Vulnerability by Design in Mobile Network Security [*]

A Jøsang[1], L Miralabé[2], L Dallot[2]

[1] *University of Oslo, Norway*
E-mail: josang@ifi.uio.no

[2]*TazTag, France*
E-mail: lm@taztag.com, leonard.dallot@taztag.com

Abstract: *The GSM network, commonly called 2G, was designed during the 1980s when the Cold War was still on. Due to political pressure from European governments, the security of GSM was deliberately made weak to allow easy interception by law enforcement agencies. Despite strengthened security in subsequent mobile network technologies of 3G and 4G, the weak security of 2G represents the 'weakest link' and thereby limits the security level of mobile networks in general. This article describes the evolution of mobile network security architectures, analyses their security vulnerabilities, and proposes solutions to mitigate the threats posed by these vulnerabilities.*

Introduction

The digital cellular mobile network GSM (Global System Mobile), commonly called 2G, was standardised by European Telecommunications Standards Institute (ETSI) during the 1980s. Weak security was purposely built into the system because various European governments requested the ability to deactivate or break the encryption on the radio link in order to eavesdrop on mobile phone conversations. At the introduction of 2G GSM in 1991, MNOs (Mobile Network Operators) outside Europe were forced to use weak encryption, whereas European operators could use relatively strong encryption. For that reason, a strong and a weak set of cryptographic algorithms were designed. Parts of the GSM 2G standards were kept confidential and only distributed to industry partners under non-disclosure agreements. Mobile handsets for 2G were designed to handle both weak and strong encryption to allow use anywhere in the world. An unfortunate consequence of this design choice is that attackers can trick mobile phones to use the weak encryption of 2G, even in countries where operators otherwise use strong encryption. Because network authentication was not included in the 2G standard, mobile phones do not know whether they are connected to a genuine 2G operator's base station, or to a fake base station set up by an attacker. This vulnerability enables attackers to break the encryption for any subscriber in a radio cell, obtain the encryption key, and then later eavesdrop on that subscriber. Under certain conditions, this vulnerability exists even if strong encryption is being used.

The subsequent Universal Mobile Telecommunications System (UMTS), commonly called 3G, was standardised by 3rd Generation Partnership Project (3GPP) under the responsibility of The International Telecommunication Union, Telecommunication Standardization Sector

[*] *The Journal of Information Warfare*, ISSN 1445-3312, Volume 14, Issue 4, 2015.

(ITU-T) and commercially launched around the year 2000. Criticism of the weak security in 2G resulted in relatively stronger mobile security being designed for 3G; this security included, for example, stronger cryptographic algorithms and a form of network authentication. However, 3G stops short of allowing the mobile phone/user to actually authenticate the identity of the MNO to which it is connected.

Then around 2010, the most recent mobile network technology named Long Term Evolution (LTE), commonly called 4G, was launched with additional security improvements.

In today's mobile networks, a combination of 2G, 3G and 4G is being used worldwide. Mobile phones sold today are typically designed with the capability to connect to all these networks in order for the phone to get maximum coverage most places. It is then obvious that 2G is the weakest link in the whole mobile network security chain. Although a mobile phone is able to communicate securely over 3G or 4G, the phone can simply be tricked not to do so. In that sense the typical ‘smartphone’ is rather ‘dumb’. It is as if someone were tricked to secure the front door with only a hook, even if the door is equipped with an un-pickable lock.

The search for the reason behind the vulnerabilities in mobile networks reveals the interesting reality that those vulnerabilities are partially created deliberately by national and industry policy. It was politically desirable to create weak mobile security in 2G during the 1980s. Even if these political reasons no longer exist today, there are currently business incentives for keeping 2G and its weak security in operation. Certainly, the designers of 3G and 4G must have realized that as long as 2G is still being used making 3G and 4G more secure does not really improve the overall security. This article discusses the unfortunate situation of mobile network insecurity and proposes solutions to mitigate the current vulnerabilities.

Mobile Network Architectures

The global mobile networks are built with a set of core technologies developed during the 1980s, combined with subsequent generations of networking technologies for improved performance.

When a Mobile Station (MS) enters into the radio cell of an MNO, the nearest base station first requests the permanent International Mobile Subscriber Identity (IMSI) in order to identify the subscriber. The IMSI is forwarded to the subscriber’s mobile operator where the MSISDN and other subscriber parameters are stored in the Home Location Register (HLR), as shown in **Figure 1**. Subsequently, a short-lived Temporary Mobile Subscriber Identity (TMSI) is generated and sent to the base station. The IMSI is sensitive information because it can be used to track the subscriber and to potentially discover the MSISDN (phone number) of the subscriber. Although the mapping IMSI–MSISDN is normally only known by the HLR, the MSISDN can be discovered by third parties. (See the section on IMSI-catchers below.)

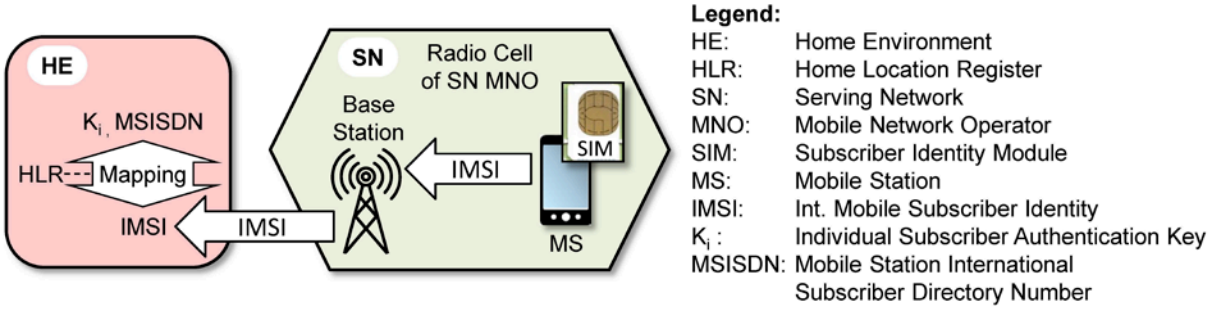


Figure 1. Transfer of IMSI for subscriber identification

The purpose of using the TMSI instead of the IMSI most of the time is precisely to minimise exposure of the IMSI. However, a base station has the possibility to request the IMSI at any time, which not only undermines the purpose of the TMSI, but also *is* the vulnerability exploited by IMSI catchers described below.

Security architecture of 2G GSM

Authentication and encryption in 2G GSM are facilitated by a long-term secret 128 bit individual subscriber key K_i which is stored within the tamper-resistant SIM card of the subscriber. The symmetric K_i is generated by the SIM manufacturer or by the MNO when the SIM card is programmed, so the operator also has a copy of this key. Three main types of cryptographic algorithms are used in 2G. These are the pair of algorithms denoted A3 and A8 (where the combined pair is commonly called COMP128) of which there exists four different sets, as well as the stream cipher algorithm A5. The key K_i is used with COMP128, or more specifically with the A3 algorithm for subscriber authentication, and with the A8 algorithm for generating the session cipher key CK. The key CK is then used with A5 for encrypting the data over the radio link between the base stations of the serving network (SN) and the handset denoted MS (Mobile Station).

The algorithm for encrypting the radio link in 2G is generally called A5, and there were originally two different versions called A5/1 and A5/2. The design of A5/1 was started in 1982 and standardised in 1987 when GSM was not yet considered for use outside Europe. The second algorithm A5/2 was added in 1989 specifically for markets outside Europe. The idea was that European countries should use the relatively strong (but known to be vulnerable) A5/1 algorithm, whereas markets outside Europe should use the much weaker A5/2 algorithm. It was originally proposed that A5/1 should have a key length of 128 bits which was projected to be secure for at least 15 years, and would even be considered secure in 2015. The British wanted weak encryption to allow easy call interception, and proposed a key length of 48 bits, while the West Germans wanted stronger encryption to protect against East German spying, so the compromise became a key length of 56 bits for both A5/1 and A5/2 (Færaas 2014). The algorithm designs of A5/1 and A5/2 were initially kept secret, but were leaked in 1994, and subsequently, were entirely reverse engineered in 1999 from the firmware of a GSM telephone (Briceno, Goldberg & Wagner 1999).

The discriminating crypto policy of 2G reflected the mindset of the Cold War and was accepted by mobile operators around the world, so network and phone manufacturers went ahead to start producing equipment that could use both A5/1 and A5/2. There is also the alternative of leaving the radio channel unencrypted, which is simply called A5/0. In addition, from around 2004, a third algorithm called Kasumi developed for UMTS 3G started to be implemented in mobile phones and 2G base stations, where the variant A5/3 uses a 64 bit key and the variant A5/4 uses a 128 bit key. Due to terribly low security strength of A5/2, the 3GPP made a decision in 2007 to prohibit the implementation of A5/2 in new mobile phones.

When a phone connects to a base station, an authentication and the key agreement protocol (sequence of messages) is executed during call set-up. System entities belonging to the subscriber's home operator are collectively called Home Environment (HE). System entities in the visited network are collectively called Serving Network (SN).

The SN sends the subscriber IMSI to the HE, which looks up the profile of that specific subscriber in the Home Location Register (HLR), where it finds the secret individual subscriber key K_i. The HE computes a set of n cryptographic authentication vectors (AV) also

called GSM triplets denoted AV_{GSM} = {CK, XRES, RAND} consisting of the cipher key CK generated by the algorithm A3, the expected response XRES generated by the algorithm A8, and the random nonce RAND. The HE sends the set of AV_{GSM} vectors to the SN which can use it for n authentication exchanges with the SIM. When the last AV_{GSM} has been used, a new set is requested from the HE.

After receiving the AV_{GSM} vector, the SN sends RAND across the radio link to the mobile phone denoted MS (Mobile Station) which in turn passes it to the embedded SIM chip. The SIM uses the algorithm A3 to compute the response RES, and the algorithm A8 to compute the cipher key CK, both as a function of RAND and the secret individual subscriber key K_i. RES is returned via the MS across the radio link to the SN which checks that XRES = RES to authenticate the subscriber. The SIM also sends cipher key CK to the MS. After successful subscriber authentication, the encrypted radio channel is established between SN and MS using key CK with one of the versions of the A5 algorithm, where the specific version of the algorithm is dictated by the SN. This simple scenario is illustrated in **Figure 2**.

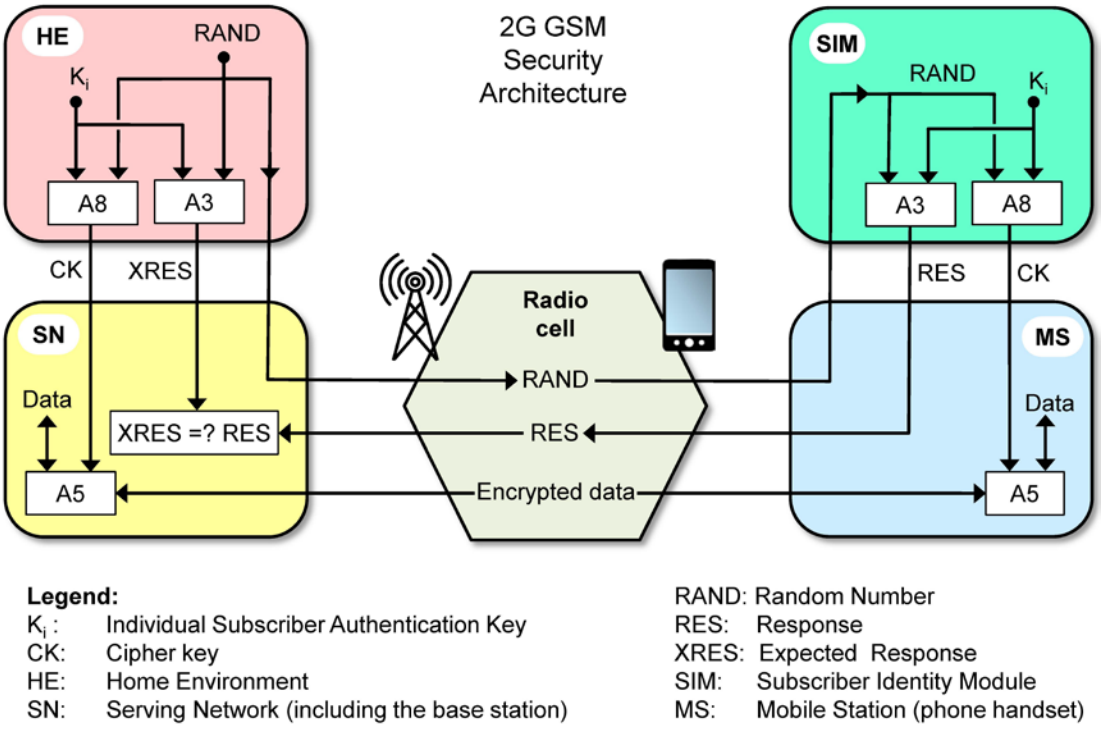


Figure 2. Security architecture in 2G GSM

The logistics of replacing the algorithms of COMP128 (A3 and A8) is relatively simple, and consists of distributing new SIM cards to subscribers of the MNO, and upgrading centralised system components in the MNO network. This can be done by one mobile network operator independently of other operators, and has typically been done several times by each operator. Unfortunately the situation is much worse for the A5 ciphers, which are embedded in the hardware of most handsets and in base station equipment around the world. Today it is possible to conduct practical attacks on A5/1 so that calls encrypted with A5/1 can easily be decrypted on a high-end PC. Due to the practical difficulty of replacing 7 billion mobile phone handsets, this vulnerability is very difficult to remove in the short to medium term. Moreover, this threat is aggravated by the fact that A5/1 is mandatory in every handset that supports GSM communication.

Security architecture of 3G UMTS

3G UMTS security builds on elements of 2G by retaining the security features that worked well, by improving those that did not, and by adding new security features. As in GSM, a smart card called the USIM (which represents the subscriber) is inserted into the MS.

The authentication vector AV_{UMTS}. = {RAND, XRES, CK, IK, AUTN} consists of a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. The array of n authentication vectors AV_{UMTS} is sent from HE to SN where it is stored in the VLR (Visited Location Register). The UMTS authentication vector is called the UMTS 'quintuplet' in analogy to the AV_{GSM} 'triplet' of 2G GSM.

In the UMTS AKA protocol (Authentication and key Agreement) the SN first selects the next authentication vector from the array and sends the parameters RAND and AUTN to the USIM via the MS. The USIM checks whether AUTN can be accepted by verifying MAC = XMAC. The AUTN token is only accepted if the sequence number contained in this token is fresh. This check is an approval of the SN identity by the subscriber's home operator, but falls short of being a proper network authentication by the USIM. After validating AUTN, the USIM returns response RES to the SN. The USIM also computes CK and IK. The SN compares the received RES with XRES. If they match, the SN considers the authentication exchange as successfully completed. The USIM generated keys CK and IK are transferred from the USIM to the MS, those received by SN through AV_{UMTS} are sent from the SN VLR to the base station in the radio cell where the subscriber is located. These keys are then used by the ciphering and integrity functions in the MS and in the SN base station as shown in Figure 3.

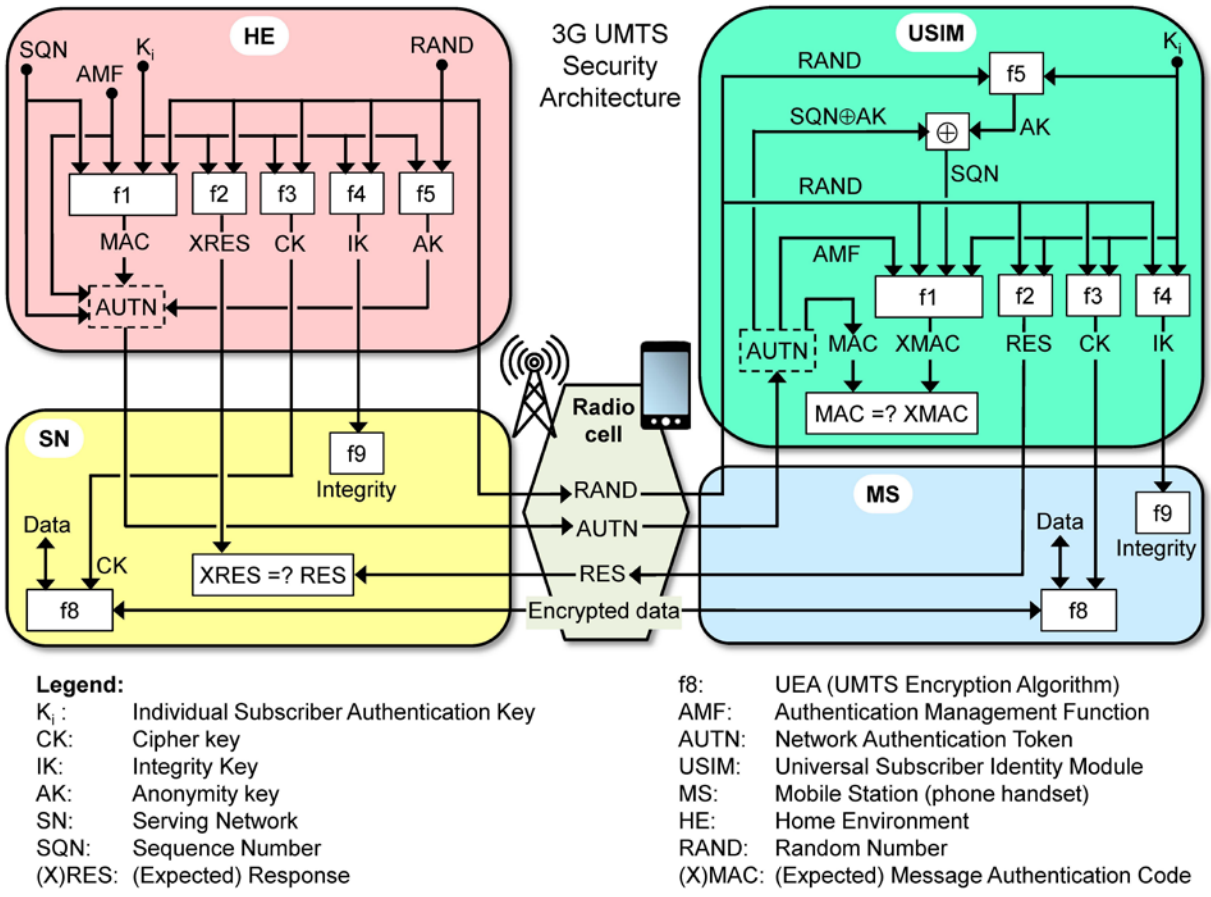


Figure 3. Security architecture in 3G UMTS

Algorithms and key derivation functions in UMTS have generic names denoted 'f#', where each function (f#) is implemented with a specific algorithm/function. The algorithms/functions f1-f5 are located in the HE/USIM domain and can be chosen by each MNO independently of others, because no global alignment of these algorithms/functions is needed. In fact, the UMTS standard does not dictate the specific algorithms/functions to be used for f1-f5; it only proposes some reference examples. As a result, the global mobile network is less vulnerable to specific cryptographic attacks because such attacks would typically only affect a limited set of MNOs. In addition, an MNO would easily be able to replace any vulnerable algorithms with new and stronger ones.

However, the functions f8 and f9 have specific implementations that are dictated by the UMTS standard because of the requirement for global interoperability. As a result, the exact same specific algorithms are implemented in every mobile handset worldwide. In particular f8 can be UEA1— the Kasumi algorithm, which is also used in 2G GSM where it is called A5/3. Alternatively, the algorithm can be UEA2, with is based on the newly introduced Snow 3G algorithm. It is also possible that SN and USIM negotiates to let f8 be instantiated as UEA0, which turns off encryption altogether; however, this is normally only used for emergency calls. The specific algorithm used for f9 to provide integrity protection is either UIA1 (UMTS Integrity Algorithm 1), which is based on Kasumi, or UIA2, which is based on Snow 3G. Integrity cannot be switched off, which means that one of these algorithms must be used.

While security in 3G UMTS is significantly stronger than in 2G GSM, it still has certain vulnerabilities. 3GPP has identified various potential threats categorised as DoS (Denial of Service), user impersonation, network impersonation, Man-in-the-Middle (MitM) attack, and identity catching (Mobarhan Mojtaba, Mobarhan, Mostafa & Shahbahrami 2012). Of these threats, Man-in-the-Middle represents the most potent attack, which can be used to identify the IMSI with the so-called IMSI catchers discussed below.

Security architecture in 4G LTE

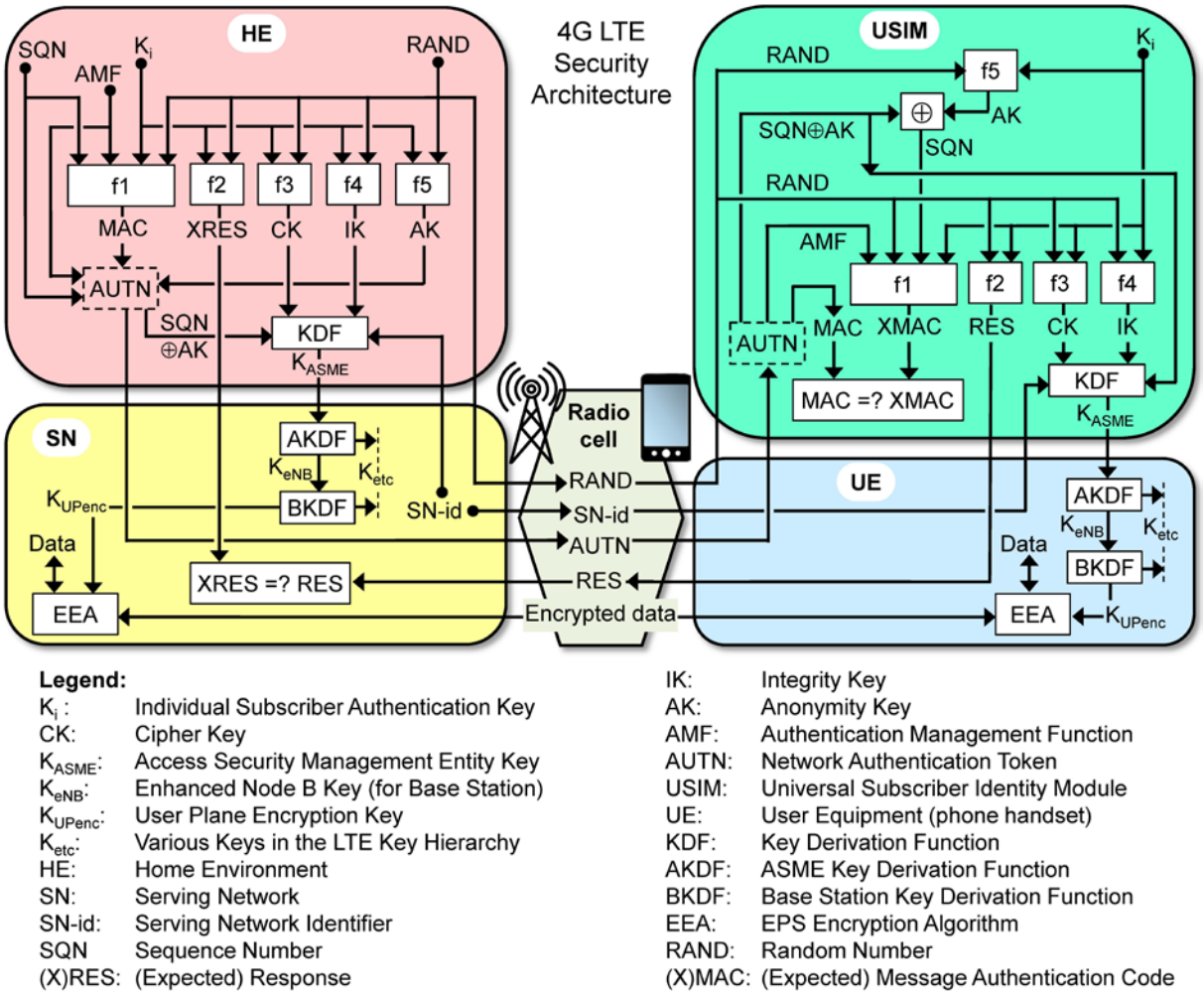
The 4G LTE architecture was developed by 3GPP. Its inception and design were informed by consideration of security principles based on 5 security feature groups (3GPP 2011).

1. Network access security, to provide a secure access to the service by the user.
2. Network domain security, to protect network elements and secure signalling and user data exchange.
3. User domain security, to control the secure access to mobile stations
4. Application domain security, to establish secure communications over the application layer
5. Visibility and configuration of security, allowing users to check if security features are in operation.

LTE is designed with strong cryptographic techniques, mutual authentication between LTE network elements with security mechanisms built into its architecture. Cryptographic protection is provided on many different layers in 4G, which requires a relatively large number of cryptographic keys. For that reason, a multi-level key hierarchy was introduced using multiple key derivation functions. The advanced security architecture puts a higher requirement on security operations management by the MNOs. While the security in 2G GSM and 3G UMTS consists of a fixed set of standardised modules, in 4G LTE, the MNO must to a

large extent decide which security functionality it wants to implement so that security management, in fact, becomes a challenge (Bhasker 2013).

The LTE authentication vector is the quadruplet AV_{EPS} = {RAND, XRES, AUTN, K_{ASME}} consisting of random number RAND, expected user response XRES, authentication token AUTN, and the Access Security Management Entity Key denoted K_{ASME}. The number of vectors provided by the HE can be less than or equal to the number of AVs requested by the SN. In LTE 4G there is a proper key hierarchy based on the functions KDF, AKDF, and BKDF (named so by the authors), and there are in fact many more keys than those shown in **Figure 4**.



Legend:

K_i :	Individual Subscriber Authentication Key
CK:	Cipher Key
K_{ASME}:	Access Security Management Entity Key
K_{eNB}:	Enhanced Node B Key (for Base Station)
K_{UPenc}:	User Plane Encryption Key
K_{etc}:	Various Keys in the LTE Key Hierarchy
HE:	Home Environment
SN:	Serving Network
SN-id:	Serving Network Identifier
SQN	Sequence Number
(X)RES:	(Expected) Response
IK:	Integrity Key
AK:	Anonymity Key
AMF:	Authentication Management Function
AUTN:	Network Authentication Token
USIM:	Universal Subscriber Identity Module
UE:	User Equipment (phone handset)
KDF:	Key Derivation Function
AKDF:	ASME Key Derivation Function
BKDF:	Base Station Key Derivation Function
EEA:	EPS Encryption Algorithm
RAND:	Random Number
(X)MAC:	(Expected) Message Authentication Code

Figure 4. Security architecture in 4G LTE

It can be seen that the key K_{ASME} depends on the network identity denoted SN-id, which has been approved by the subscriber's home operator and used in the KDF function. This authentication can be considered to be proper network authentication, in contrast to the method used in 3G UMTS, which is only network approval without necessarily knowing the network identity explicitly.

There are three different versions of the traffic encryption algorithm EEA (EPS Encryption Algorithm) denoted EEA1, EEA2, and EEA3, where the latter is used specifically in Chinese mobile networks. EPS (Evolved Packet System) is the packet-based transmission and switching architecture developed for LTE. It is also possible to let EEA be instantiated as

EEA0 which turns off encryption altogether, but this mode is only used for unauthenticated emergency calls. There are three versions of the integrity algorithm EIA (EPS Integrity Algorithm) denoted EIA1, EIA2, and EIA3 (not shown in **Figure 4**). Integrity cannot be switched off, so one of the EIA algorithms must be used.

Cryptographic security in 4G LTE is considered by experts to be relatively strong, so that the most significant security vulnerabilities are no longer found in the architecture of **Figure 4**. Since 4G LTE introduces full IP capability, many of the typical vulnerabilities of the Internet also become relevant for LTE. Potential threats of this category are described by Macaulay (2013) but are outside the scope of this paper.

Call Interception with IMSI-Catchers

An IMSI-catcher is an eavesdropping device used for intercepting mobile phone traffic and for tracking the movement of mobile phone users. Essentially it is a 'fake' base station acting between the target mobile phone(s) and the MNO's real base station, and it is considered to be a man-in-the-middle (MITM) attack. **Figure 5** illustrates the principle of IMSI-catchers.

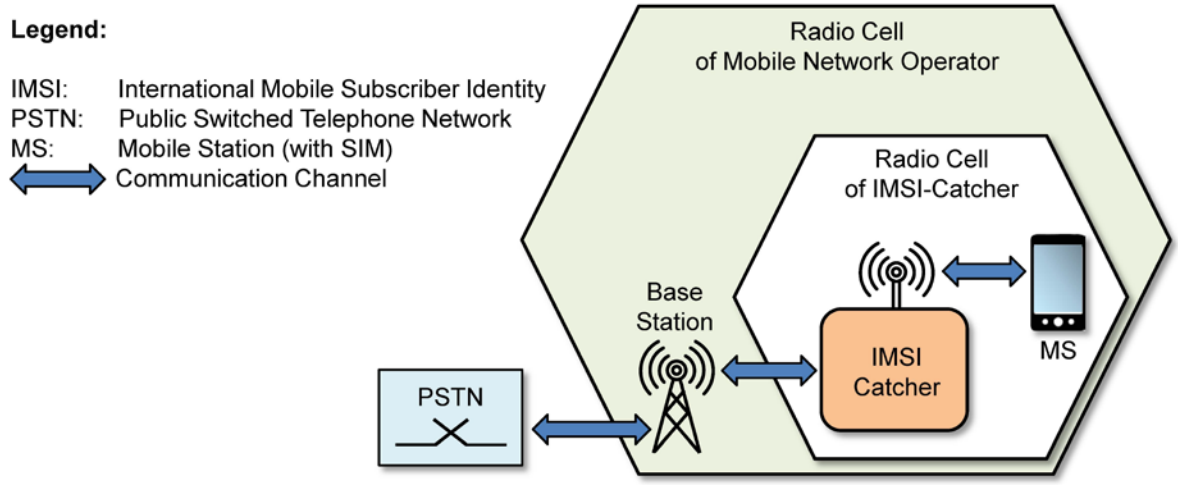


Figure 5. IMSI-catcher principle

IMSI-catchers are typically used by national law enforcement agencies, but they can also be used by criminal organisations and foreign (hostile) intelligence bodies. Primarily, this raises the question of whether the right balance currently exists between legal law enforcement usage and criminal usage. Secondly, it also raises the question of whether governments can be trusted to use IMSI-catchers according to national legislation. In countries governed by totalitarian regimes, the use of IMSI-catchers is probably used arbitrarily by the (secret) police. In countries governed according to democratic principles, the usage of IMSI-catchers is normally controlled according to law, but there are cases where (secret) police bodies are suspected of bypassing their mandate for using IMSI-catchers, which is problematic in a democratic society.

In addition to the vulnerabilities exploited by IMSI-catchers, the telecommunication signalling system SS7 is affected by severe security vulnerabilities that can be exploited by law enforcement agencies and criminals alike. These attacks allow tracing of subscribers as well as interception of SMS messages (Nohl 2014), (Nohl and Melette 2015). The combination of IMSI-catchers and attacks against SS7 can also be used to find the MSISDN (phone number) that corresponds to a particular IMSI (Feest 2015).

Discussion

The global mobile network is, in fact, an access network, either for accessing the Public Switched Telephone Network (PSTN) or for accessing the Internet. The purpose of accessing the PSTN is for making national or international voice calls, and the purpose of accessing the Internet is for accessing the vast resources available on the Internet. Making a comparison with other access networks is useful for understanding the fundamental security problem underlying mobile networks.

Wi-Fi is an access technology for accessing Local Area Networks (LANs) in an organisation as well as for accessing the global Internet. In that sense, Wi-Fi is very analogous to mobile networks with regard to accessing the Internet. Similarly to mobile network security, Wi-Fi security has evolved through several generations, where each new generation was developed in response to vulnerabilities found in the previous version. Wired Equivalent Privacy (WEP), introduced in 1999, was the first security technology for Wi-Fi. The intention of WEP was to provide data confidentiality comparable to that of a traditional wired network. However, serious security flaws were quickly discovered so that attackers could easily intercept or access other people's Wi-Fi access networks. In 2003, the Wi-Fi Alliance announced that WEP had been superseded by WPA (Wi-Fi Protected Access). In 2004, with the ratification of the full 802.11i standard (WPA2), the IEEE declared that WEP had been deprecated. What this meant was the WEP was no longer to be implemented and used in devices and Wi-Fi routers.

The contrast between mobile networks and Wi-Fi is pedagogic. For Wi-Fi access networks, previous generations of weak security technology was phased out after only five years; whereas in mobile access networks, the first generation of weak security technology dating twenty-five years back is still in use.

The politically motivated choice of a weak 56 bit key for A5/1 in 2G GSM made by European countries around 1985 (Færaas 2014) is in line with the politically motivated choice of a 56 bit key for the DES encryption algorithm made by the USA in 1976 (Johnson 2009, p.232). Both design choices were made during the Cold War and had the purpose of allowing cryptanalysis by law enforcement agencies. In contrast to DES which was phased out by the introduction of AES in 2001, A5/1 and 2G GSM are still in use today.

While modern and strong secure technology for mobile networks has been developed and is being used in the form of 3G and 4G, the stakeholders in the mobile industry have decided, for various reasons, to let weak security from 2G remain in the network. The consequence of keeping outdated security in the mobile network is that overall security is actually not strengthened by adding modern security technology because the outdated security technology represents a weakest link as illustrated in **Figure 6**.

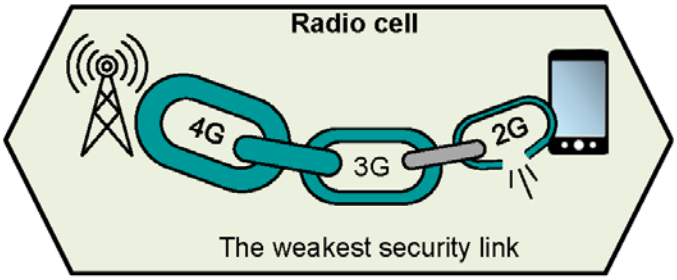


Figure 6. 2G GSM as the weakest security link in mobile networks

In 2000, around 130 million GSM 2G customers relied on A5/1 to protect the confidentiality of their voice communications; and by 2011, it was 4 billion. In 2015, the number of mobile phones that can communicate over 2G is approximately equal to the total world population of 7 billion.

The reason that the weak security of 2G is still implemented in most mobile networks and in all mobile phones worldwide seems to be a mix of business models and national security policies. The original policy of allowing weak or no encryption is still in force in the sense that many states around the world require the ability to request unencrypted radio traffic between mobile phones and the base stations, with the purpose of intercepting mobile phone traffic for law enforcement. Because the mobile networks share the same global standards, this has consequences for all other countries as well. In order to get optimal coverage, a mobile phone must have 2G, 3G and 4G connectivity, and according to the standards must be able to send radio traffic in both encrypted form and in clear, where the network can decide which of these modes to use. If the phone could be configured to always encrypt, then it would be denied network access if it requests encryption in a country where encryption is not permitted. Manufacturers do not produce phones that only allow encrypted traffic or that do not support 2G GSM because these phones would have inferior network coverage and, therefore, would not sell in the mass consumer market.

Security-aware subscribers would be interested in knowing whether the radio traffic is encrypted or not, and the specifications for 2G, 3G and 4G published by ETSI and 3GPP actually do say that phones can give an alert to the subscriber in case of unencrypted traffic, where this alert should be triggered by the SIM/USIM. However, most MNOs de-activate this function in the SIM/USIM so that subscribers get no alert in case of unencrypted traffic (Paget 2010). Disabling the alert function is understandable, as alerts would make many people confused or worried and would most likely result in many people ending calls, which would lead to reduced revenue from network usage and increased help desk calls which would be an extra burden for operators in terms of subscriber management.

Figure 2 (above) makes it obvious that the MS (the mobile phone) actually knows whether the traffic is encrypted or not, as a function of which version of the 2G encryption algorithm is being used. The traffic is unencrypted when using A5/0; and is encrypted when using A5/1 (weak strength) or A5/3 (moderate strength). A mobile phone could thus give alerts independently of triggers from the SIM, but most phones do not. The rationale for phone manufacturers is similar to that of network operators. Many people would be confused and worried by a phone that gives alerts, so they might be reluctant to use it and instead buy a phone from a competitor. This simple analysis indicates that neither MNOs nor phone manufacturers have any incentive for alerting subscribers in case of non-encrypted traffic.

The combination of national security policy and commercial business consideration results in a situation where all mobile phones can send unencrypted traffic and can be dictated to do so by the network operators, to which subscribers will not be alerted. This is, in fact, an ideal situation for IMSI-catching and phone traffic interception.

The term ‘IMSI-catcher’ denotes a fake base station which can be used to obtain the IMSI (International Mobile Subscriber Identity) from nearby mobile phones and which can intercept the radio traffic from the same mobile phones. An IMSI-catcher pretends to be a 2G base station and sends out stronger signals than legitimate 2G base stations in the same area. As a result, handsets nearby determine the IMSI-catcher to be the closest 2G base station and will

send requests for connection. On first time connection, the mobile phone must send the permanent IMSI, which is why the fake base station is called an IMSI-catcher. On subsequent connection to the same fake base station, a pseudonymous TMSI is sent, but this does not help since the IMSI has already been caught. The IMSI-catcher can dictate the settings for the connection and is free to dictate the use of A5/0, which means unencrypted traffic, so that phone calls can be intercepted. The IMSI-catcher must prevent phones from connecting to legitimate base stations with 3G or 4G, and can use radio jamming of the spectrum for 3G and 4G for that purpose. For mobile phones, then, it is as if no 3G or 4G network is available in the area, so they will connect to the IMSI-catcher instead. In order to complete calls, the IMSI-catcher must have a SIM and be able to connect to a legitimate base station nearby, so that it operates as a relay station between mobile phones and legitimate base stations.

IMSI-catchers are normally only sold to national law enforcement organisations, but they can easily be bought by individuals and private organisations. The price has dropped significantly in recent years. Originally they were sold for several hundred thousand dollars but can now be purchased for less than US$1000. Most IMSI-catcher implementations are relatively bulky so that installation in cars is the most practical. However, body-worn IMSI-catchers are also available (Goodin 2013).

The policy of allowing interception of radio traffic for national law enforcement purposes necessarily has as a consequence the reality that criminal organisations and other nation states also are able to intercept mobile phone traffic. The balance of making security weak enough for national law enforcement organisations and at the same time strong enough to thwart attacks by criminal organisations is almost impossible to make. The rationale of having weak security must, thus, be that the legal interception is more valuable than protecting subscribers against criminals and foreign intelligence organisations.

Assuming that 2G with its weak security will stay in mobile networks for years to come, it is worth considering mitigation strategies. Possible strategies include the following ideas:

1. Use phones that can detect when the mobile network is being attacked.
2. Deploy sensors at strategic geographic places to detect fake base stations
3. Include technology and intelligence in every base station to detect fake base stations.

With regard to strategy (1) there are apps for various mobile phone operating systems available that can detect IMSI-catchers with relatively good accuracy. Alternatively, mobile phones can have this as an integrated function which can be activated by subscribers whenever needed.

Strategies (2) and (3) would require major expenditures by governments, individuals, or MNOs, and the questions whether it should be implemented and how it should be financed are political questions. A citizen-oriented approach for (2) could be to use phones of strategy (1) to populate a crowd-based database of known fake base stations.

Conclusion

Policy and technology decisions made twenty-five years ago resulted in intentional integration of security vulnerabilities in mobile networks and handsets. Paradoxically these vulnerabilities still limit the security level of mobile networks today. In other areas, such as Wi-Fi and encryption algorithms, old security technology is phased out and replaced with modern, strong security technology. Despite strong security technology being introduced in mobile networks,

there are business and political incentives to keep the old insecure technology in mobile networks. The paradoxical consequence is that current mobile network traffic can be intercepted just as easily as it could be twenty-five years ago.

The authors propose a set of mitigation strategies for strengthening mobile network security. A serious vulnerability is that most handsets do not detect attacks by default. Security-aware users can install apps for detecting attacks, and mobile phone manufacturers can offer secure phones that detect and prevent attacks. Finally, governments and mobile network operators can deploy sensors in specific geographical areas for detecting attacks. The best-case scenario would utilise a combination of these strategies.

References

3GPP 2011, '*3rd Generation Partnership Project, 'TS 33.401: System Architecture Evolution (SAE); Security Architecture*', <http://www.3gpp.org/DynaReport/33401.htm>, (viewed 09/13/2015).

Bhasker, Daksha 2013, '4G LTE Security for Mobile Network Operators', *Journal of Cyber Security and Information Systems*, vol.1, num.4, October 2013, Cyber Security and Information Systems Information Analysis Center (CSIAC).

Briceno, Marc, Goldberg, Ian & Wagner, David 1999, '*A pedagogical implementation of A5/1'*, <http://www.scard.org/gsm/a51.html>, (viewed 09/13/2015).

Feest, Christian 2015, '*Protecting Mobile Networks from SS7 Attacks*', Telesoft White Papers, 23 June 2015. <http://telesoft-technologies.com/document-library/milborne-ss7-firewall-ips/12-telesoft-whitepaper-protecting-mobile-networks-from-ss7-attacks/file>, (viewed 09/13/2015).

Færaas, Arild 2014, '*Sources: We were pressured to weaken the mobile security in the 80's'*, Aftenposten online 25 December 2014. <http://www.aftenposten.no/nyheter/uriks/Sources-We-were-pressured-to-weaken-the-mobile-security-in-the-80s-7413285.html>, (viewed 09/13/2015).

Goodin, Dan 2013, '*The body-worn "IMSI catcher" for all your covert phone snooping needs*', Ars Technica, <http://arstechnica.com/security/2013/09/the-body-worn-imsi-catcher-for-all-your-covert-phone-snooping-needs/>, (viewed 09/13/2015).

Johnson, Thomas R. 2009, '*American Cryptology during the Cold War, 1945-1989, Book III: Retrenchment and Reform, 1972-1980*', National Security Agency, <https://www.nsa.gov/public_info/_files/cryptologic_histories/cold_war_iii.pdf>, (viewed 09/13/2015).

Macaulay, Tyson 2013, '*The 7 Deadly Threats to 4G*', McAfee White Paper. McAfee, Inc., <https://prod2.secureforms.mcafee.com/verify?docID=763A7BB3-3208-433B-8F25-AC8954D1384E>, (viewed 09/13/2015).

Mobarhan, Mojtaba Ayoubi, Mobarhan, Mostafa Ayoubi & Shahbahrami, Asadollah 2012, 'Evaluation of security attacks on UMTS authentication mechanism', *International Journal of Network Security & Its Applications, (IJNSA*), vol.4, no.4, July 2012, (pp.37-52).

Nohl, Karsten 2014, '*Mobile self-defense*', Chaos Communication Congress, Hamburg, 27 December 2014, <https://events.ccc.de/congress/2014/Fahrplan/events/6122.html>, (viewed 09/13/2015).

—— & Melette, Luca 2015, '*Advanced interconnect attacks: chasing GRX and SS7 vulnerabilities*', Chaos Communication Camp, Zehdenick, Germany, 13 August 2015, <https://events.ccc.de/camp/2015/Fahrplan/events/6785.html>, (viewed 09/13/2015).

Paget, Chris 2010, '*Practical Cellphone Spying*' , DEFCON 18, Las Vegas, July/August 2010, <https://www.defcon.org/html/links/dc-archives/dc-18-archive.html>, (viewed 09/13/2015).