Private Identification of Subscribers in Mobile Networks: Status and Challenges

Stig F. Mjølsnes and Ruxandra F. Olimid

Abstract

The privacy of individuals in the context of mobile networks is crucial nowadays. Nevertheless, too few improvements have been made over the years to secure the privacy of subscribers. As a consequence, current generations of mobile networks, including 4G/LTE, are susceptible to sensitive information leakage. In particular, the individuals are exposed to location disclosure and movement tracking by revealing the subscribers' permanent identifiers. In this article, we discuss the subscribers' private identification problem in light of the recent standardization for 5G. We introduce the problem and discuss existing cryptographic solutions, with a focus on the ECIES-based solution adopted for 5G. We then investigate to what extent the privacy protection mechanisms introduced by the 5G security architecture answer our problem. Finally, we identify challenges, and we distinguish domains of interest and specific research activities to address these challenges.

Introduction

Digital privacy for individuals gained special attention lately, being subject to new privacy regulations. The General Data Protection Regulation (GDRP), adopted by the EU Parliament in 2016, was enforced in May 2018 [1]. Meanwhile, a proposal for a Regulation on Privacy and Electronic Communications is under discussion [2]. In this context, the support for the privacy of subscribers in mobile communication networks becomes crucial. However, privacy has been proved hard to achieve in mobile communication networks over the years. Current generations of mobile networks, including 4G/LTE, are susceptible to sensitive information leakage. In particular, they expose the subscribers' permanent identifiers to unauthorized parties. Naturally, this allows testing for the presence or absence of subscribers in a geographical area by collecting the subscribers' persistent identities. Furthermore, advanced attacks can track the movements of mobile subscribers. These attacks show that the consequences of exposing the permanent identifiers are severe.

In the absence of suitable protection mechanisms, the growing number of connected devices in the fifth generation of mobile communication (5G) would entail increased exposure for damages to user privacy. In this context, smart-phones, smart-watches, and a variety of emerging wireless wearables would intensify the privacy concerns and risks associated with users' traceability by being used at a larger scale. Moreover, the development of the Internet of Things (IoT) would bring new privacy challenges in the business sectors too, such as sensor networks (with high impact for healthcare applications when data is available through remote access) and vehicle-to-vehicle communication (e.g. identification and tracking of cars).

In the standard subscription model, a subscriber must declare and prove his identity to access the mobile network. But this should not damage the user's privacy in any way. Under these circumstances, the problem of the subscriber's identifier exposure in mobile networks needs to be solved. Hence, the following question arises: *How can a subscriber privately transmit its identity over the mobile communication network?* The problem itself is not new but continuously in the interest of both researcher and practitioners. We have described the problem in more technical terms before [3], and other researchers studied it in different technologies (e.g., RFID communication [4]). Our previous work [3] discusses the problem in existing mobile networks including 4G/LTE, while this article extends the discussion to 5G. In particular, it provides insights into how the 3rd Generation Partnership Project (3GPP) recently addressed the problem in the security architecture specifications for 5G [5] and came with a countermeasure to existing attacks such as IMSI Catchers, location disclosure and movement tracking [6,7,8]. We maintain the problem of subscribers' private identification open to a broad range of solutions, investigate to what extent these solutions answer the problem, and discuss their limitations. We examine the adopted solution for 5G [5,9], discuss possible limitations and weaknesses, and identify new challenges and research directions. We intend this article to be a starting point for further research motivated by a pressing practical problem.

This article is organized as follows. In the next section, we give the background. Then, we classify the possible adversarial and attacks types and define the problem of subscribers' private identification in mobile networks. Next, we present and analyze solutions, outlining a very recently adopted solution for 5G. Finally, we discuss security aspects, identify challenges and specific research directions.

Stig F. Mjølsnes is with NTNU - Norwegian University of Science and Technology, Trondheim, Norway.

Ruxandra F. Olimid is with University of Bucharest, Romania and NTNU - Norwegian University of Science and Technology, Trondheim, Norway.

Background

A *mobile communication network* provides voice and data services to subscribers that connect via a wireless link. The network coverage is organized in *cells*. A cell is a geographical area served by a transceiver called *base-station*. A *User Equipment* (UE) is a device (e.g., smartphone) equipped with a tamper-resistant chip that stores and process identifiers and authentication data that corresponds to the profile of one subscriber in the core of the *Home Network* (HN). The terminology from 3G/4G refers to this chip as *Universal Subscriber Identity Card* (USIM). A UE attaches to the "best" base-station in its vicinity and uses it as an access point to the *serving network*. The serving network usually belongs to the subscriber´s operator, being also the *home network*. If roaming mode is enabled, the serving network can be a different operator; if so, it is called the *visiting network*. The visiting network communicates with the home network to allow the UE access to mobile services. Figure 1 shows a simplified three-tier architecture of mobile communication networks.

The serving network initiates a mutual authentication procedure before granting access. A unique permanent identifier called *International Mobile Subscriber Identity* (IMSI), and a permanent subscriber cryptographic key are inputs for the subscriber's identification and authentication. The first 5 or 6 decimal digits of the IMSI – the Mobile Country Code (MCC) and the Mobile Network Code (MNC) – uniquely identify the home network. For security reasons, the cryptographic key never leaves the USIM, nor the database of subscribers in the home core network. The same does not apply for the IMSI, which the UE sends at the very beginning of the authentication procedure. Subsequently, the serving network provides a *Temporary Mobile Subscriber Identity* (TMSI) over a cryptographically secured wireless link. The IMSI is used instead of the IMSI to minimize the exposure of the IMSI on the wireless link. A TMSI value is periodically refreshed accordingly to the serving's network security policy.

The Problem of Private Identification

The following two subsections classify adversaries and attacks against mobile communication networks and introduce the subscribers' private identification problem.

Adversarial Types and Attacks

There are two main types of adversaries in mobile communication networks: (1) *passive adversaries*, which can only eavesdrop the communication; (2) *active adversaries*, which, in addition to eavesdropping, can actively disrupt the communication (e.g., inject, delete, or modify messages). Passive adversaries can damage privacy by sniffing sensitive data sent over the communication channel [6,7]. Active adversaries can mount more powerful attacks, such as provoking UEs to submit identifiers in clear (IMSI Catching) or detecting and tracking the location of UEs [7].

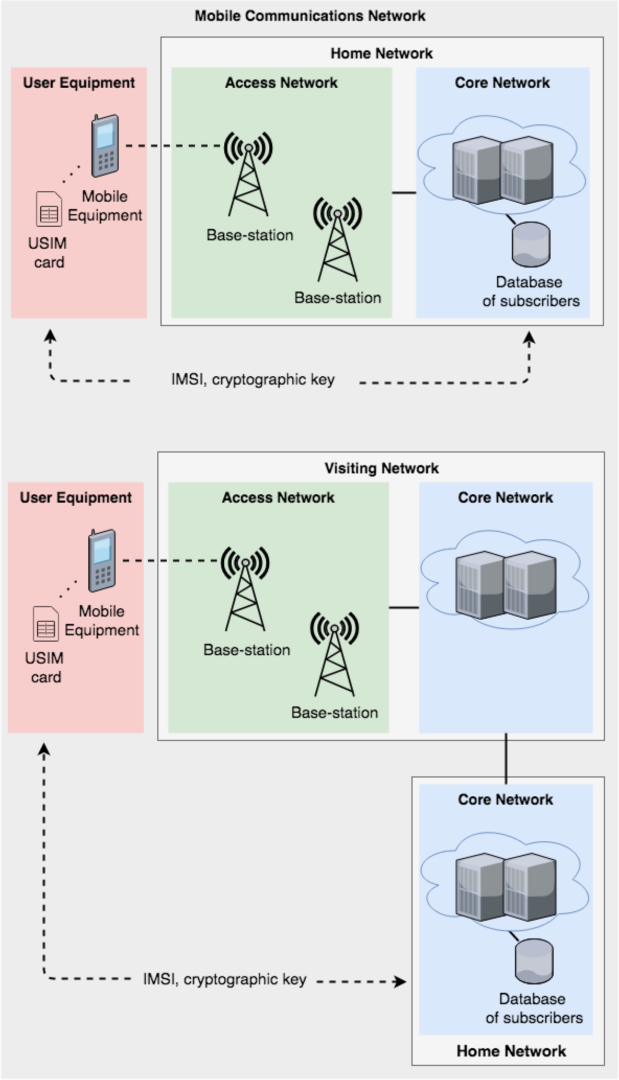

Figure 1 Generic three tier architecture of mobile networks: the mobile user equipment, the access network, and the core network. Top: Access via the home network. Bottom: Roaming via a visiting network

Passive Attacks. Passive attacks are in principle feasible because with suitable tools an adversary can eavesdrop the wireless link at a distance. Cryptographic protocols can successfully prevent communication content disclosure to some extent, but there are (always) network management messages and channel signals that are sent in clear before a secure channel is established. Although these do not threaten the subscribers' privacy directly, they are usually prerequisites for active attacks.

Moreover, a mobile access network uses *paging messages* to locate and activate user devices, for instance for incoming calls. These messages contain the identifier of the UE, and are broadcast within a cell or tracking area and can be exploited by eavesdroppers as a direct source of identification and tracking of subscribers [7,9].

Active Attacks. Active attacks demand more skills and resources than passive attacks, but they are feasible at large scale. IMSI Catchers - attack devices that successfully query the permanent identity of UEs - are easily accessible because of available open source software and low-cost hardware such as Software Defined Radio (SDR). Today, the cost to build an IMSI Catcher is less than $3,000 and the operational skills required are minimal [3]. The IMSI Catchers exploit a long-standing breach in the security architecture of mobile networks, which was recognized by 3GPP in the technical specifications leading up to the fourth generation Long-Term Evolution (LTE): *"[... the base-station ...] requests the user to send its permanent identity. The user's response contains the IMSI in cleartext. This represents a breach in the provision of user identity confidentiality"* [10]**.** In other words, whenever the serving network sends an *Identity Request* asking for the permanent identity of the UE, the UE will reply with the IMSI in cleartext. This fallback procedure solves the problem of the first attach to the network (before the UE has a TMSI), and the synchronization problem if the TMSI is lost. But a rogue base-station can forge the *Identity Request* at any time to collect IMSIs. There is currently no mechanism for a UE to distinguish between an authentic and a forged *Identity Request.* Figure 2 shows the basic functionality of an IMSI Catcher.

Rupprecht et al. systemize these and other attacks, together with their root causes in [11]. Strong security mechanisms and agile management are necessary to combat these attacks. Reactive defenses such as *detections* are useful, but they cannot prevent attacks (e.g., the adversary caught the IMSIs before the IMSI Catcher itself is discovered), so proactive defenses must be considered.

THE PROBLEM DEFINITION

To access mobile services, the UE must send its identity to the network. However, this should not jeopardize the privacy of the subscriber in the presence of adversaries. So, the *private identification problem* arises. A *private identification protocol* is a protocol that allows the UE to successfully identify itself to the mobile network without damaging the privacy of the subscriber, nor breaking the security of the communication [3]. Naturally, the protocol must protect the IMSI and the associated cryptographic key, and it must stand against *location disclosure* and *movement tracking.* This means that an adversary cannot test the presence or absence of the UE in an area, cannot find the UE's position, and cannot track its movement in time. To some extent, an adversary can damage privacy if it can decide whether messages and actions originate from the same subscriber. Hence, the protocol should grant the *unlinkability* property too. All these properties must hold for multiple executions of the protocol, regardless of whether the communication sessions are successful or not, consecutive or not, authentic or fake.

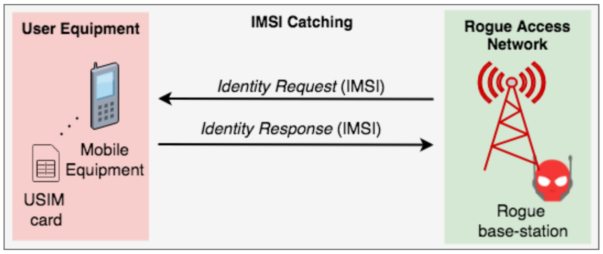

Figure 2 IMSI Catching: a rogue base station forges *Identity Request* messages to collect IMSIs

In the context of mobile networks, it is natural to require secrecy and integrity of the IMSI and the cryptographic key at both the subscriber and the network operator (the USIM must be tamper-resistant, and the core network must be properly secured). Hence, we are mainly concerned with the privacy of parameters in transit. Finally, a good solution to the private identification problem should not depend on a central trusted authority, but only use bi-directional communication between a UE and the serving network. From a practical perspective, no (or minimal) changes in the architecture of the mobile network are of interest.

SOLUTIONS

With unbounded computational power, the problem of private identification is easy. But, in practice, mobile devices and even network elements cannot perform expensive computations efficiently. Moreover, the solution must scale beyond millions of subscribers without notable delay for the end user. Scalability must be considered a decisive factor, especially in the context of 5G and the emerging wireless IoT. From a computational perspective at the network side, constant time protocols (i.e., protocols for which the running time is independent of the number of subscribers) are ideal. Even linear time protocols (i.e., protocols for which the running time is linear in the number of subscribers) become very inefficient at large scales.

We further analyze various solutions from a cryptographic perspective, where private identification protocols can be *symmetric*, *asymmetric,* or *hybrid.*

Symmetric Solutions. The security architectures of mobile networks preceding 5G are built using symmetric key cryptography. Each subscriber has a permanent cryptographic key, which is stored both in the USIM and in the core home network. The subscriber key is further derived to obtain ephemeral keys used to establish secure channels. Under these settings, a scalable solution to the private identification problem is not trivial.

If the protocol is *stateless* (i.e., the UE and the network do not maintain a synchronized state), then only the IMSI can be used for identification. But, to protect privacy, the IMSI cannot be sent in clear. However, encrypting it, for instance using the permanent key (or a derivation of it), results in a

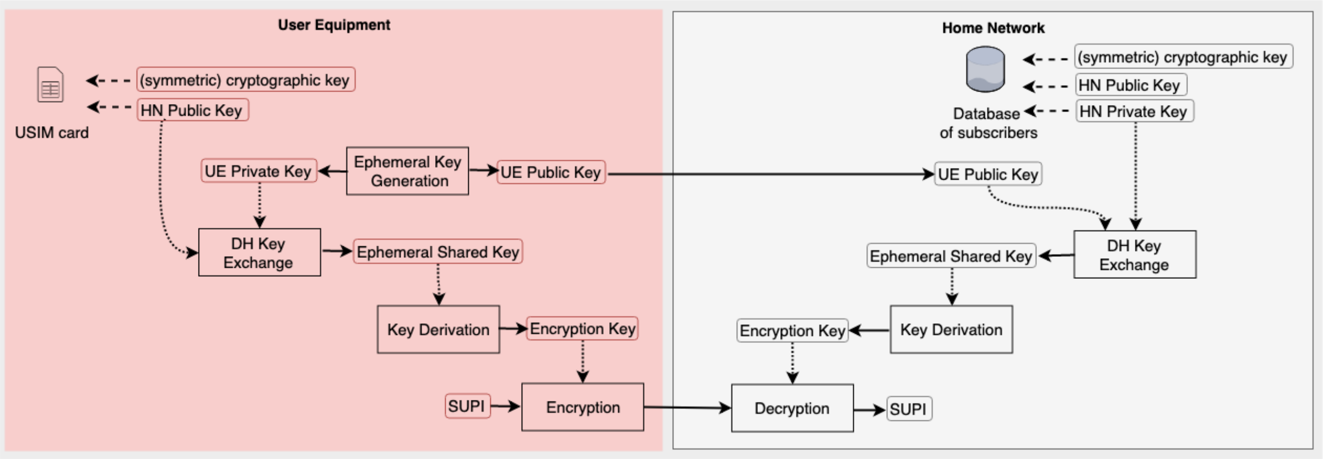

Figure 3 Concealment of SUPI in 5G

paradox: the network needs the key to decrypt the IMSI, but at the same time it needs the IMSI to identify the corresponding decryption key in the database [4]. An alternative is brute force: try all possible keys until the ciphertext decrypts to the correct IMSI. But this is a linear time solution, so it becomes very inefficient at large scale. Besides, this will open up the possibility for a denial-of-service attack by an adversary that floods the network with ciphertext requests. For more details and related solutions, see [3].

If the protocol is *stateful* (i.e., the UE and the network maintain a synchronized state), then temporary identifiers can be used for identification in constant time. However, stateful symmetric protocols suffer two main shortcomings by design [4]. In current mobile networks, the main temporary identifier is the TMSI. The first shortcoming is that the network renews the TMSI after authentication only. So, whenever the UE is outside radio coverage or in countries without roaming agreements with the home operator, then the UE always replies with the same TMSI. The second and more important concern is the recovery procedure when synchronization is lost: the UE falls back to sending the IMSI in clear. Of course, a fallback procedure must be in place, but it should not expose the IMSI. As we showed in Figure 2, IMSI Catchers exploit this design flaw: a rogue base-station masquerades synchronization loss, starts the recovery procedure, and collects the IMSI in clear.

Asymmetric and Hybrid Solutions. An elegant way to solve the problem of private identification is to use asymmetric cryptography. In an asymmetric key solution, the network operator generates a pair of cryptographic keys: a public key and a private key, and transmits the public key to all subscribers. The UE sends its identifier encrypted under the home operator's public key, and the home network decrypts using its corresponding private key. Therefore, stateless asymmetric protocols can solve the problem in constant time. In the case of mobile networks prior to 5G, 3GPP has analyzed asymmetric solutions and decided to accept the privacy risks rather than adopt public key cryptography, because of the complexity it introduces in the network. But things change for 5G.

Researchers from Ericsson Research and KTH Stockholm conducted a practice study on the usage of public key cryptography computations by commodity mobile devices [9]. They claim asymmetric encryption of IMSI is feasible without significantly affecting the functionality and delay of user services, by experimenting with an Android implementation of Elliptic Curve Integrated Encryption Scheme (ECIES). (To be precise, the authors experimented with an implementation of ECIES*, a variant of ECIES without a Message Authentication Code). As a consequence, the idea was recently accepted by 3GPP and introduced in the technical specifications TS 33.501 that describe the security architecture for 5G [5]. Figure 3 shows a simplified version of the process. The permanent identifier in 5G is called *SUbscription Permanent Identity* (SUPI), but it maintains the scope and the functionality of the IMSI. Whenever the UE needs to make its SUPI known to the network, the parties agree on an ephemeral shared key using *asymmetric Diffie-Hellman* (DH) key exchange over elliptic curves. To run the DH key exchange, both the UE and the home network need a pair of public and private keys. The home network owns a long-term pair of keys *(HN Public Key, HN Private Key)*, and the USIM is pre-provisioned with the public key of the home network (*HN Public Key)*. On the other hand, the UE generates an ephemeral pair of keys *(UE Public Key, UE Private Key)* every time it needs to transmit the concealed SUPI. The ephemeral keys generated by the UE introduce randomization, which is necessary for security. The UE uses its ephemeral private key (*UE Private Key)* and the public key of the home network (*HN Public Key)* stored in the USIM to generate the ephemeral shared key. This ephemeral shared key is further derived into an encryption key by a key derivation function. Finally, the UE encrypts the SUPI using the encryption key and transmits the ciphertext over the network. On the network side, the encryption key is derived similarly. The home network receives the ephemeral public key of the UE (*UE Public Key)* and inputs it together with its private key (*HN Private Key*) in the DH key exchange to derive the ephemeral shared key. By construction, DH key exchange guarantees that the output key for the UE and the home network is the same. The home network further derives the symmetric encryption key (using the same key derivation function as the UE), decrypts the received ciphertext and finds the SUPI.

Except for the UE, the home network is the only party that can derive the correct key for decryption. In roaming, the serving network has to forward the ciphertext to the home network for decryption, so it needs to know the identity of the home network. For this, the UE transmits the home network identity MCC and MNC in clear, along with its ephemeral public key and the encryption of the SUPI.

Similar to previous generations of mobile systems, the network allocates a 5G-TMSI to the UE when authentication succeeds. So, the elliptic curve computations are executed only if the network cannot identify the UE by the 5G-TMSI. When a valid temporary identifier is available, the symmetric subscriber cryptographic key remains provisioned in the USIM, as with 4G.

Regarding privacy protection of the broadcast paging messages, there are not many references in the technical specifications. The single mention is that 5G-TMSI should be refreshed after the UE replies to a *Paging Request* [5]. However, protecting the identity in the paging messages can be done in the same way as explained previously [9].

Discussion

Although the 3GPP standardization consortium was aware of the privacy risks introduced by exposing the permanent identifier of subscribers, no protection mechanism was adopted prior to 5G. At the time, the added technical complexity was considered to be improperly justified by the perceived security threats. Things changed for 5G, and after several solutions were analyzed [12], one privacy protection mechanism has been introduced in the 5G security architecture [5]. The accepted solution avoids the complexity introduced by a Public Key Infrastructure (PKI), and this was an essential point for its selection. Supposedly, the new European regulations for fundamental privacy rights [1,2] reinforced the technical spurs to strengthen subscribers` privacy, in the light of the technological progress that brings the possibility to build low-cost IMSI Catchers. Another aspect is the increased computational power of wireless devices that enables complex computation without noticeable delay time for the end user. Likely these factors triggered a change in the mindset and previously disregarded asymmetric solutions have been adopted in 5G.

But the technical problem remains open in purely symmetric key settings: *Does it exist an efficient symmetric solution to the private identification problem?* If yes, it might be a better alternative than the hybrid system adopted in 5G. In general, symmetric solutions are more efficient and thus preserves longer battery life than asymmetric solutions, which is very important for constrained IoT devices (e.g., sensors). Another aspect in favor of symmetric encryption is the simplicity of key management. No architectural changes would be required if the permanent key (or its derivations) stored in the USIM can be sufficient for private identification. Finally, in contrast to the established asymmetric cryptographic algorithms, symmetric cryptography is considered to be secure against quantum computer attacks, so a post-quantum secure protocol is designed with less effort in the symmetric settings.

Strengths of the adopted ECIES-based solution include reasonable computation time (meaning longer battery life for the mobile device) and practicable key size (meaning fewer radio resources used for communication) [12]. The scheme has a formal security proof that claims security under some computational assumptions, but there is room for discussion regarding some practical aspects and implementation best practices.

First, ECIES is not resistant to post-quantum cryptanalysis. If (when) quantum computers become a reality, the key agreement scheme in ECIES will have to be replaced by a post-quantum cryptographic protocol [12]. Substantial research work is currently seeking efficient post-quantum asymmetric key cryptography. A quantum-resistant alternative for the Diffie-Hellman key exchange will benefit many other applications too.

Second, the UE still transmits parameters such as the home network's identifier in clear over the network. *Does the exposure of MCC and MNC affect subscribers' privacy? If yes, does it exist an efficient way to hide the identity of the home network (to all parties except the serving network)?* In essence, MNC and MCC are not very sensitive parameters, but they can reveal individuals with a particular profile. For example, MCC can be used to identify individuals by the country of origin, which might be of interest when the targeted individuals are traveling abroad. A natural way to hide MCC and MNC is by encryption. A simple solution in the asymmetric settings is to encrypt them with the public key of the visiting network. But the public key needs to be certified, which brings in the complexity of PKI. Attribute-Based Encryption (ABE) might be a good candidate to solve this, by allowing the UE to encrypt using the public attributes of the visiting network. But ABE also brings a significant drawback: a trusted authority needs to generate and distribute the private keys used for decryption. Alternatively, distributing trust among the operators is hard to manage, and the renewal of keys becomes complex. In fact, ABE proposals have been analyzed as candidates for a complete privacy solution but lost the race [12].

Third, the security architecture for 5G leaves important decisions to the network operator, such as the provisioning and the renewal of *HN Public Key* in the USIM [5,12]. *How often should the network operator refresh its public and private key pair? How is the public key of the home operator renewed in the USIM?* A good practice might be that the public key is never renewed in the USIM, and changed by USIM replacement only. If so, the operator might use

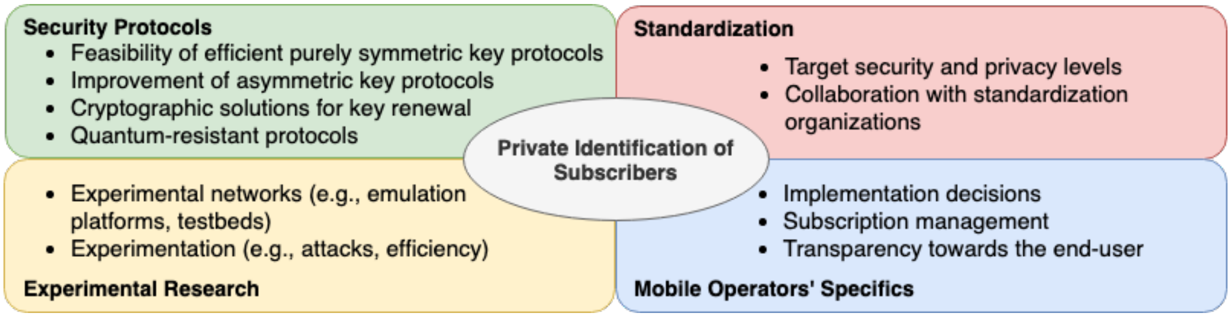
Security Protocols
Feasibility of efficient purely symmetric key protocols
Improvement of asymmetric key protocols
Cryptographic solutions for key renewal
Quantum-resistant protocols
Standardization
Target security and privacy levels
Collaboration with standardization organizations
Private Identification of Subscribers
Experimental networks (e.g., emulation platforms, testbeds)
Experimentation (e.g., attacks, efficiency)
Experimental Research
Implementation decisions
Subscription management
Transparency towards the end-user
Mobile Operators' Specifics

Figure 4 Research domains and specific research directions

distinct keys for different subscribers, depending on their lifetime in the network. As a consequence, the operator needs to manage the key disablement and a customer-friendly replacement of expired USIMs. This is a safe approach that excludes all risks associated with transmitting the renewed key over the wireless link, in particular, a wireless man-in-the-middle attack that tries to impersonate the network and place its public key in the USIM.

Finally, the security architecture for 5G does not guarantee universal privacy for the subscribers: "*Subscriber privacy enablement shall be under the control of the home network of the subscriber*" [5]. This leaves the decision of implementing the privacy policy to each network operator: "*If the home network has not provisioned the public key in USIM, the SUPI protection in initial registration procedure is not provided. In this case, the null-scheme shall be used by the ME [Mobile Equipment]"* [5]. The null-scheme means no protection. It needs to exist for special situations such as emergency access, but it leaves space for security breaches too. The responsibility is left entirely to the network operator, which can choose between the null-scheme, two predefined ECIES-based profiles, or implement proprietary protection mechanisms [5]. The two predefined profiles discard backward compatibility, which we consider a positive point. Backward compatibility is usually a weakness that opens up the possibility of known attacks. From a user perspective, it is unclear if the 5G subscriber will know whether the privacy mechanism is activated or not. Similar to previous network generations, standards recommend to show which security mechanisms are in place on the user's device, but the device manufacturers and the network operators commonly neglect to implement this.

A recent update to the security architecture for 5G brings a significant change: "*In response to the Identifier Request message, the UE never sends the SUPI*" [5]. Under these circumstances, *will IMSI Catchers be possible in 5G?* To answer this question, we need to investigate new ways of attack, different from the ones used in 4G/LTE. We estimate that considerable work needs to be done once the technical specifications become stable and practical experiments can be done.

The current standardization of the embedded Subscriber Identity Module (eSIM) is highly relevant to our problem investigation. The eSIM replaces the physical card with a chip embedded into the mobile device. An eSIM allows multiple subscription profiles, belonging to the same or different operators, to co-exist. Only one profile can be enabled at a time. A high number of profiles may bring some flexibility in terms of pseudonymity, but it is clear that this alone can be used to accommodate a high privacy level. In more general terms, *Can new distribution schemes for subscription profiles (e.g., eSIM) facilitate subscribers' privacy or, to the contrary, 5G subscription schemes will make privacy more challenging to preserve?*

RESEARCH DIRECTIONS

We envision a research roadmap for the mobile network privacy problems, in particular, the private identification problem detailed in this article. The research priorities are extrinsically motivated by the emerging international privacy regulations. We distinguish four main domains, illustrated in Figure 4. For each domain, we identify specific research activities directly related to our main problem. The activities principally derive from the questions raised in the preceding Discussion section. Note that our research questions entail activities in multiple domains.

Security protocols. Security protocols, perceived as a generalization of cryptographic protocols, are the central pillar of privacy enhancements. Research priorities include the design and analysis of privacy-enhancing protocols, with emphasis on efficiency. Examples of specific directions of research include improving the existing asymmetric key solutions, checking the feasibility of purely symmetric key solutions, building cryptographic solutions for key renewal and designing post-quantum cryptographic protocols.

Experimental research. Efficiency depends on the technical capabilities of devices, and theoretical results should be validated by practical testing. Access to 5G devices and experimental networks (including emulators and testbed environments) are crucial for the confirmation of privacy results. Research priorities include the development of open-source 5G platforms for experimentation with protocol efficiency and attacks validation.

Standardization. Standardization plays a decisive role in the subscribers' privacy, by establishing the expected security and privacy level as a tradeoff with usability.

Research priorities include working together with the standardization organizations and manufacturers, proposing research results to the standards committees, contributing to the evaluation and testing of various proposals.

Mobile operators' specifics. Many network security implementation decisions are left to the mobile operator. An in-depth analysis of how and to what extent the implementation decisions or the subscription management (e.g., renewal of the cryptographic keys) influence subscribes' privacy is a research direction by itself. Also, the study of the best practices for providing increased transparency for the end-user (e.g., make the user aware of the actual privacy level and mechanisms) is of significant interest to regulatory authorities and consumer organizations.

Conclusions

This article discusses the problem of subscribers' private identification in the context of mobile networks. In the absence of proper security mechanisms to avoid identity exposure, attacks such as subscribers' location disclosure and movement tracking become possible. In particular, all generations of mobile networks up to 4G/LTE have been proved vulnerable to IMSI Catchers. In the context of the increased number of wireless wearable devices in 5G and the development of IoT, and in the light of new privacy regulations, the 5G security architecture adopts an asymmetric solution to the private identification problem. We find that employing asymmetric cryptography comes naturally because of the lack of symmetric key solutions and the increased computational capabilities of current mobile devices. However, concluding that the privacy of the overall identification mechanism in 5G holds is still premature. Further investigation needs to be done once the technical specifications are stable, and hands-on experimentation becomes possible at a larger scale. We have discussed different technical approaches to the problem and state-of-the-art solutions, and we have identified further research directions. Finally, we note that the possibility of building an efficient purely symmetrical protocol to solve the problem remains an open problem, and we highlight the long-term need to accommodate a post-quantum secure scheme.

References

[1] European Parliament and Council, General Data Protection Regulation (GDPR), Available online : https://eugdpr.org/ ; Accessed on: October 2018.

[2] European Comission, "Proposal of a Regulation on Privacy and Electronic Communications", Available online: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications; Accessed on: October 2018.

[3] S.F.Mjølsnes, R.F.Olimid, "The Challenge of Private Identification" in *Proceedings of the International Workshop on Open Problems in Network Security (iNetSec)*, 2017, pp. 39–53.

[4] B. Alomair, R.Poovendran, "Privacy versus Scalability in Radio Frequency Identification Systems" in *Computer Communications*, vol. 33, 2010, pp. 2155–2163.

[5] 3GPP Technical Specification, TS 33.501: "*Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system*", Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169 ; Accessed on: October 2018.

[6] M.Lichtman, R.P.Jover, M.Labib, R.Rao, V.Marojevic, J.H.Reed, "LTE/LTE-A Jamming, Spoofing, and Sniffing: Threat Assessment and Mitigation" in *IEEE Communications Magazine*, 54(4), 2016, pp.54-61.

[7] I.Bojic, Y.Yoshimura, C.Ratti, "Opportunities and Challenges of Trip Generation Data Collection Techniques Using Cellular Networks" in *IEEE Communications Magazine*, 55(3), 2017, pp.204-209.

[8] S.F.Mjølsnes, R.F.Olimid, "Experimental Assesment of Private Information Disclosure in LTE Mobile Networks" in *Proceedings of the 14th International Joint Conference on e-Business and Telecommunications vol.6, SECRYPT (ICETE 2017)*, 2017, pp. 507–512.

[9] E.C.Jiménez, P.K.Nakarmi, M.Näslund and K.Norrman, "Subscription Identifier Privacy in 5G Systems" in *Selected Topics in Mobile and Wireless Networking (MoWNeT),* 2017, pp.1-8.

[10] 3GPP Technical Specification, TS 33.401: "*3GPP System Architecture Evolution (SAE); Security architecture*", Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2296 ; Accessed on: October 2018.

[11] D.Rupprecht, A.Dabrowski, T.Holz, E.Weippl, C.Pöpper, "On Security Research towards Future Mobile Network Generations", in *IEEE Communication Surveys & Tutorials*, 20(3), 2018, pp.2518-2542.

[12] 3GPP Technical Requirement: TR 33.899, "*Technical Specification Group Services and System Aspects; Study on the security aspects of the next generation system*", Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045 ; Accessed on: October 2018.

Stig Frode Mjølsnes (stig.mjolsnes@ntnu.no) is professor at the Department of Information Security and Communications Technology, Norwegian University of Science and Technology (NTNU). He is founder and research group leader of the NTNU Applied Cryptology Lab. He received the doctoral degree on cryptographic protocols and digital cash in 1990, and the Master`s degree in physical electronics in 1980. His research interests are centered around crypto-protocols and their privacy applications to the communication world at large. His anthology book *A Multidisciplinary Introduction to Information Security* presents a wide technical perspective of the ICT security field. He holds memberships in IEEE, ACM, and IACR since 1985.

Ruxandra F. Olimid (ruxandra.olimid@fmi.unibuc.ro) is Lecturer at the Department of Computer Science, University of Bucharest and Adjunct Associate Professor at the Department of Information Security and Communication Technology, Norwegian University of Science and Technology (NTNU). She received her Ph.D. in Computer Science from the University of Bucharest in 2013. She has background in both computer science (BSc and MSc from the University at Bucharest, 2008 and 2010) and telecommunications (BSc from the University Politehnica of Bucharest, 2009). Her research interests include cryptography and privacy, with current focus on security and privacy in communication networks.