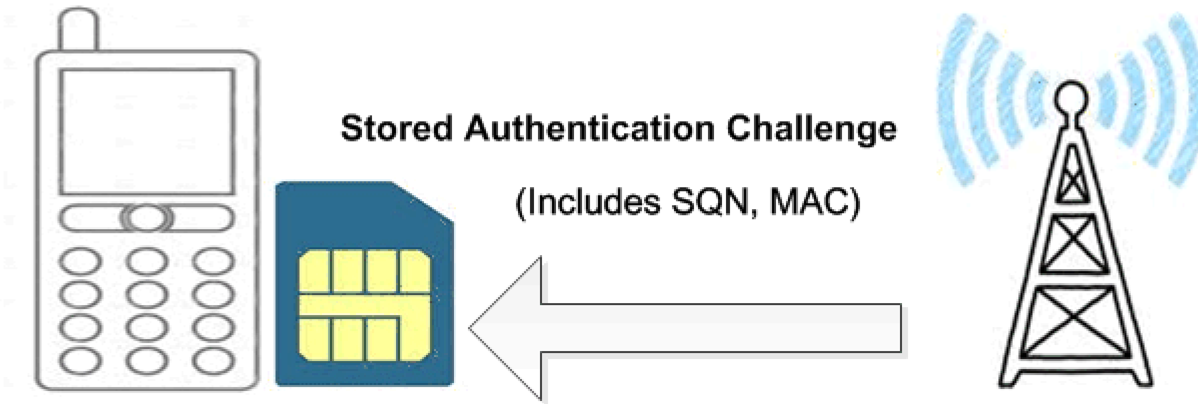
- In GSM, the challenge sent by a network to a phone as part of AKA is not authenticated, and will always elicit a response from a phone.
- If the same challenge is sent twice, the same response will result (since response is computed using a fixed secret key).
- That is, the response for a fixed challenge characterises a phone (actually the SIM).
- Hence an attacker can send a challenge to a phone addressed by its TMSI, and determine whether it is the same as a previously monitored phone.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

AKA threats II

- The GSM problem seems to go away in 3G, since the challenge is authenticated (and 'old' challenges will not be responded to).
- Arapinis et al. (2012) showed that 3G AKA protocol error messages can be used to break privacy just like the GSM problem.
- Different error messages result from:
  - an incorrect challenge (computed using the wrong key);
  - an 'old' but valid challenge.
- These error messages reflect the order in which checks are done by the USIM.

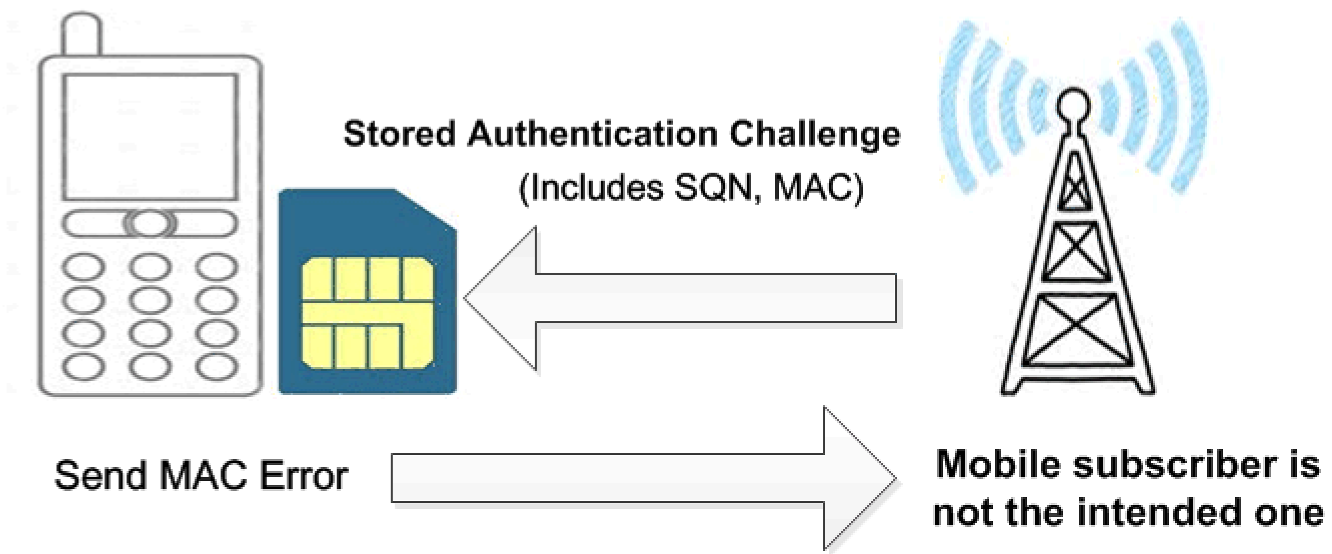
Error message attack I



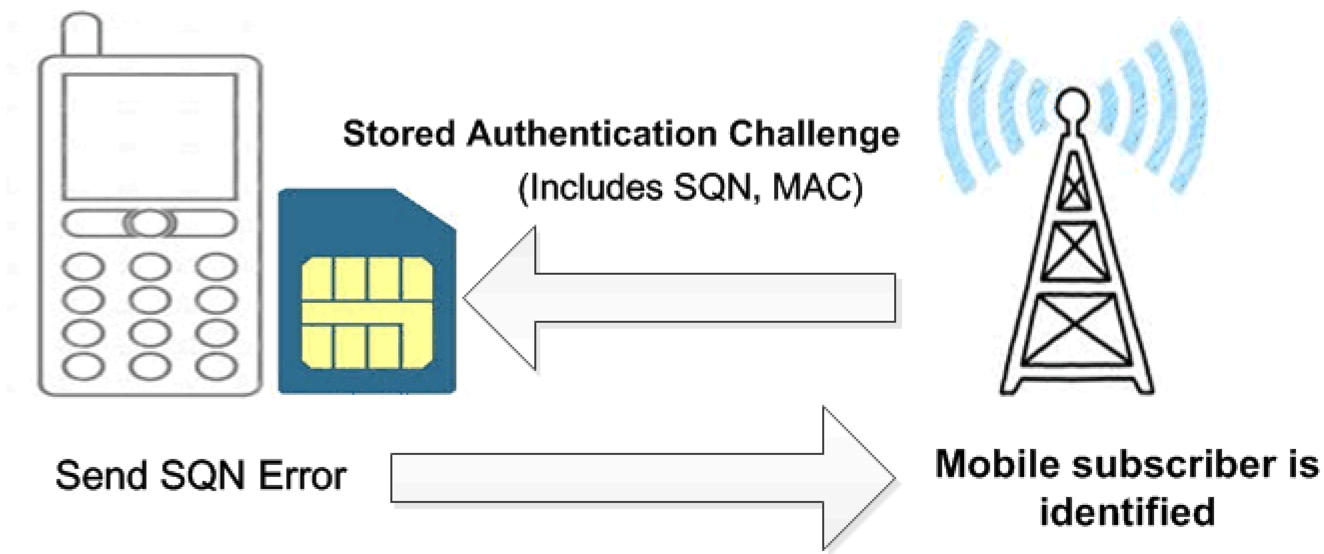
Steps:

1. Check MAC
2. If successful then check SQN
3. Otherwise send MAC error

Error message attack II



Error message attack III



ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Need for IMSI transmission

- Given a TMSI will not always be available, there is a fundamental need for the radio transmission of a user identifier which a home network can recognise.
- This could be an IMSI or some other user-specific identifier.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Encrypting the IMSI

- Perhaps the most ‘obvious’ solution is to encrypt the IMSI when it is sent over the air interface.
- However, unless asymmetric encryption is used, there is no obvious key to use.
- Introducing asymmetric cryptography would add significant complexity, which is why such a solution was not adopted in 3G.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Protocol changes I

- A considerable number of papers have been published proposing changes to the air interface protocol, typically involving IMSI encryption.
- However, deploying such protocol changes presents huge practical difficulties, since existing phones and networks would not interoperate with the new system.
- Essentially it would mean a completely new system, which is not likely to happen.

Protocol changes II

- Arapinis et al. (2012) proposed a suite of changes to address the newly-identified AKA error message issue, as well as other issues with user identity confidentiality.
- We have analysed these carefully, and identified a number of practical issues with their implementation (over and above general problem of deploying a changed protocol).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

What can be done?

- There would seem to be two fundamental problems in trying to fix user privacy:
  - dealing with the need to transfer the IMSI;
  - addressing the AKA error message issue.
- The latter is simple to fix – namely, never send one of the error messages (i.e. use one error message to cover both cases).
- We are proposing a new approach to the IMSI compromise problem, namely to make IMSI compromise less serious …

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Use of the IMSI

- Currently, the IMSI is fixed for life of the USIM.
- IMSI is a 15 decimal digit number, of which:
  - first 3 form the mobile country code;
  - next 2/3 identify network (country-dependent)
  - last 9/10 identify the subscriber.
- First 5/6 digits enable visited network to learn the home network.
- Last 9/10 digits enable the home network to uniquely identify the user account, and hence the shared secret key and other user information.

Multiple IMSIs

- There is nothing to prevent a USIM being equipped with two or more IMSIs.
- The USIM could decide which one to use when.
- We have identified a way in which the USIM can signal to the phone that the phone should re-read USIM data, including the IMSI.
- When the IMSI changes, a phone will simply appear as a newly arrived phone to the visited network.
- The home network will need multiple pointers to the same user account in its database.

Transparency

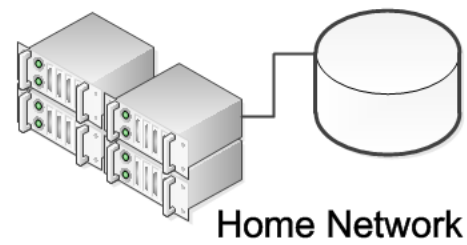
- Such use of multiple IMSIs would give improved identity confidentiality without changing the air interface protocol in any way.
- No changes needed to phones or networks.
- Only changes would be to:
  - home network database;
  - USIMs – which are issued by the home network.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Fixed multiple IMSIs

- One way in which this could be done would be for the USIM to be:
  - pre-equipped with a number of IMSIs, and
  - programmed to switch IMSIs, e.g. at random.
- Could be offered as a value-added service.
- Advantage is that no signalling is required between USIM and home network.
- Disadvantages are:
  - IMSIs are in limited supply;
  - attacker might eventually learn all the IMSIs for a user.

- Pre-equipped with a number of IMSIs and some additional logic
- Include logic to decide when to change an IMSI



Activities:

- Triggering an IMSI change
- Enforce an IMSI change

- All pre-equipped IMSIs are linked to a subscriber account in home network database

Predefined multiple IMSIs – Scenario one

- Pre-equipped with a number of IMSIs and some additional logic
- All pre-equipped IMSIs are linked to a subscriber account in home network database
- Equipped with additional logic to decide when to change an IMSI

Predefined multiple IMSIs – Scenario two

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Dynamic multiple IMSIs

- Disadvantages of fixed multiple IMSIs could be avoided by having the home network change the IMSI for a USIM on a regular basis (only two in use at any time).
- However, need a way for the home network to send a message to the USIM without changing the air interface protocol.
- Such signalling is not supported by current protocol specs, so we have to get smart!

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

The signalling problem

- We need a way for the home network to send a message to a USIM containing a new IMSI.
- This signalling method must be:
  - transparent to the visited network;
  - transparent to the mobile phone;
  - engineered in such a way that the system is resilient to lost messages, i.e. so that there is no way a USIM and the home network can become desynchronised.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Candidates for signalling channel

- The only data sent directly from the home network to the USIM (as opposed to the phone) is *RAND* and *AUTN*.
- *AUTN* already has meaning, and hence cannot convey any further information.
- This leaves RAND, the only requirement for which would appear to be that the same value should never be used twice with a particular USIM.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Embedding an IMSI in *RAND* I

- The ‘business part’ of an IMSI contains 9 or 10 decimal digits, i.e. it can be encoded in at most 34 bits (we propose the use of BCD for simplicity resulting in at most 40 bits).
- We propose encrypting the IMSI as a function of *K* and *SQN*, padding it to a 64-bit string with random bits, and appending a 64-bit *SMAC* (a MAC computed as a function of SQN and *SQN*) to obtain the RAND.
- This is used to generate a 5-tuple in the normal way.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Embedding an IMSI in RAND II

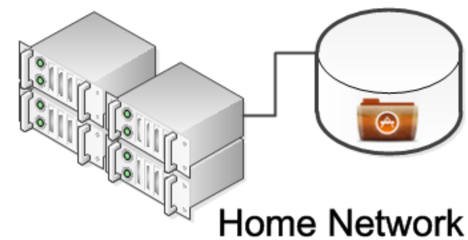
- USIM can distinguish between a random *RAND* and one holding a new IMSI by always computing the *SMAC* (from *SQN* and *K*) and checking if it matches last 64 bits of *RAND*.
- Probability of a false match is infinitesimal.
- Home network keeps sending 'update IMSI' *RAND* values until evidence of use of the new IMSI occurs.
- Hence desynchronisation is not possible.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Embedding an IMSI in RAND III

- Note that the integrity of the IMSI-embedded *RAND* is guaranteed by the *MAC* in *AUTN*.
- This prevents denial of service attacks.
- The IMSI-embedded *RAND* is made up of:
  - an encrypted BCD-encoded IMSI;
  - some random padding; and
  - a MAC.
- Hence should be indistinguishable from a random string, if algorithms are sound.

Modified with additional logic



Activities:
- Decode signal
- Decode new IMSI
- Enforce an IMSI change

Activities:
- Encode new IMSI
- Embed signal
- Send to USIM
- Include logic to decide when to send a new IMSI

Modifiable multiple IMSIs

Agenda

- GSM, 3G and 4G security and privacy
- Threats to privacy
- Previous work and shortcomings
- Using multiple IMSIs
- Managing multiple IMSIs
- Concluding remarks

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Related work

- Sung, Levine and Liberatore (2014) also described a system which allows frequent IMSI changes.
- However, their system involves active involvement of the phone and a virtual USIM.
- Requires use of a virtual network operator, and addresses a network model in which even ‘home’ operator is untrusted.
- Highly complex, and not clear whether would ever meet licensing rules.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Ongoing work

- We need to verify that a phone really can change IMSI easily.
- We (well, Shafi actually) are currently performing experiments to verify this, the results of which will be included in the final paper.
- We also hope to verify the correctness of all aspects of the revised protocol specification for the home network and the USIM.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Papers

- M. S. A. Khan and C. J. Mitchell, 'Another look at privacy threats in 3G mobile telephony', in: W. Susilo and Y. Mu (eds.), *Proc. ACISP 2014, Wollongong, NSW, Australia, July 2014*, **LNCS 8544**, pp.386-396.
- M. S. A. Khan and C. J. Mitchell, 'Improving air interface user privacy in mobile telephony', arXiv:1504.03287 [cs.CR].

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Thank you!

- Any questions …?