A Survey on the Security Vulnerabilities of Cellular Communication Systems (GSM-UMTS-LTE)

Vasileios Gkioulos[1], Stephen D. Wolthusen[1,2] and Athanasios Iossifides[3]

(vasileios.gkioulos, stephen.wolthusen)@ntnu.no, aiosifidis@el.teithe.gr
[1] *Norwegian Information Security Laboratory, Norwegian University of Science and Technology, Norway*
[2] *School of Mathematics and Information Security, Royal Holloway, University of London, United Kingdom*
[3] *Department of Electronics Engineering, Alexander Technological Educational Institute of Thessaloniki, Greece*

Abstract

The development of mobile communication systems started immediately after the end of world war two, with increasingly significant and global impact. The available systems faced various challenges, enforcing the development of new practices and the introduction of emerging technologies. An important aspect of those systems is security, due to their widespread use, the significance of the transmitted information and possible service abuse. Through this study, the identified security vulnerabilities of digital mobile communication systems are examined, in parallel to the emerging threats. This will provide a valuable understanding on the historical efficiency of the deployed security mechanisms and guidelines for the security requirements of future generation systems.

1 Introduction

A threat is defined as a probable incidental or premeditated subversion of a systems security. The risks imposed by a potential threat can be magnified, due to existing security vulnerabilities or omissions, both in terms of occurrence probability and of the potential impact. Additionally, a security related countermeasure, as defined at [1], refers to an element that diminish the risk of a threat. Such an element may reduce the probability of occurrence of a threat, or minimize the potential impact. Additionally, a countermeasure may be deployed in order to identify an ongoing attack and report it accordingly. Countermeasures can be utilized in various forms, such as an action or a procedure, a dedicated protocol or function, a part of the overall system infrastructure. Usage constraints, implemented into the security policy of a system, are also an element of the deployed countermeasures against threats.

Presented at the Norwegian Information Security Conference 2016 (NISK 2016).

This study aims to the identification of the correlation among the deployed countermeasures over commercial digital cellular communication systems, the exploitation of their residual risks and how their relations affected the design of future system generations. The security features provided by each generation of commercial digital cellular communication systems, are defined in the specification [2] for GSM (Global System for Mobile Communications), [3] for UMTS (Universal Mobile Telecommunications System), and [4] for LTE (Long Term Evolution). Figure 1 provides a graphical representation for the evolution of the fundamental security features, moving through these three systems and their various versions, as described in the aforementioned specifications. The presented enhancement of the supported security features was promoted by two main factors. Initially, the implementation of additional functionalities to the newest network generations required the realization of supplementary security related processes, while the widespread use of such systems alongside with various known cases of attacks, promoted the continuous study and evaluation of the provided security.

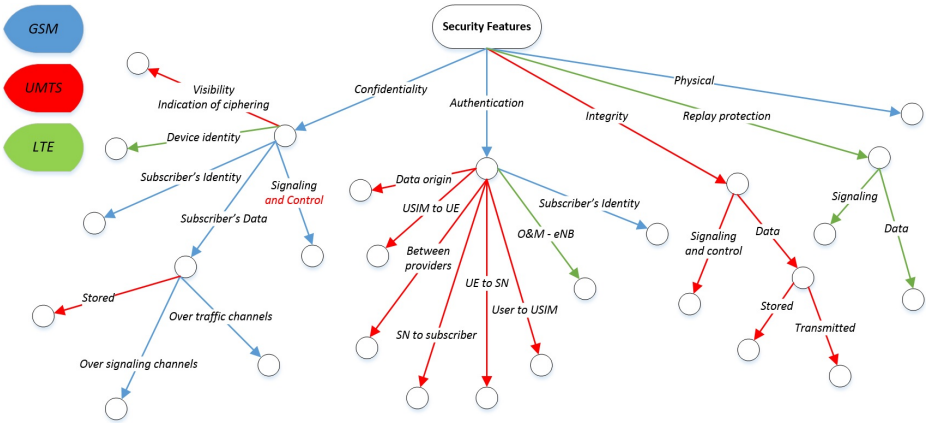

Figure 1: Development of fundamental security features.

2 GSM

Known vulnerabilities of GSM networks

GSM represents the first successful globally established digital cellular communication system, since it surpassed three billion connections during 2008, in a total of over four billion mobile connections [5]. Multiple improvements of the original GSM security specification have been achieved with the introduction of newer versions, such as the GPRS (General Packet Radio Service) and the EDGE (Enhanced Data rates for GSM Evolution).

The study of the vulnerabilities of GSM networks is highly significant for three reasons. Some operators still maintain the original GSM configuration, especially in developing countries. Additionally, the serving networks and user equipments are designed in order to provide backward compatibility, while the selection of the serving network is achieved based either on the coverage or the capacity of the deployed network, making this way possible the enforcement of degradation to GSM from the new and supported technologies.

As presented in [6], due to their open nature, communications that utilize the wireless medium are inherently vulnerable to various threats. GSM was designed in order to minimize the risk of interception, incorporating technologies with transitive benefits to

security assurance, such as frequency hopping. Yet, interception remained feasible, while even commercial interception systems, specifically designed for GSM, are available. Additionally, as presented in Figure 1 authentication was only defined towards the Serving Network-to-subscriber's identity path. offering this way open ground for a variety of attacks, including the notorious GSM vulnerability to the *man in the middle* attack. The complete absence of integrity protection is also noticeable in the same figure. The initial GSM protocol did not took under consideration the integrity protection of neither signalling nor data messages, facilitating this way unidentified message tampering.

Another security weakness is identified on the fact that encryption mechanisms are only utilised through the wireless link of the air interface, with complete lack of user visibility, and not through the fixed network connections. The backbone network, comprising of all the network elements and connections other than the one among the MS (Mobile Station) and BTS (Base Transceiver Station), is mainly based on unencrypted communication. Regarding the backbone network, the deployed SS7 (Signalling System No. 7) system also carries security vulnerabilities, regarding the feasibility of message modification, due to the amount and complexity of the existing interfaces and the tight relations of SS7 with the internet. [7].

Additionally, various flaws have been identified at the implementation of both the authentication and encryption algorithms, allowing the extraction of the Ki (Subscriber authentication) and Kc (Encryption) keys. The most commonly used A3/A8 algorithms are versions of COMP128, which was based on security by obscurity [8]. This algorithm raised many concerns, while various implementation flaws allowed the extraction of the key, with relatively limited physical access given to the ME and a set of pre-calculated challenges. Similarly, over the air extraction of the Ki is also feasible with the use of a pre-defined loop of challenges towards the mobile equipment, allowing the mathematical calculation of the key. The cryptographic algorithms A5-1/2 were also based on security by obscurity. Various cryptanalysis methods have been discovered, able to identify the ciphering key in real time using a personal computer with moderate capabilities, to analyse encrypted conversation [10] [11].

Since the extraction of security related keys and numbers such as the Ki, Kc and IMSI (International Mobile Subscriber Identity) is reasonably inexpensive, both financially and computationally, the creation of clone SIM cards is feasible. However, the GSM incorporates a safety valve, that would recognize a duplicate SIM card operating in distinct location area and deactivate the subscriber's account until further action is taken. Maintenance of user anonymity is also a significance weakness of GSM networks. Although TMSI (Temporary Mobile Subscriber Identity) was implemented in order to avoid the mobile equipment clearly using IMSI for identification, there are cases where this is required. Thus, the IMSI might be clearly revealed, either by eavesdropping regular message transactions, or by enforcing an IMSI identification by a false BTS.

Finally it must be mentioned that GSM has significant vulnerabilities towards DOS (Denial-of-Service) [12] [13] and Replay attacks [14]. Multiple methods have been identified that make the execution of DOS attacks feasible in GSM networks, mostly utilizing the limited signalling channels and the architectural choice of the MS to connect to the BTS that provides the higher transmitted power.

Possible attacks against GSM networks

The presented vulnerabilities of GSM networks have been exhaustively studied, since they can be exploited in order to launch and successfully achieve a variety of attacks

[15]. Since they have been identified, some of these threats have been taken under consideration during the development of GSM enhanced versions and future generation cellular communication systems. In this section the most common and severe of these attacks are presented.

Eavesdropping on traffic or signalling: An adversary may eavesdrop user traffic or signalling and control data over the radio path. This may disclose user sensitive information, or provide access to security management information that can be further used in order to conduct additional active attacks. The used A5 ciphering algorithm received extended criticism since various cryptanalysis methods have been identified. The first known attack of this family [16] was a TMTO (Time Memory Trade Off) based on the birthday paradox. Yet, its successful realization had strict requirements both in the quantity of the required information and processing time. Future TMTO based attacks though [10], required only a small portion of non-ciphered information and limited computational power. The weaknesses of the A5 algorithm becomes easily identifiable by the amount of the proposed cryptanalysis mechanisms. Although some of them impose unrealistic requirements, many have been used to successfully demonstrate attacks against the all three GSM encryption algorithms (A5/1, A5/2, A5/3-KASUMI) [11], [17], [18], [19], [20], [21], [22].

Masquerading: Various masquerading attacks are possible within the GSM network. An adversary can impersonate a network element, in order to intercept or passively analyse user traffic or related signalling and control messages. Signalling and control information can be further used, so that the adversary can masquerade as another network subscriber, gaining access to services on behalf of the legitimate user. The main steps of such an attack require the adversary to first masquerade as a legitimate BTS towards the subscriber, and after authentication has been achieved, use the extracted information to masquerade as the subscriber towards the network [23], [24]. Such attacks, as presented at [25], are feasible due to the lack of subscriber-to-network oriented authentication, allowing this way the introduction of fake BTS. Such equipment can be further used for IMSI/IMEI catching attacks or selective jamming attacks. Similarly, an adversary can manipulate the behaviour of the terminal or the SIM card by masquerading as a legitimate originator of applications and data. Finally, an intruder can impersonate a legitimate user and utilise the authorised services, simply (assuming that he has the required access privileges) by receiving the required information by other entities such as the serving network or the user.

Man in the middle: An adversary using similar methodologies can get nested between a subscriber and the serving network. This can allow him to execute a wide variety of illegitimate actions, such as deleting, modifying, spoofing and replaying signalling messages or user data. [26]

Interface and backbone link security: As mentioned in the previous paragraph, encryption mechanism are only utilised oven the wireless MS-BTS link. The backbone channels are usually unencrypted, including the usual installation of BTS-BCS microwave links. This allows adversaries to eavesdrop subscriber data and signalling messages. Furthermore, the SIM-ME interface is not protected. Thus, transferred information is possible to be tapped. [27]

Privilege abuse: An inherit threat towards commercial cellular communication systems, is the subscriber's capability to misuse their privileges and gain unauthorised access to services or intensively overuse their subscriptions, even if such cases can only have a short and limited duration. Similar types of subscriber originated attacks may include use

of stolen terminals, IMEI manipulation, and terminal/SIM data modification or extraction. Additionally, as presented at [28], the commercial cellular networks become increasingly interconnected with the internet, inheriting this way some of its security threats such as un-traceability or identity theft, including the widespread of viruses and malware.

Denial of service and Jamming: These are two of the most severe attacks against GSM networks, due to the extensive network sensitivity towards them and the variety of methods that can be used, in order to execute such attacks. The most common and successful method of realising a DOS attack against a GSM network, requires the exhaustion of the network resources, aiming mostly on the limited signalling channels. Such an attack makes use of the fact that initial communication among a MS and the network, is executed before authentication. Thus, a MS may repeatedly follow the appropriate protocol steps, requesting additional signalling channels without ever completing the protocol cycle and release them [12]. Regarding jamming attacks, these can exploit the broadcast channels of the network and more precisely the synchronization bursts or registration identifiers, forcing a MS to lose signalling interconnection with the network [29], [30].

3 UMTS

As presented in the UMTS specifications [31], [32], [33], security of the third generation cellular communications system was based on the following principles:

1. UMTS security is build on top of 2G security mechanisms. Furthermore, the following elements are maintained through the transition:
   (a) Subscribers authentication for service access, while relevant identified problem should be resolved.
   (b) Radio interface encryption must be maintained and strengthened.
   (c) Subscriber identity confidentiality must be maintained with the use of a more secure mechanisms than the one used at 2G systems.
   (d) The SIM is maintained as a removable security module.
   (e) The user is not involved in the operation of the security features. Yet, increased visibility must be provided.
   (f) The trust of the Home Environment towards the Serving Network, regarding security functionalities, is minimised.
   (g) Subscriber generated or relating information must be adequately protected.
   (h) The serving network (SN) resources must be protected against misuse.
   (i) The standardised security mechanisms are compatible, interoperable and available worldwide.
2. UMTS security must improve the one provided by GSM, addressing the identified weaknesses. The most significant of which, have been defined to be:
   (a) Attacks based on the use of false BTS stations.
   (b) Open transmission of cipher keys and authentication data.
   (c) The limitation of encryption only on the ME-SN link.
   (d) Lack of data integrity protection.
   (e) Lack of complete IMEI protection.
   (f) Lack of strong protection against fraud.
   (g) Lack of knowledge regarding the implemented security mechanisms, in roaming environments.
   (h) Lack of flexibility regarding the improvement of the security functionalities.

3. UMTS must provide new security features and guaranty the secure realisation and operation of the new services.

Known vulnerabilities of UMTS networks and identified attacks

Despite the given attention to the aforementioned vulnerabilities of GSM networks, during the design of the UMTS, various vulnerabilities have been identified over the 3G systems as well. The official ETSI report over the design and evaluation of the MILENAGE algorithm set [34], identifies that the prime attack point against the implemented algorithms, is the USIM. For the f2 to f5* functions, it is mathematically proven that, no combination of significantly less than 2^{64} output values can be used in order to predict any new output value.

Furthermore, the f1/f1* functions are equivalent to a standard Cipher Block Chaining-Message Authentication Code, while they use distinct output bits acquiring this way sufficient cryptographic separation. A simple internal collision attack exists against the CBC MAC, which requires about 2^{64} values. Thus, the report summarises that the f1/f1* functions appear to be sound. The same report also investigates the independence between the f1/f1* and f2 to f5* algorithms, since a connection among them can be exploited by an adversary for the execution of a variety of active attacks. A mathematical analysis of these algorithms supports that a sufficient separation exists, among these two groups of functions.

Several attacks against the f1/f1* functions, combinations of f2-f5 and combinations of f1-f1* and f2-f5* have been defined. These attacks require about 2^{64} queries and among them is the well known CBC-MAC internal collision attack. Yet, these attacks at the time of the report where considered to be impractical. Similarly, a variety of attacks against the Rijndael-AES algorithm have been identified [35], [36], [37], [38].

Furthermore, as presented in a 3GPP technical report [33], attacks based on camping on a false BS and camping on a false BS/MS are not resolved by 3G security architecture. Such an attack requires the use of modified BS or MS in order to entice a subscriber to connect a false BS that acts as a repeater, being able to relay, modify or ignore certain messages between the SN and the subscriber. Similarly, the UMTS security architecture only partly counteract attacks aiming to hijacking incoming and outgoing calls when encryption is disabled, which also require a modified BS/ MS. Such attacks are feasible among the periodic integrity protection messages. The same report recognizes exploitable vulnerabilities regarding the impersonation of both the SN and the user and eavesdropping of user data. This is achievable by the enforced use of compromised key vectors. Additional vulnerabilities that have been identified in UMTS networks [39] include:

1. Unencrypted IMSI transmission during new TMSI allocation.
2. The IMEI is not considered a security feature. Thus, it is not protected.
3. No protection against jamming attacks.
4. A subscriber is possible to be enticed to connect on a false BS.
5. GEA0 is supported, meaning that unencrypted communication is possible and acceptable, allowing hijacking and Man-in-the-middle attacks.
6. It is possible to enforce a ME to fall back to GPRS/EDGE, if support of UMTS/HSPA services is not available.

Possible attacks against UMTS networks

The described vulnerabilities can be exploited for an execution of a wide variety of attacks. These include [40], [41], [42], [43], [44]:

Denial of service: Can be achieved by an attacker with a modified ME who is able to send a de-registration request to the SN regarding the legitimate user. The same result can be achieved if an attacker sends a location update request from a different LA than than of a legitimate user. Furthermore, an attacker may entice the legitimate user to connect to a false BTS, completing the attack by blocking the traffic towards the SN.

Identity catching: Some explicitly defined cases exist where the IMSI is requested by the network to be transmitted unencrypted. Such cases allow passive or active identity catching, by an attacker who uses a modified MS (passive) or BS (active).

SN impersonation and eavesdropping: An attacker is possible to masquerade as the legitimate SN towards the subscriber. This can be achieved by an intruder who sets his modified equipment between the SN and the subscriber, being able at this point to control the level of encryption used. Additionally, an adversary can modify the ciphering capabilities of the ME, causing this way a mismatch with the SN, possibly enforcing it to select the lowest level or complete deactivation of encryption. Finally, an attacker may entice a subscriber to make use of a compromised authentication vector and a modified BS.

Subscriber's impersonation: Many feasible methods have been identified in order to successfully achieve such an attack. These include the use of compromised authentication vectors, eavesdropped authentication responses and hijacking of ingoing/outgoing calls with both disabled and enabled encryption

4 LTE

Known threats against LTE networks

The threats faced by LTE networks, as described in the system specifications [45], can be categorized as:

Threats towards the UE.

1. IMSI catching: There are cases where plain-text IMSI queries are necessary. This security vulnerability is of increased exploit-ability in certain areas, such as airports. Additionally service identifiers are send in clear, a decision made based on IMSI safety, thus increasing the potential impact of IMSI vulnerabilities.
2. UE tracking: Multiple cases exist regarding attacks of this nature:
   (a) Tracking of subscriber's temporary ID can be used based on data logging techniques, in order to monitor the actions taken by the temporary ID and correlate them to a user when enough information becomes available. In combination with IMSI catching techniques, the assigned temporary ID can be identified and be used to track user activities.
   (b) Identification of the links between the IMSI/ TMSI and RNTI can be achieved due to the weaknesses of 2G/3G confidentiality schemes. The exploitation of this vulnerability requires the use of a false network element (eNB/BTS), in order to request a new IMSI registration from the UE.
   (c) Tracking due to link identification among the used IP-address and the TMSI/IMSI is also feasible. Such an attack can be achieved if the assigned IP address is kept static, without being renewed periodically.
   (d) A mapping between a new and old RNTI can provide tracking capabilities to

an adversary, if the allocation procedure is not confidentiality secured. The tracking of the RNTI can be used for unique UE identification.

(e) Passive tracking of signalling messages can also provide valuable information to an attacker, such messages can provide the capability to approximate the current location and moving pattern of a subscriber.

(f) Cell level measurements transmitted between the UE and the eNB can also be used for the approximation of the subscriber's location.

3. Threats related to forced handover require the use of a compromised eNB, which can request or entice the UE to connect on an eNB that deliberately or unintentionally drops the established connection.
4. Enforced handover towards a legacy RAT can be feasible if an adversary can generate RRC signalling messages, which request the UE to relocate towards a network with decreased security features, reduces resources or in a selected network, designed for UE capturing.
5. Bootstrap signalling and some multicast signalling messages are unprotected in LTE. Thus, creating a vulnerability that can be exploited for DoS attacks.
6. False system information can be introduced by an intruder to UE, by the use of broadcasting messages. Such attacks are inherited from UMTS and can lead to DoS or service degradation.

Threats towards the eNB

1. Achieving the physical compromise of the eNB or hijacking, packet injection/ modification is possible. This gives the intruder the ability of upstream (towards the core network) and downstream (towards the reachable UE) packet injection and service degradation. Physical attacks on eNB can also cause key and unencrypted data extraction, combined with DoS attacks and integrity violation.
2. Eavesdropping of user plane packets is possible at the links among the UE and SAE gateways or within a compromised eNB. The feasibility and impact of such attacks is highly correlated to the implemented confidentiality mechanisms.
3. DoS attacks impose a significant threat both on the network-eNB and the eNB-UE paths. Packet injection from a false UE or network element can be used in order to enforce a DoS, radio jamming or service degradation state on the eNB.

Threats towards the MME/SAE gateway. Such attacks may include DoS against the MME, based on signalling messages coming from the RAN. This may include the utilization of various system procedures, such as the initial access authentication.

Threats regarding the mobility management procedures.

1. Access to control plane data can disclose critical information, such as network resource allocation and mobility management traffic. Such information may be further used to achieve confidentiality and privacy violations.
2. Control plane data integrity may also be violated, facilitating the execution of replay attacks and the compromise or masquerading of network encryption points.
3. Similarly, service disruption or misuse is achievable. Respectively to the adversary's capabilities this may allow traffic redirection, flooding attacks both at the RAN and the core network or replay attacks.
4. Finally, unauthorised service access is achievable by masquerading as legitimate network elements or users.

A variety of countermeasures has been defined in the same study, in order to address the potential risk of these threats. Yet, a plethora of other security risks regarding LTE has been identified. In [46] the authors distinguish a weak point on the extended amount of

external connectivity points towards peer operators, third party application providers, the public internet and various heterogeneous technologies of variable security thresholds. Additionally the same article identifies the new generation of end user equipment as a potential *trojan horse*, since the provided functionalities allow the spreading of malicious software through virus, worms, spam and calls, that can be used to violate integrity and authorization or to consume the available bandwidth, degrading the quality of service.

In [47], the authors study the possible availability threats against LTE networks, including DoS, jamming, HSS saturation and DDoS attacks. The authors analyse the feasibility of this type of attacks alongside with the potential impact, concluding that the LTE must not only reassure privacy, confidentiality and authentication, but explicitly resolve the availability threats. Furthermore, the authors of [48] suggest that despite the proposed solutions for the aforementioned threats, there are remaining vulnerabilities of the LTE and LTE-Advanced networks, that impose significant security risks.

5 Conclusions

Through this study, the evolution of the identified security threats and vulnerabilities, throughout the various developed and deployed digital mobile communication systems was presented. Starting with the first generation of GSM and moving forward to UMTS and LTE, it was clarified that although the provided level of security was significantly enhanced, a variety of high impact attacks is still feasible. It is noticeable that mobile communication systems are inherently vulnerable to some specific attack types, such as denial of service, with various implementation methods and attack points. The study of the identified vulnerabilities of each system alongside with the defined exploitation methods, is a valuable asset towards the definition of the required security measures, for the next generation systems.

References

[1] R. Shirey, "Internet Security Glossary, Version 2." RFC 4949 (Informational), Aug. 2007.

[2] 3GPP, "Security aspects," TS 02.09, 3rd Generation Partnership Project (3GPP), June 2006.

[3] 3GPP, "3G security; Security architecture," TS 33.102, 3rd Generation Partnership Project (3GPP), June 2008.

[4] 3GPP, "3GPP System Architecture Evolution (SAE); Security architecture," TS 33.401, 3rd Generation Partnership Project (3GPP).

[5] "Groupe Speciale Mobile Association-Brief History of Global System for Mobile Communications & the Groupe Speciale Mobile Association." `http://www.gsma.com/aboutus/history`.

[6] M. Toorani and A. Beheshti, "Solutions to the GSM Security Weaknesses," in *Next Generation Mobile Applications, Services and Technologies, 2008. NGMAST '08. The Second International Conference on*, pp. 576–581, Sept 2008.

[7] G. Lorenz, T. Moore, G. Manes, J. Hale, and S. Shenoi, "Securing SS7 Telecommunications Networks," in *In Proceedings of the IEEE Workshop on Information Assurance and Security*, pp. 5–6, 2001.

[8] S. Gindraux, "From 2G to 3G: a guide to mobile security," in *3G Mobile Communication Technologies, 2002. Third International Conference on (Conf. Publ. No. 489)*, pp. 308–311, May 2002.

[9] A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," in *Fast Software Encryption* (G. Goos, J. Hartmanis, J. van Leeuwen, and B. Schneier, eds.), vol. 1978 of *Lecture Notes in Computer Science*, pp. 1–18, Springer Berlin Heidelberg, 2001.

[10] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," *J. Cryptol.*, vol. 21, pp. 392–429, Mar. 2008.

[11] V. Bocan and V. Cretu, "Mitigating denial of service threats in GSM networks," in *Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on*, pp. 6 pp.–, April 2006.

[12] V. Bocan and V. Creu, "Security and Denial of Service Threats in GSM Networks-PERIODICA POLITECHNICA, Transactions on AUTOMATIC CONTROL and COMPUTER SCIENCE," 2004.

[13] K. Kumar, G. Shailaja, A. Kavitha, and A. Saxena, "Mutual Authentication and Key Agreement for GSM," in *Mobile Business, 2006. ICMB '06. International Conference on*, pp. 25–25, June 2006.

[14] G. Cattaneo, G. De Maio, P. Faruolo, and U. Petrillo, "A Review of Security Attacks on the GSM Standard," in *Information and Communication Technology* (K. Mustofa, E. Neuhold, A. Tjoa, E. Weippl, and I. You, eds.), vol. 7804 of *Lecture Notes in Computer Science*, pp. 507–512, Springer Berlin Heidelberg, 2013.

[15] J. D. Golic, "Cryptanalysis of Alleged A5 Stream Cipher," in *Advances in Cryptology - EUROCRYPT '97* (W. Fumy, ed.), vol. 1233 of *Lecture Notes in Computer Science*, pp. 239–255, Springer Berlin Heidelberg, 1997.

[16] P. Ekdahl and T. Johansson, "Another attack on A5/1," *Information Theory, IEEE Transactions on*, vol. 49, pp. 284–289, Jan 2003.

[17] O. Dunkelman, N. Keller, and A. Shamir, "A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony," *Journal of Cryptology*, vol. 27, no. 4, pp. 824–849, 2014.

[18] G. Rose, "A precis of the new attacks on GSM encryption-QUALCOMM," 10 September 2003.

[19] K. Nohl, "Attacking phone privacy-Security research labs," 2010. Berlin.

[20] E. Biham and O. Dunkelman, "Cryptanalysis of the A5/1 GSM Stream Cipher," in *Progress in Cryptology âINDOCRYPT 2000* (B. Roy and E. Okamoto, eds.), vol. 1977 of *Lecture Notes in Computer Science*, pp. 43–51, Springer Berlin Heidelberg, 2000.

[21] F. van den Broek, "Eavesdropping on GSM: state-of-affairs," *CoRR*, vol. abs/1101.0552, 2011.

[22] C. Paget, "Practical cellphone spying." http://www.tombom.co.uk/blog/?p=262, August 2010.

[23] C. Paget and Karsten, "GSM: SRSLY?." http://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html, December 2009.

[24] Y. Song, K. Zhou, and X. Chen, "Fake BTS Attacks of GSM System on Software Radio Platform," *Journal of Networks*, vol. 7, no. 2, 2012.

[25] U. Meyer and S. Wetzel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks," in *Personal, Indoor and Mobile Radio Communications, 2004. PIMRC 2004. 15th IEEE International Symposium on*, vol. 4, pp. 2876–2883 Vol.4, Sept 2004.

[26] P. S. Pagliusi, "A Contemporary Foreword on GSM Security," in *Proceedings of the International Conference on Infrastructure Security*, InfraSec '02, (London, UK, UK), pp. 129–144, Springer-Verlag, 2002.

[27] A. Castiglione, R. De Prisco, and A. De Santis, "Do You Trust Your Phone?," in *E-Commerce and Web Technologies* (T. Di Noia and F. Buccafurri, eds.), vol. 5692 of *Lecture Notes in Computer Science*, pp. 50–61, Springer Berlin Heidelberg, 2009.

[28] M. Petracca, M. Vari, F. Vatalaro, and G. Lubello, "Performance evaluation of GSM robustness against smart jamming attacks," in *Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on*, pp. 1–6, May 2012.

[29] M. Ståhlberg, "Radio jamming attacks against two popular mobile networks," in *In: Helsinki University of Technology Seminar on Network Security. (2000*, 2000.

[30] 3GPP, "Security Objectives and Principles," TS 33.120, 3rd Generation Partnership Project (3GPP), Apr. 2001.

[31] 3GPP, "3G security; Security threats and requirements," TS 21.133, 3rd Generation Partnership Project (3GPP), Jan. 2002.

[32] 3GPP, "Guide to 3G security," TR 33.900, 3rd Generation Partnership Project (3GPP), Dec. 1999.

[33] 3GPP, "3G Security; Report on the design and evaluation of the MILENAGE algorithm set; Deliverable 5: An example algorithm for the 3GPP authentication and key generation functions," TR 33.909, 3rd Generation Partnership Project (3GPP), July 2001.

[34] J. Daemen and V. Rijmen, "AES Proposal: "Rijndael, AES algorithm submission"," September 1999.

[35] H. Gilbert and M. Minier, "A collision attack on 7 rounds of Rijndael," *The Third AES Candidate Conference, printed by the National Institute of Standards and Technology*, pp. 230–241, April 2000.

[36] S. Lucks, "Attacking Seven Rounds of Rijndael Under 192-bit and 256-bit Keys," *The Third AES Candidate Conference, printed by the National Institute of Standards and Technology*, pp. 215–229, April 2000.

[37] N. Fergusoon, "Improved Cryptanalysis of Rijndael," *The preproceedings of the Fast Software Encryption Workshop*, April 2000.

[38] D. Perez and J. Pico, eds., *A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications*, Taddong-securtity in depth-Black Hat DC, January 2011.

[39] G. Kambourakis, C. Kolias, S. Gritzalis, and J. Hyuk-Park, "Signaling-Oriented DoS Attacks in UMTS Networks," in *Advances in Information Security and Assurance* (J. Park, H.-H. Chen, M. Atiquzzaman, C. Lee, T.-h. Kim, and S.-S. Yeo, eds.), vol. 5576 of *Lecture Notes in Computer Science*, pp. 280–289, Springer Berlin Heidelberg, 2009.

[40] A. Bais, W. Penzhorn, and P. Palensky, "Evaluation of UMTS security architecture and services," in *Industrial Informatics, 2006 IEEE International Conference on*, pp. 570–575, Aug 2006.

[41] U. Meyer and S. Wetzel, "A Man-in-the-middle Attack on UMTS," in *Proceedings of the 3rd ACM Workshop on Wireless Security*, WiSe '04, (New York, NY, USA), pp. 90–97, ACM, 2004.

[42] F. Ricciato, A. Coluccia, and A. DâAlconzo, "A review of DoS attack models for 3G cellular networks from a system-design perspective," *Computer Communications*, vol. 33, no. 5, pp. 551 – 558, 2010.

[43] M. Khan, A. Ahmed, and A. Cheema, "Vulnerabilities of UMTS Access Domain Security Architecture," in *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2008. SNPD '08. Ninth ACIS International Conference on*, pp. 350–355, Aug 2008.

[44] 3GPP, "Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE)," TR 33.821, 3rd Generation Partnership Project (3GPP), Jan. 2008.

[45] Y. Park and T. Park, "A Survey of Security Threats on 4G Networks," in *Globecom Workshops, 2007 IEEE*, pp. 1–6, Nov 2007.

[46] R. Jover, "Security attacks against the availability of LTE mobility networks: Overview and research directions," in *Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on*, pp. 1–9, June 2013.

[47] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," *Communications Surveys Tutorials, IEEE*, vol. 16, pp. 283–302, First 2014.