© 2015 IEEE
Presented at The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, 20-22 August, 2015
Will be available in IEEE Xplore®

Towards 5G Security

Günther Horn, Peter Schneider
Nokia Networks
München, Germany
guenther.horn@nokia.com, peter.schneider@nokia.com

***Abstract*—This paper discusses potential security requirements and mechanisms for 5G mobile networks. It does not intend to do so exhaustively, but rather aims at initiating and spurring the work towards a 5G security architecture.**

Keywords—security; 5G; mobile network protection;

I. Introduction

While mobile networks of the second and third generations, such as GSM and UMTS, will be still much in use for quite some time to come in many regions of the world, and the deployments of the fourth generation, commonly referred as LTE, are still significantly growing, there is no doubt that work towards the fifth generation, 5G, has gained a lot of momentum. As the NGMN Alliance puts it in its recent white paper [1], 5G addresses the demands of 2020 and beyond, and "is expected to enable a fully mobile and connected society and to empower socio-economic transformations in countless ways". For this, new levels of performance in terms of throughput, latency, and connectivity density are required, but, at the same time, as [1] continues, the "enhanced performance is expected to be provided along with the capability to control a highly heterogeneous environment, and capability to, among others, ensure security and trust, identity, and privacy".

Besides protecting the privacy of subscribers and the confidentiality and integrity of their communication, also the protection of the network itself against any forms of cyber attacks is of paramount importance. In particular, a superior degree of network availability is required to support future use cases like control of critical infrastructures, car traffic control or remote surgery. At the same time, communication networks are more and more becoming the target of cyber attacks, ranging from small local security breaches using simple exploits to highly sophisticated operations carried out at a global scale with what appears to be close to unlimited resources. In the past years, OpenSource projects have provided open implementations of radio baseband stacks, and more and more security researchers or hackers have turned their attention towards mobile networks, resulting in a number of "proof of concept" attacks exploiting vulnerabilities in the implementation or configuration of mobile network nodes.

Additional exposure of future mobile networks to attacks must be expected from the trend away from implementing mobile network functions on dedicated platforms using proprietary software and hardware. Simply speaking, using more and more regular information technology (IT) for platforms to implement network functions exposes those functions to all the vulnerabilities that may be present in IT equipment and the crowd of hackers that are familiar with discovering and possibly exploiting such IT vulnerabilities. Similarly, telco-specific protocols have already given way to all-IP technology, which also increases the vulnerability to hackers.

An important factor to be taken into account is the long time frame that holds for 5G. Considering the expected start of deployment in 2020, and the longevity of former mobile network generations such as GSM, 5G networks may well be in use at times when major, even disruptive, advances in computing technology, in particular in the field of quantum computing, could allow breaking crypto algorithms that have been considered "future-proof" until now.

Considering all this, it is obvious that in 5G networks security must be "built-in". When designing 5G networks, architectural considerations must be accompanied with respective security considerations, and such security considerations are expected to influence architectural decisions.

In line with this goal, this paper raises a number of questions that need to be addressed in the design of 5G networks. While we do not believe that it is already necessary to give final answers to these questions, we feel it is important to make the 5G architects aware of them and start discussion on them.

In the remainder of this paper, we first outline our current view of the most important 5G security requirements (section II). After a brief discussion of the relation of 5G to existing systems (section III), we examine a number of potential 5G security mechanisms in more detail (section IV) and discuss briefly security aspects of new network paradigms such as virtualization and software defined networking (section V). We conclude our paper with some proposals for the next steps towards specifying the 5G security architecture.

II. Requirements

A. *Influence of General 5G Requirements*

A significant part of the work on 5G today naturally is dedicated to the discussion of use cases and requirements. Obviously, general 5G requirements can be highly relevant for the 5G security architecture. For example, a requirement to initiate communication extremely fast will have impact on

how and how often authentication and key agreement procedures are executed in the respective use cases. Moreover, a general flexibility requirement could also be applicable to the security mechanisms and procedures supported in 5G.

B. Potential Security Requirements

Clearly, there will be also dedicated security requirements. We begin by revisiting the LTE security requirements in [2]:

- Confidentiality of user and device identity (also providing location privacy)
- Entity authentication (mutual authentication and key agreement between mobiles and the network)
- Signaling data confidentiality and integrity
- User data confidentiality (not in LTE: integrity)
- Security visibility and configurability
- Platform security requirements

We assume that all these requirements will hold in some form also for 5G. Furthermore, security requirements that were discussed, but not adopted, for UMTS or LTE may be re-discussed. (Parts of this discussion are captured in [3].) These comprise user data integrity, non-repudiation (e.g. for service requests) and protection against active attacks on the subscriber identity confidentiality (aka "IMSI catching").

Further improvements on the security provided by LTE networks may also be considered, like more robustness against Denial of Service (DoS) attacks in the control plane or against the radio interface. Adoption of new networking paradigms like Network Function Virtualization (NFV) and Software Defined Networking (SDN) may further raise requirements aiming at properly securing these techniques.

It is beyond the scope of this paper to provide a comprehensive list and discussion of all potential 5G security requirements. However, in sections IV and V below, we provide a more detailed discussion on some of them.

C. Flexible Security

Flexibility is a general 5G requirement that could apply also to security. Taking user plane security as an example, some applications may not want to rely on security provided by the network, but may rather use end-to-end security. Underlying network-terminated security would not provide a higher degree of security to the applications, but may have an impact on delay or resources on the terminal. Other applications, however, may want to rely on user plane security supported by the network, and may even need user plane integrity protection in addition to encryption. To adapt to those varying security requirements, rather than enforcing user plane protection, the network may allow applications to select the way the user plane is protected.

It is clear, however, that it must be guaranteed that the network operator's infrastructure remains protected from abuse even when security can be flexibly selected by the application.

III. Should 5G Security Build on LTE?

LTE has so far not exhibited any significant security weaknesses, so it seems natural to use LTE security, cf. [4], as a starting point for research into 5G, considering the vast base of LTE networks expected for the time of introduction of 5G. On the other hand, the 5G security architecture will critically depend on the overall 5G system architecture, which will be designed during the next years but is largely unknown today.

For security, it may not matter so much whether the 5G (physical layer) radio interface follows a clean slate approach or not, as security is, in our view, likely to be provided above the physical layer also in 5G. (But we are aware of ongoing research efforts in wireless physical layer security, cf. e.g. [5].) But the architectures of radio access networks and core networks and the trend towards virtualization will be crucial for anwering questions about e.g. the termination points of security associations extending from the terminals into the network.

Backwards compatibility requirements, e.g. regarding the access of legacy terminals to 5G networks and vice versa, will also have a strong influence on the 5G security design and complexity, and so will requirements on mobility (seamless or not) between different generations of mobile systems.

Furthermore, additional security requirements, as discussed in section II, may have to be taken into account.

Finally, in addition to the 3GPP specified radio access technologies, also security concepts from other radio technologies, such as Wi-Fi (i.e. IEEE 802.11), may be relevant for mobile operators, for example for traffic offload. The relevant specification for carrier grade deployments is the Wi-Fi Alliance's "HotSpot 2.0" specification [6], which specifies the use of strong security mechanisms.

IV. Discussion of Potential Security Mechanisms for 5G

In this section, we discuss security mechanisms that may be potentially useful to address the security requirements listed in section II above. Nothing is fundamentally new, and some of it, like public-key based authentication, has even already been discussed during the design of UMTS security in the mid 1990s; but it is certainly worth revisiting the previous arguments in the light of the new architectural and service requirements for 5G and the changed threat landscape.

A. User Identity and Device Identity Confidentiality

In GSM, UMTS, and LTE, the permanent user identity is the IMSI (International Mobile Subscriber Identity). The mechanism employed for user identity confidentiality has remained the same across these three technologies: they provide protection against passive, but not active attacks.

The situation with the confidentiality of the device identity, the IMEI (International Mobile Equipment Identity), is a little different: in GSM and UMTS, the network, and hence an attacker, may request in an unprotected message that the IMEI be sent in the clear, while the IMEI shall be sent in LTE only in a confidentiality-protected message. This feature is certainly worth keeping in 5G.

The protection against passive attacks on the IMSI, i.e. mere eavesdropping, is achieved through the use of temporary identities, which are assigned in an encrypted form when the terminal attaches to the network and updated at regular intervals in order to prevent tracing of the user. It should be noted that confidentiality of signalling is required for the mechanism to work.

However, in order to prevent a permanent lock-out of the subscriber when the temporary identities in the terminal and the network get out of synch, e,g, through a crash of an entity, the subscriber can be requested to contact the network using his permanent identity.

An active attacker can exploit this mechanism to perform so-called IMSI catching, i.e. harvest the IMSIs of all subscribers in the vicinity of the attacker's false base station. In GSM, the attacker can even go further and eavesdrop on the subscriber's traffic by downgrading to weak or no encryption. The latter is not possible in UMTS or LTE due to the mandatory use of signalling integrity.

IMSI catching attacks were known already when UMTS was designed, and they were re-discussed during the LTE design phase. For a discussion see e.g. clause 5.1.1.2 of [3] where public key methods (with the public key owned by the visited or the home network), symmetric key methods and the use of pseudonyms are mentioned as potential countermeasures. All these countermeasures have issues, and none of them has finally been adopted in UMTS or LTE, but it may be worth revisiting the arguments.

B. Mutual Authentication and Key Agreement

Authentication corroborates the identity of the other party at the moment the authentication protocol is run. In order to provide continued assurance about the identity of the other party in ongoing communications, authentication between UE (User Equipment) and network has to be always coupled with key agreement. From the agreed keys, further keys have to be derived that are then used to provide confidentiality and integrity for signalling and user data. The possession of the confidentiality and integrity keys then implicitly proves the identity of the other party.

The authentication and key agreement protocols used in UMTS and LTE are called AKA. UMTS AKA provides a guarantee to the subscriber that it is connected to a network entity authorised by the home network, which, together with signalling integrity, prevents the false base station attacks possible in GSM. EPS AKA, which is used in LTE, is almost identical to UMTS AKA, except that EPS AKA provides an additional guarantee to the subscriber about the identity of the serving network.

UMTS AKA was first proposed to 3GPP in 1999, EPS AKA in 2007 . No security vulnerabilities of UMTS AKA or EPS AKA have become known since. Besides being secure, UMTS AKA and EPS AKA are also efficient:

- The messages are short compared to other authentication protocols;
- Only one handshake between UE and serving network and between serving network and home network is required;
- The HSS (Home Subscriber Server) does not need to keep protocol state as the HSS just responds to a request from the serving network and updates its data base, which completes the instance of the authentication protocol from the HSS point of view. There is no need for the HSS to wait for another response from the serving network. This allows the HSS to handle large numbers of requests efficiently.
- The protocol is symmetric-key-based; this makes the computations required in the Authentication Centre, which is part of the HSS, and in the USIM (Universal Subscriber Identity Module) very efficient compared to public-key-based mechanisms.

Investigations into further evolution of authentication and key agreement mechanisms for 5G should, of course, not be precluded, but the above-mentioned properties, together with the fact that EPS AKA is widely deployed, make EPS AKA the benchmark against which new proposals have to be measured.

One possible further development would be the use of public-key-based mechanisms for authentication and key agreement in 5G. In fact, the use of such mechanisms for authentication and key agreement in mobile networks has been under discussion since the mid-1990s when UMTS was being prepared. Several public-key-based proposals were made to the standardisation group ETSI SMG5, which at the time was responsible for preparing UMTS (before this responsibility was handed over to 3GPP founded in 1999). One can find such proposals also in scientific publications appearing around that time, e.g. in [7].

Advantages of the use of public-key-based authentication and key agreement schemes could include that the home network does not need to be contacted for each authentication or that non-repudiation could be provided, e.g. for the purposes of non-repudiable billing. It was already mentioned in a previous section that the user identity confidentiality could be protected against active attacks in this way.

In addition, more recently, the use of permanent symmetric keys as a basis for authentication and key agreement in mobile networks was questioned as a result of the alleged attacks by powerful agencies against the SIM provision process (cf. 'The Great SIM Heist' [8]). It was claimed that a property called Perfect Forward Secrecy (PFS) could have helped in thwarting these attacks. PFS is typically provided using a form of the Diffie-Hellman (DH) mechanims. The use of DH would force an attacker to play man-in-the-middle at the time of eavesdropping. However, it needs to be very carefully investigated whether this attack would justify a fundamental change in the paradigm for authentication in mobile networks Furthermore, possibilities of strengthening the security of provisioning procedures for symmetric keys and efficiency aspects need to be taken into account.

Another aspect that needs to be considered in 5G is the storage of credentials on the UE side. Today, the long-term credentials, i.e. the (symmetric) permanent authentication keys, are stored in the USIM, which is an application on the UICC (Universal Integrated Circuit Card), a smart card platform. Present UICCs are removable and pre-provisioned with credentials for one operator. A change of operator is only possible by changing the UICC. This may be cumbersome or even prohibitive especially for devices used for machine-type communication that are not attended by humans. Therefore, ETSI and the GSMA have developed the concept of embedded UICCs [9] that allows remote provisioning of new sets of credentials. Embedded UICCs may further ease the implementation of the UE as there no longer is the requirement of removability of the smart card. However, embedded UICCs are not yet in widespread use, and, hence, no corresponding experience is available. It has also been under discussion to not use UICC, but 'soft SIMs', meaning that the credentials would be stored on the terminal, either in regular non-volatile memory or in some form of Trusted Platform Module. A thorough investigation of the security, technical and commercial implications of soft SIMs is, however, not known to us. Commercial aspects might include that network operators would be no longer in full control of the subscribers' credentials.

C. Security between Terminal and Network

Signalling integrity is indispensable for preventing impersonation of users and networks. Signalling confidentiality is currently required for providing user identity confidentiality, as discussed in a previous section. The amount of signalling data sent in a mobile system is mostly very small compared to the amount of user data. Therefore, in general, the processing capacity needed for providing signalling data confidentiality and integrity does not seem to have a serious impact on the overall capacity. There may be, however, use cases that may warrant special investigation, e.g. when very small amounts of data are infrequently sent by machine-type applications.

Furthermore, an issue that may need further investigation for 5G is the time needed for setting up security contexts. (For example, in idle-to-connected transitions in LTE, delay is introduced by setting up security between terminal and base station.) This may matter for very delay-sensitive applications.

Another aspect worth remembering is that there is a distinction in LTE, as opposed to UMTS, between NAS layer signalling (NAS = Non-Access Stratum extending between the UE and the core network) and AS layer signalling (AS = Access Stratum extending between the UE and the base station). This prevents base stations that may have been compromised e.g. by a physical attack, from accessing the NAS signalling – a threat that was not present in UMTS, as UMTS radio interface security reaches beyond the UMTS base stations, up to the radio network controller. It may be easily overlooked that this division also provides a strengthening of security in LTE over UMTS because the NAS security context may be always available in the UE and the network, even when the UE is deregistered, while the AS security context is only available when the UE is in connected mode. Hence the latter needs to be explicitly set up when the UE changes into connected mode, which has the consequence that, without an additional NAS security context, some signalling messages between the UE and the network cannot be protected when there is no existing AS security context. This became evident in a discussion on an attack using fake paging responses, which can be easily thwarted in LTE [10] by ignoring paging responses with incorrect integrity protection. We mention this so that this aspect is taken into account in the 5G discussions, not because we believe that no reasonably secure system could be designed without this separation between AS and NAS signalling security.

Regarding user plane security, the reader is referred back to the considerations in section II C.

D. Security on Network Interfaces

Currently, 3GPP specifications mandate (under certain conditions) using IPsec to protect core and backhaul interfaces. For the core network interfaces, only signalling protection is addressed while the protection of the backhaul link is also specified for the user plane. Questions to be discussed here for 5G include whether this different treatment of the user plane for backhaul and core network interfaces is still justified in 5G. The questions also include whether protection mechanisms at layers different from the IP layer would be needed. These questions can only be answered once more about the 5G architecture is known; as of yet, it is not fully clear whether the distinction between backhaul and core network interfaces still makes sense in 5G, which non-IP protocols would be used on which interfaces, and whether these interfaces would require separate protection.

E. Security Visibility and Configurability

In existing mobile networks, it is the network that decides on the security features and algorithms applied. The choice typically applies to all users in the same way (providing the UE capabilities support it). In particular, the network may choose to not activate encryption due to legal constraints in the country of operation; or the network may support only certain algorithms. Since GSM, specifications therefore demand that the user shall have the possibility to see whether encryption is applied (through a so-called ciphering indicator [11]). Unfortunately, it seems that the number of terminal types supporting a ciphering indicator is decreasing. Furthermore, some operators choose to suppress the use of a ciphering indicator by setting a suitable bit on the SIM or USIM.

Further forms of security visibility have been envisaged, but never implemented, such as the use of certain strong or weak algorithms (which would matter especially for GSM where some algorithms still in use have been badly broken).

Security configurability, on the other hand, is, according to [2] "the property that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation." However, the only use case explicitly mentioned in [2] is "enabling/disabling user-USIM authentication". In 5G, there may be a need to extend the concept of security configurability: it was mentioned further

above that, in 5G, the user may enjoy more flexibility regarding the security features to be applied to the user's communication session, depending on the needs of the application and the user's security policy, cf. section II. This would imply that the user can tell the network, which security features should be enabled. Questions to be discussed in this context may differ between human-attended terminals and machine-type terminals. The questions may include whether users have sufficient awareness of consequences of security decisions or whether security should be rather transparent to users. Furthermore, selecting security features based on application needs may also require a formalisation of security policies and corresponding automated security decisions in the user equipment. Threats through mobile malware interfering with this process may also have to be discussed in this context.

F. Platform Security

The LTE specifications mention the need for secure execution environments and trusted platforms in two places: in TS 33.401 [2] for eNBs, and, in a much more detailed way, for Home eNBs in TS 33.320 [12]. It needs to be discussed what type of platform requirements would be appropriate for 5G. This can be decided only once more is known about the envisaged types of base stations and their deployment scenarios, as well as the termination points for 5G security in the network.

Furthermore, also platforms for network functions in the core may require secure execution requirements, which is particularly critical in virtualized environments, cf. section V.

G. Protection against Denial-of-Service Attacks

Denial-of-Service (DoS) attacks aiming at exhausting resources at the victim are very common in the Internet today, targeted mostly against web services. As mobile networks become increasingly important as parts of the critical infrastructure, they are also becoming a very relevant potential target for DoS attacks as acts of cyber crime, cyber terrorism or even cyber warfare.

A specific threat for mobile networks are DoS attacks carried out by mobiles, for example by a mobile botnet. Mobiles may, in particular, attack control plane elements, like the MME (Mobility Management Entity) or the HSS in 4G networks. As an example, [13] presents an attack against an HLR (Home Location Register) that can be carried out by rather simple means. Better availability of protocol stacks (in form of OpenSource software) that can be expected for the future will further lower the hurdles for external attackers and thus increase the likelihood of serious DoS attacks carried out by mobile botnets.

Another type of DoS attack that is specific to wireless communication is radio interface jamming. While simply blocking frequency bands by transmitting a signal with high power, more smart and stealthy jamming attacks against 3GPP-specified mobile networks can be carried out by selectively blocking control channels essential for the overall operation of the radio interface. While a single jamming device will only cause locally restricted DoS, a smart jamming attack carried out by a regular mobile could have much more impact, if the attacker for example managed to acquire a botnet of mobile devices that he could turn into jamming devices.

It is well known that DoS attacks, in particular distributed DoS attacks (i.e. coordinated attacks from many distributed sources), are hard to counter. Measures such as limiting the rate of incoming traffic from other networks, in particular the Internet, or blocking offending sources temporarily provide limited protection and may be applied in 5G networks like in today's mobile networks. Control plane protocols between mobiles and the network should be designed in a way that the effort required at the network side is as low as possible during the phase when the network cannot be sure that the request is legal. Moreover, overload protection mechanisms must be implemented ensuring that network functions remain operational in the presence of any amount of requests.

Countering the threat of smart jamming, potentially even by a botnet of mobiles, will require cooperation between radio and security researchers.

To summarize, we believe that DoS attacks will pose one of the major threats to future 5G networks, and that investigation on how to mitigate this threat should be one of the major security research topics during the next years.

V. USAGE OF NFV AND SDN

There is a clear trend visible in the evolution of mobile networks towards the adoption of the concepts of NFV and SDN. These techniques are already being applied to existing mobile networks, but in 5G, much stronger adoption in all areas of the network, including the radio access network, can be expected. While a comprehensive and detailed discussion of this issue is far beyond the scope of this paper, we still want to raise some points we consider important.

With NFV, network functions become virtual network functions (VNFs) and are no longer isolated from each other in dedicated hardware. Instead, isolation fully relies on the virtualization layer, which, as a complex software system, cannot be expected to be flawless. So it may be useful to investigate, design and implement ways to control the allocation of software components to physical computing resources, in a way that retains the capability to use available hardware efficiently and be able to dynamically scale VNFs according to changing capacity demands. Such an approach would for example allow isolating certain VNFs by preventing other software components to run on the same physical computing blade.

Network security concepts typically rely on separating traffic types, such as user, control and management traffic. Moreover, often network zones are distinguished, like handling traffic arriving from external networks in dedicated parts of the network separated from network parts where only internal nodes have access. Such concepts can clearly be transferred into an NFV environment. For example, hypervisors support the instantiation of virtual switches providing VLANs (Virtual Local Area Networks) for interconnecting VMs (Virtual Machines) on a computing blade. Also the networking layer within and between racks

holding the computing blades typically supports approaches for logical traffic separation. Security devices such as firewalls required between different network zones, or intrusion detection and prevention systems, can be implemented as VNFs and fulfill their tasks like in traditional network setups.

A relevant issue with NFV is software integrity protection. Images of VNF implementations must be readily available in the cloud, in order to support dynamic on demand instantiation of new VNF instances. Integrity and confidentiality protection is for sure a requirement here. A secure boot as well as runtime software integrity protection of a traditional network element may rely on specific hardware trust anchors, and the question arises, how this approach has to be transformed when the network function is now implemented as a VNF, meant to be launchable on any of the commodity computing blades forming a telco cloud.

Within a (possibly distributed) datacenter, connectivity may be enabled by means of SDN. SDN is not restricted to this, but may also be used to control wide area networks. In 5G networks, depending on the architectural decisions, SDN may apply to fronthaul or backhaul networks, or more generally, to wide area networks interconnecting the various, distributed sites implementing the radio access network and core cloud(s). SDN comprises the separation of the control plane from the forwarding plane, allowing to implement SDN controllers as logically centralized network functions within a cloud. Moreover, SDN comprises programmability, meaning that an SDN controller may allow various applications to execute control over forwarding plane resources via an application programming interface (API) or via a protocol interface.

While SDN is supposed to bring significant advantages in terms of flexibility, agility, automation and efficiency of network control, possible security threats must not be neglected but suitably be mitigated by protection measures. In particular, an SDN controller running in a cloud is a highly attractive target for attacks. An SDN controller may not only be compromised via a flaw in the virtualization software, but also via an API or protocol interface it exposes to applications. Very careful hardening of such interfaces as well as proper authentication and authorization concepts for applications accessing the SDN controller seem essential therefore.

While such potential security threats of SDN and usage of a cloud pose some risk and must carefully be mitigated, on the positive side, SDN and the cloud may also bring security advantages for 5G networks. As an example, flexible, scalable allocation of resources to a VNF may help significantly in overcoming certain DoS attacks, which are otherwise difficult to counter. The programmability provided by SDN may allow deploying security solutions very flexibly and efficiently, running as applications on top of SDN controllers. Last but not least, both NFV and SDN may support the automation of tasks that otherwise need to be done in a more manual style and thus could be more prone to human errors inducing security vulnerabilities.

VI. Conclusion and next steps

Work towards the fifth generation of mobile networks has gained a lot of momentum recently. As 5G research projects, for example in the framework of the EU's 5G Public Private Partnership [14] have already started or are about to start, and 5G activities in standardization bodies, in particular 3GPP, have already been scheduled, it is important to start also the work on the security architecture, in order to ensure that security is built into 5G networks right from the start. Important steps will be the clarification of the security requirements, the review of existing security architectures, in particular the LTE security architecture, and finally the selection of the 5G security measures in tight interworking with the design of the general 5G network architecture. With this paper, we go one step in this direction and hope to promote the overall work towards a sound 5G security architecture.

References

[1] Next Generation Mobile Network Alliance, "5G White Paper", Version 1.0, Feb 17, 2015.

[2] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[3] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE)".

[4] D. Forsberg, G. Horn, W.-D. Moeller, V. Niemi: "LTE Security", 2nd ed., Wiley, 2013.

[5] IEEE Communications Magazine, Issue: "Wireless Physical Layer Security", to appear in June 2015, http://www.comsoc.org.

[6] Wi-Fi Alliance® Technical Committee Hotspot 2.0 Technical Task Group, "Hotspot 2.0 (Release 2) Technical Specification".

[7] G. Horn, B.Preneel: "Authentication and Payment in Future Mobile Systems", ESORICS 1998, Lecture Notes in Computer Science 1485, Springer-Verlag, pp. 277–293, 1998.

[8] "The Great SIM Heist", The Intercept, 2015, https://firstlook.org/theintercept/2015/02/19/great-sim-heist/

[9] "Remote Provisioning Architecture for Embedded UICC. Technical Specification. Version 2.0", October 2014, www.gsma.com.

[10] Change Request to 3GPP TS 24.301, CP-130799, ftp://ftp.3gpp.org/tsg_ct/TSG_CT/TSGC_62_Busan/Docs/.

[11] 3GPP TS 22.101: "Service aspects; Service principles".

[12] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[13] Patrick Traynor et al., "On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core", Proceedings of the 16th ACM conference on Computer and communications security, 2009

[14] 5G PPP home page: http://5g-ppp.eu/.