Chapter 1

Introduction

Privacy has been a concern for people since the ancient times. Exposure of many of the activities such as movement, access to resources, usage behaviour, etc., of a person may lead to his/her risk of physical security as well as security of his/her resources. Ones activities may be revealed if his identity is known to the adversaries [1]. Hence, the confidentiality of ones identity is of paramount importance.

According to a recent press release of The World Bank, around three-quarters of the World’s inhabitants now have access to a mobile phone [2] and the number is increasing with every passing day.

These days, a subscriber uses a mobile phone to access variety of services including voice, rich communication services, and value added services. These services are used for making important communications, accessing valuable resources, and for carrying out financial transactions, because of which a mobile phone is becoming an important tool for an individual’s existence. Therefore, the need to protect an individual’s identity that is used in a mobile system is as important as the need to protect other important personal identities like social security number and bank account numbers.

A common practice among mobile operators to extend their services beyond their own service area is to establish roaming agreements with third party operators [3]. Roaming allows a subscriber of one operator to use the services of another operator when inside the latter’s coverage area. The trust model
Chapter 1. Introduction

adopted for roaming in mobile systems developed by Third Generation Partnership Project (3GPP), a collaboration of reputed organisations that is responsible for developing some popular and market winning mobile systems, does not protect the identity privacy of the subscribers from the visited/serving networks. In fact, the visited/serving networks that may often belong to third party operators are required to be trusted with the identity of the subscribers. Such trust requirement makes roaming agreements between operators difficult as it requires elaborate trust agreement amongst them, thereby limiting the ease and span of extending an operator’s services beyond its own circle or zone [4]. Moreover, it makes the identity privacy of the subscriber vulnerable to eavesdroppers (over an unencrypted wireless link) and fake serving networks. The study reported in this thesis, aims at improving identity privacy of the subscriber of a 3GPP mobile system while relaxing the trust requirement for roaming between operators.

1.1 Subscriber Identity in Mobile Systems

In mobile networks, each subscriber is registered with a home network. During registration, the subscriber is assigned a Subscriber Identity Module (SIM) that contains a unique and a permanent identity called the International Mobile Subscriber Identity (IMSI) that identifies the subscriber. The IMSI is a number (Figure 1.1) that constitutes of a maximum of 15 decimal digits [5]. The first 3 digits are the Mobile Country Code (MCC), which is followed by the Mobile Network Code (MNC) (either 2 digits, in case of European standard or 3 digits, in case of North American standard). The length of the MNC depends on the value of the MCC. The remaining digits are the Mobile Subscription
Chapter 1. Introduction

Identification Number (MSIN) [6]. Thus,

\[ IMSI = MCC||MNC||MSIN \]  

where, '||' denotes concatenation. The IMSI is used by the home network to uniquely identify each and every subscriber for authentication, authorisation and billing purposes. The MCC identifies the country of domicile of the mobile subscriber, whereas the MNC identifies the home network of the mobile subscriber. The MSIN is used to uniquely identify a subscriber within the subscriber's home network.

1.2 Subscriber Identity Privacy in Mobile Systems

Identity Privacy is considered a standard security requirement in any mobile telecommunication system [7][8][9]. The identity privacy of a subscriber is compromised if his/her permanent identity (i.e., the IMSI) is exposed to an adversary. Knowledge of the IMSI may allow an adversary to track and amass comprehensive profiles about individuals - where, data about movement, usage, etc., of a subscriber is collected over a period of time and linked with his/her IMSI. Such profiling may expose an individual to various kind of unanticipated risks and above all will deprive an individual of his privacy. Thus, with more and more people accessing voice, Internet, rich communication services, value added services, mobile banking, mobile commerce, etc., through mobile networks, the importance of identity privacy cannot be underestimated.

1.3 3GPP Mobile Systems: An Overview

3GPP is a collaboration of six influential telecommunications standard development organisations worldwide (ARIB of Japan, ATIS of USA, CCSA of China, ETSI of France, TTA of Korea and TTC of Japan). The original scope of 3GPP was to produce Technical Specifications (TSs) and Technical Reports (TRs) for
a third generation (3G) mobile system that is based on a second generation (2G) mobile telecommunication system called the Global System for Mobile Communication (GSM). The scope was subsequently amended to include the maintenance and development of TSs and TRs for GSM and evolved radio access technologies (e.g., General Packet Radio Service (GPRS) and Enhanced Data rates for GSM Evolution (EDGE)). The technologies standardised by 3GPP are constantly evolving through generations of mobile systems. Since the completion of the first Long Term Evolution (LTE) specification, 3GPP has become the focal point for mobile systems beyond 3G. In this section, we present an overview of some prominent mobile systems developed by 3GPP, viz.: Universal Mobile Telecommunication System (UMTS), LTE, interworking between 3GPP System and WLAN (3GPP-WLAN) and Non 3GPP Access to the EPS (Non3GPP-EPS).

1.3.1 UMTS

UMTS is a 3G mobile system developed and maintained by 3GPP. It has evolved from the GSM standard and therefore borrows heavily from the established network architecture of GSM. In fact, many of the network elements used in GSM are reused (with some enhancements) in UMTS. The radio access network, however, in UMTS is significantly different from that of GSM, GPRS, and EDGE. In UMTS, the radio access network is known as the Universal Terrestrial Radio Access Network (UTRAN). The components that make up the UTRAN are significantly different from the corresponding elements in the GSM architecture. It supports both circuit switched and packet switched connections for real time and data communication services respectively [10]. It uses Wideband Code Division Multiple Access (W-CDMA) radio access technology to offer greater spectral efficiency and bandwidth compared to its 2G counterpart (i.e., GSM). It includes two of the air interface proposals submitted to the International Telecommunications Union (ITU) as proposed solutions to meet the requirements laid down for International Mobile Telephony 2000 (IMT-2000). One solution uses Frequency Division Duplex (FDD) and the other uses Time Division Duplex (TDD) [11]. In the FDD option, paired 5-MHz carriers are used in the uplink and downlink
(1920 MHz to 1980 MHz for uplink and 2110 MHz to 2170 MHz for downlink). For the TDD option, a number of frequencies have been defined, including 1900 MHz to 1920 MHz and 2010 MHz to 2025 MHz.

1.3.2 LTE

The increase in demand for higher data rates and quality of service due to emergence of applications such as MMOG (Multimedia Online Gaming), mobile TV, Web 2.0, etc., have inspired the 3GPP to work on the Long Term Evolution (LTE). LTE is the latest standard in the mobile network technology tree that previously realised the GSM/EDGE and UMTS network technologies [12]. LTE is designed to meet the continued demand for cost reduction and to ensure the continuity of competitiveness of the 3GPP systems for the future.

LTE, whose radio access network is called Evolved Universal Terrestrial Radio Access Network (E-UTRAN) [13], substantially improves end-user throughputs, sector capacity and reduces user plane latency, bringing significantly improved user experience with full mobility [14]. With the emergence of Internet Protocol (IP) as the protocol of choice for carrying all types of traffic, LTE provides support for IP-based traffic with end-to-end Quality of service (QoS). Voice traffic is supported mainly as Voice over IP (VoIP) enabling better integration with other multimedia services.

As a part of its System Architecture Evolution (SAE) initiative, 3GPP has specified a new flat IP based core network called the Evolved Packet Core (EPC) to support the E-UTRAN through a reduction in the number of network elements, simpler functionality, improved redundancy and allowing connections to other fixed/wireless access technologies, giving the service providers the ability to deliver a seamless mobility experience.

LTE is designed to meet aggressive performance requirements that rely on physical layer technologies, such as, Orthogonal Frequency Division Multiplexing (OFDM), Multiple-Input Multiple-Output (MIMO) systems and smart antennas to achieve these targets. The main objectives of LTE are to minimise the system and user equipment complexities, allow flexible spectrum deployment in existing
or new frequency spectrum, and to enable co-existence with other 3GPP radio access technologies. LTE supports scalable carrier bandwidths, from 1.4 MHz to 20 MHz and supports both FDD and TDD. With LTE, the highest theoretical data rate is 170 Mbps in uplink and with MIMO the rate can be as high as 300 Mbps in the downlink.

1.3.3 3GPP-WLAN

Mobile telecommunication systems like EDGE and UMTS that are proposed by 3GPP are called 3GPP systems. 3GPP systems have large coverage, high speed mobility, efficient subscriber management, expertise in billing and nearly universal roaming. Whereas, WLAN provides hot-spot/limited coverage with a data rate much higher and cost which is much lesser than that of 3GPP systems. The combination of 3GPP systems and WLAN technologies offer the possibility of achieving any time, anywhere services, bringing benefits of both technologies to the end users and the service providers. Thus, with the intent to extend 3GPP services and functionality to the WLAN access environment, 3GPP has proposed specification for interworking between 3GPP system and WLAN [15].

1.3.4 Non3GPP-EPS

As a part of the 3GPP's LTE/SAE initiative for the evolution of GSM, EDGE and UMTS architecture, a purely IP based system called the Evolved Packet System (EPS) is standardised. E-UTRAN is the access part of the EPS whereas the EPC is its core network. In order to expand the reach of 3GPP services beyond 3GPP defined accesses, viz., GSM EDGE Radio Access Network (GERAN) of GSM/EDGE, UTRAN of UMTS, E-UTRAN of LTE, etc., 3GPP has proposed the technical specification for interworking between the EPS and accesses that were not defined by 3GPP (Non-3GPP accesses) [16]. This specification provides description for providing IP connectivity using Non-3GPP accesses, viz., World-wide Interoperability for Microwave Access (WiMAX), Code Division Multiple Access 2000 (CDMA2000), WLAN, etc., to the EPC.
1.4 Subscriber Identity Privacy in 3GPP Mobile Systems

For access security in mobile systems developed by 3GPP, an Authentication and Key Agreement (AKA) protocol is performed between the subscriber’s user equipment and the subscriber’s home network. During this procedure, both the user equipment and the home network mutually authenticate each other. To initiate the AKA procedure during roaming, the subscriber is required to present its identity to the visited/serving network through the wireless link between them, for onward transmission to the home network. Since, identity presentation during an AKA precedes all other security, a challenging task at this stage, is to protect the identity privacy of the subscriber from the visited/serving network and from eavesdroppers in the vulnerable wireless link.

In order to provide identity privacy to the subscribers in mobile systems developed by 3GPP, the permanent identity (i.e., the IMSI) of the subscriber is replaced by temporary identities and pseudonyms. Instead of the IMSI, short lived temporary identities/pseudonyms are used for identity presentation. In case of mobile systems like UMTS and LTE, temporary identities are allotted to the user equipment by the visited/serving network. Whereas, in case of mobile systems like 3GPP-WLAN and Non3GPP-EPS, pseudonyms are allotted to the user equipment by the home network. A mapping between the temporary identities and the corresponding IMSIs are also maintained by serving network (in case of UMTS and LTE) or the home network (in case of 3GPP-WLAN and Non3GPP-EPS), so that the serving/home network can resolve them back to corresponding IMSI when required. While generating temporary identities/pseudonyms, the following is ensured:

- A temporary identity/pseudonym should not have any correlation with any previously generated temporary identity/pseudonym.
- It should not be possible for anyone except the visited network (in case of UMTS and LTE) or the home network (in case of 3GPP-WLAN and Non3GPP-EPS) to resolve the corresponding IMSI from a given tempo-
1.5 Motivation of the Thesis

In this section, we discuss the vulnerabilities related with identity privacy in mobile systems developed by 3GPP. These vulnerabilities provide scope for further improvement and are the motivating factors behind the work presented in this thesis.

The trust model adopted by 3GPP for roaming requires an operator and its subscribers to have full trust on the visited/serving networks (that may even belong to third party operators). The existing mechanism for identity privacy in the AKA protocols used in 3GPP mobile systems (Section 1.4) is based on this trust requirement. As a result, the mobile systems developed by 3GPP have the following limitations:

1. In situations when the visited/serving network cannot resolve a presented temporary identity/pseudonym to its corresponding IMSI, there is a backup mechanism under which the visited/serving network has a provision to request the subscriber for its permanent identity. A subscriber has to oblige such a request by transmitting its IMSI in clear text through the radio path. Such a provision makes the subscriber vulnerable to the following types of adversaries:

   - Eavesdroppers: An eavesdropper listening to the radio link will be able see the IMSI being transmitted in clear text.

   - Impersonators/Man-in-the-middle: A man-in-the-middle can impersonate as a genuine network and after drowning the signals of the actual network with its own signals, can send a request for permanent identity to the subscriber. A response will contain the IMSI in clear text.

   - Corrupt visited/serving network: Because of the above provision, a roaming subscriber will have to trust a serving network with its IMSI,
even if the serving network does not belong to the same mobile operator as the home network. A corrupt serving network operator may take advantage of this situation by compromising the identity related information to a malicious third party.

2. To provide secured roaming services including identity privacy to the subscribers, the operators are required to set up prior trust relationships through elaborate roaming agreements with the third party operators. However, such roaming agreements limit the ease and span of extending services beyond an operator's own circle/zone.

Hence, there is need that the requirement of trust on third party operators for roaming is relaxed or even entirely eliminated.

1.6 Contributions of the Thesis

The contribution of the work reported in this thesis can be summarised as follows:

1. In order to relax trust requirement for roaming, a new trust model which is more flexible compared to the existing trust model is proposed. In this trust model, the need to trust the visited/serving network is relaxed with respect to identity of the subscriber.

2. A security extension for the AKA protocols used in 3GPP mobile systems is developed to implement the proposed trust model. In this extension, the permanent identity of the subscriber is restricted to the subscriber's mobile device and the home network. Hence, we call it End to End User Identity Confidentiality (E2EUIC). In situations when the visited/serving network cannot resolve a presented temporary identity/pseudonym to its corresponding IMSI, in E2EUIC a dynamic identity whose value keeps changing after every successful AKA is transmitted instead of the permanent identity. Advantages of E2EUIC are the following:

- There is no need to trust the serving network for identity privacy of the subscriber.
Chapter 1. Introduction

- Contrary to several recent proposals in this area, E2EUIC can be adopted as an extension to the existing AKA protocols used in 3GPP mobile systems.

- E2EUIC can be implemented at the operator's level without needing any modification in the intermediary networks.

3. Adoptions of this extension are developed for 3GPP mobile systems like UMTS, LTE, 3GPP-WLAN and Non3GPP-EPS.

4. Various analyses like statistical analysis, formal analysis, computational cost analysis, complexity analysis, space overhead analysis, communication overhead analysis and security analysis of E2EUIC are performed that establishes its robustness, correctness and effectiveness.

5. A comprehensive review of the literature has been carried out which provides an insight into the existing methodology used for identity privacy in 3GPP mobile systems and the proposed alternatives. It also helped us in formulating an approach that is different from the solutions already proposed in the literature and we believe, is more suitable for mobile systems developed by 3GPP.

1.7 Organisation of the Thesis

The thesis is organised as follows:

- In Chapter 2, the existing trust model used for roaming in 3GPP mobile systems is discussed. A new trust model that overcomes the limitations of the existing trust model is proposed in this chapter.

- In Chapter 3, a security extension called E2EUIC for the AKA protocol used in UMTS is proposed.

- In Chapter 4, the adoption of E2EUIC to the AKA protocol used in LTE is presented.
Chapter 1. Introduction

- In Chapter 5, the adoption of E2EUIC to the AKA protocol used in inter-working systems proposed by 3GPP, viz., 3GPP-WLAN and Non3GPP-EPS, are presented.

- In Chapter 6, various analyses like formal analysis, computational cost analysis, complexity analysis, space overhead analysis, communication overhead analysis and security analysis of E2EUIC are presented that establishes its robustness, correctness and effectiveness.

- In Chapter 7, a comprehensive review of the literature is performed and discussed with reference to E2EUIC.

- In Chapter 8, concluding remarks are given and some of the future research directions are highlighted.