**Disclaimer**: Be sure to use a faraday bag or cage before transmitting cellular data so you don’t accidentally break any laws by illegally transmitting on regulated frequencies. Additionally, intercepting and decrypting someone else’s data is illegal, so be careful when researching your phone traffic.

**Some useful terminology**:

*Mobile Phone Related*:

* MS    mobile station (phone)
* SIM    subscriber identity module (sim card)
* IMSI    international mobile subscriber identity (subscriber ID)
* TMSI    temporary IMSI (helps with privacy by obfuscating ISMI)
* Ki   128-bit unique subscriber key (paired with IMSI)

*Tower Related*:

* BTS    base transceiver station (contains the equipment for transmitting and receiving radio signals, antennas, and equipment for encrypting and decrypting communications with the base station controller (BSC))
* BSC    base station controller (handles allocation of radio channels, receives measurements from the mobile phones and controls handovers from BTS to BTS)

*Core Network Related*:

* NSS    Network Subsystem responsible for the routing of calls by way of the BSC and BTC
* MSC    mobile switching center (network switching)
* VLR    visitor location register (database of mobile stations that have roamed the area)
* HLR    home location register (main database of permanent subscriber information)
* AuC    authentication center

*Variables*:

* RAND    128-bit random number (sent to MS by AuC to facilitate MS authentication challenge)
* SRES    challenge sent to MS (generated using RAND + Ki  + A3 algorithm)
* KC    uniquely generated key (generated using RAND + Ki + A8 algorithm)

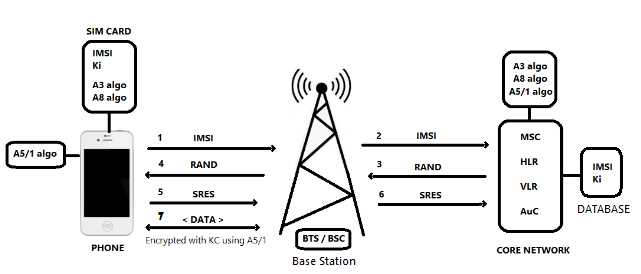
    — note: data is encrypted using KC + A5/1 algorithm

**Preliminary Information**:

Before proceeding to the encryption process, it may be helpful to know that although there are three different algorithms (A3, A8, and A5/1), we can simplify the overall process significantly by stating upfront, the following:

* The A3 (**authentication**) **algorithm** is ‘only’ used to facilitate authenticating that the mobile station (MS) has permission to be on the network.
* Once authenticated, the A8 (**ciphering key generating**)**algorithm** is ‘only’ used to create a unique key (KC), that ultimately will be used (by the MS and the Network) for encrypting/decrypting data using the **A5/1 stream cipher algorithm** on-the-fly.
* The A3 algorithm, A8 algorithm, IMSI and Ki all exist on the MS (phone) SIM card and the A5/1 stream cipher algorithm exists in the MS (phone) hardware.
* Additionally, the Home Network (HLR, VLR, MSC, AuC), has access to the same information via its databases.

**Typical Process**:

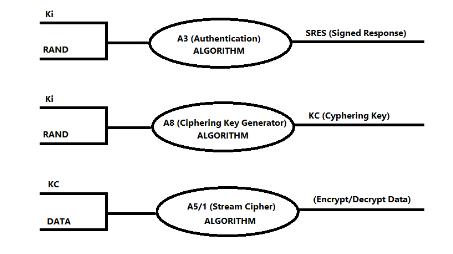
**Diagram 01**

**Process:**(follow diagram-01)

1. Mobile station (MS) requests access to the network,  MS sends its IMSI to the Network Subsystem (NSS) via the BSC / BTS.
2. The IMSI sent by the MS is forwarded to the MSC on the network, and the MSC passes that IMSI on to the HLR and requests authentication.
3. The HLR checks its database to make sure the IMSI belongs to the network.
   * If valid, The HLR forwards the authentication request and IMSI to the Authentication Center (AuC).
   * The AuC will access its database to search for the Ki that is paired with the given IMSI.
   * The Auc will generate a 128-bit random number (RAND).
   * The RAND and Ki will be passed into the A3 (authentication) algorithm, creating a 32-bit SRES (signed response) for the challenge-response method.
   * The RAND is transmitted (via the BSC / BTS) to the mobile station (MS).
4. The RAND received by the MS, together with the SIM card-Ki are passed into the SIM card-A3 (authentication) algorithm, generating the phones SRES response.
5. The phones SRES response is transmitted (via the BSC / BTS) back to the AuC on the network.
6. The AuC compares the sent SRES with the received SRES for a match. If they match, then the authentication is successful. The subscriber (MS) joins the network.
7. The RAND, together with the SIM card-Ki are passed into the SIM card-A8 (ciphering key) algorithm, to produce a ciphering key (KC).
   * The KC generated is used with the A5 (stream ciphering) algorithm to encipher or decipher the data.
   * The A5 algorithm is stored in the phone’s hardware and is responsible for encrypting and decrypting data on the fly.

**Levels of Security:**

*Algorithms*:



**IMSI Obfuscation**:

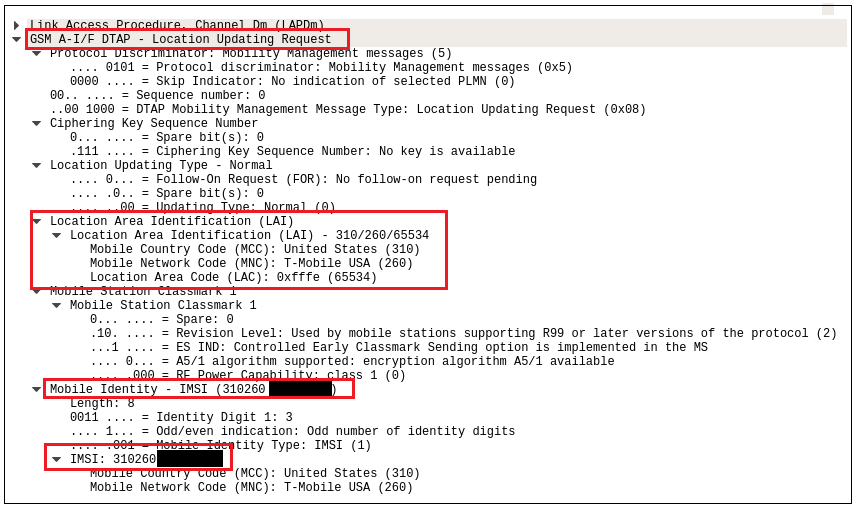
The first time a subscriber joins the network, the Authentication Center (AuC) assigns a TMSI (temporary IMSI) which will be used in place of the subscribers IMSI going forward. I say “temporary”, but in fact, the TMSI is stored (along with the IMSI) in the VLR (visitor location register).

When the phone is switched off, the phone saves the TMSI on its SIM card, ensuring it is available when switched on again.

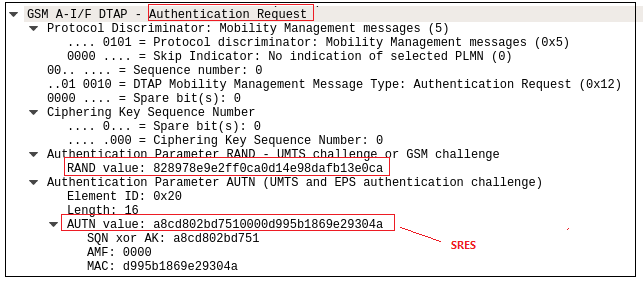
Every new update (roaming, handoffs, etc) results in a new TMSI being created. The TMSI is used in place of the IMSI to protect the subscriber’s identity.

**Sample Packet Screenshots:**

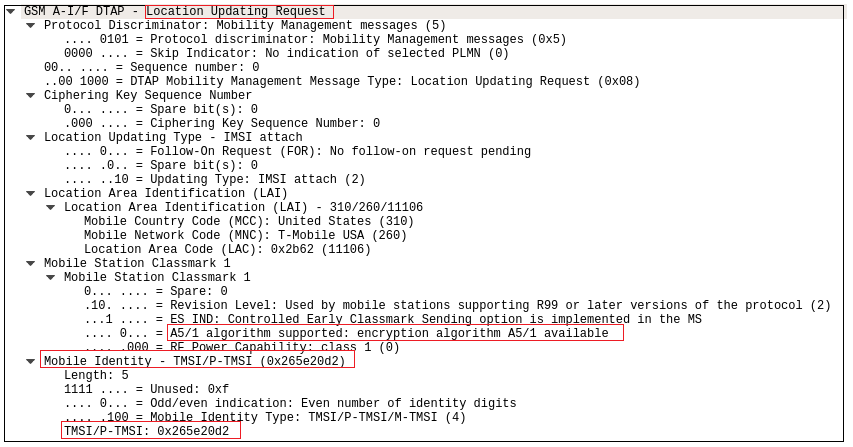
*Location Updating Request (TMSI not established yet)*



*Authentication Request*



*TMSI / A5/1 Algorithm Supported*



**Summary**

This write-up documents some of my follow-up research with regard to analyzing the GSM traffic packets I captured using Software Defined Radio. My attempt was to better understand the GSM mobile network protocols and procedures, with an emphasis on the authentication and ciphering algorithms being deployed.

In my opinion, there is a huge demand for exploring this relatively untouched attack vector, especially as we move towards adopting 5G technologies. The A5/1 stream cipher algorithm, is still in use today on many GSM networks, has a prior history of being exploitable, and there are quite a few networks that do not even implement ciphering in their protocols (SMS data completely exposed).

These vulnerabilities can potentially expose our private SMS messages, personal data, and even our GPS locations to the public if left unguarded. More research in this area is required to ensure our privacy remains secure. From an InfoSec perspective, the areas of concern might be MiTM attacks, network breaches, etc. The playing field is wide open.

**References:**

<https://www.sans.org/reading-room/whitepapers/telephone/gsm-standard-an-overview-security-317>

<https://en.wikipedia.org/wiki/GSM>

<https://payatu.com/blog_28> by <https://payatu.com/blogger_by%20Rashid%20Feroze>

***Join the BHIS Blog Mailing List – get notified when we post new blogs, webcasts, and podcasts.***

Top of Form

Join 2,783 other subscribers

Bottom of Form