International Journal of Modern Electronics and Communication Engineering (IJMECE) ISSN: 2321-2152
Volume No.-7, Issue No.-2, March, 2019

Simplified Roaming Pacts among Operators vis-à-vis Improved Subscriber Identity Privacy in Global Mobility Network

Hiten Choudhury
Department of Computer Science and Information Technology
Cotton University
Guwahati, Assam, India
hiten.choudhury@cottonuniversity.ac.in

Abstract: In a Global Mobility Network, every subscriber is identified by a unique identity. This identity is used for authentication, authorization and billing. Before extending any service to a subscriber, s/he has to be authenticated. Since authentication requires identity presentation, it precedes all other forms of security like confidentiality, integrity protection, etc. Thus, the subscriber has to present his/her identity through an insecure channel in plain text, before any service is extended to him/her. Ensuring identity privacy to the subscriber is therefore a challenging security issue in mobile networks. Numerous research works have been carried out to strengthen the subscriber's identity privacy in mobile networks. Early researches in this area were focused on protecting the subscriber's identity from an eavesdropper over the radio link between the user equipment and the visited network. Recent research however has gone a step ahead, by making an attempt to enhance the subscriber's privacy by protecting the subscribers' identity from even the visited network that may practically be forged or compromised. In this paper, a positive impact of this new development, in the form of simplified roaming pacts among the mobile operators, is highlighted.

Keywords: Identity Privacy, Roaming Pacts, Global Mobility Network, Mobile Operator, Mobile Network

I. INTRODUCTION

Mobile devices are becoming an integral part of an individual due to the increase in availability and popularity of a range of mobile services through global mobility networks. However, threats like location tracking and comprehensive profiling, where data about movement, usage, etc., of a subscriber is collected and linked to his/her identity to explore various attacks, have also emerged. Thus, identity privacy in mobile systems has become an important security issue.

Early researches in this area were focused on protecting the subscribers' anonymity from an eavesdropper over the radio link between the user equipment and the visited network. However, recent research has gone a step ahead, by making an attempt to enhance the subscriber's anonymity by protecting the subscriber's identity from even the visited network that may practically be forged or compromised. This, as perceived by the author, would also bring in a supplementary benefit of simplifying 'roaming agreements', which is a pact between mobile operators. This pact enables a roaming subscriber of one operator to continue having access to the mobile services while in the service area of another operator. In this paper, an effort is made to elaborate on this additional benefit.

The rest of the paper is organized as follows. In Section II, we explain the concept of identity privacy in global mobility networks. In Section III, we give an overview of the current status of identity privacy in global mobility networks with reference to a prominent network called Universal Mobile Telecommunications Network (UMTS). In Section IV, we discuss the identity privacy vulnerabilities in global mobility networks. In Section V, we discuss related work that envisages enhanced identity privacy in global mobility networks. In Section VI, we elaborate on how enhancing identity privacy may contribute in simplifying roaming agreements between operators. Finally, in Section VII, we conclude the paper.

II. IDENTITY PRIVACY

Privacy has been a concern for people since the ancient times. Exposure of many of the activities such as movement, access to resources, usage behavior, 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 one's 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.

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 (Eq. 1) that constitutes of a maximum of 15 decimal digits [3]. The rest 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 Identification Number (MSIN) [4]. Thus,

$$IMSI = MCC||MNC||MSIN \quad (1)$$

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

Identity Privacy is considered a standard security requirement in any mobile telecommunication system [5] [6] [7]. 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 kinds 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.

III. CURRENT STATUS OF IDENTITY PRIVACY IN GLOBAL MOBILITY NETWORKS

In global mobility networks, three parties are involved, viz., the user equipment that the subscriber carries with him/her (say U), the home network with which the subscriber is registered (say H), and the visited network that allows the subscriber to access mobile services while h/she is roaming outside the home networks service area (say V). U and H shares a long term secret key Ki and a set of one way hash functions (f1-f5). U communicates with V through wireless link, whereas communication between V and H happens through wired medium.

For access security in global mobility systems, an Authentication and Key Agreement (AKA) procedure, which is a challenge response mechanism, is executed between U and H. During this procedure, U and H mutually authenticate each other.

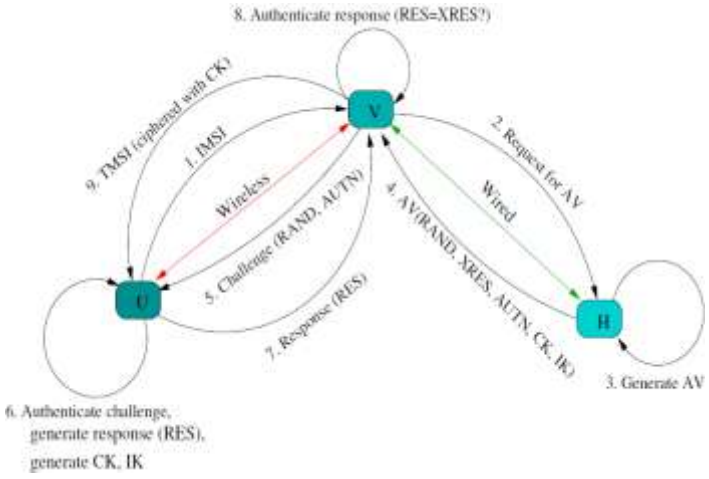

Figure 1. Authentication and key agreement procedure.

In Universal Mobile Telecommunication System (UMTS), a commercially successful global mobility network, the AKA procedure (Fig. 1) is carried out in the following two stages [8] [9]:

In the First stage, U presents its IMSI to V. With the help of IMSI, V obtains the security credentials of U in the form of an Authentication Vector (AV) from H. AV are generated using Ki and the hash functions f1-f5 (Fig. 2). It contains a random number RAND, an authentication token AUTN, an expected response XRES, a cipher key CK and an integrity key IK.

In the second stage, V utilizes AV to perform mutual authentication with U through a challenge response mechanism. To begin the process, V challenges U by transmitting RAND and AUTN. U in turn, generates response RES, CK, IK and AUTN. For this, f1-f5, RAND and Ki are used. It then authenticates V by verifying the generated AUTN against the received AUTN. After this, U sends a response to V's challenge, by transmitting RES. Finally, V authenticates U by comparing RES with XRES. At the successful end of this AKA procedure, a Cipher Key (CK) and an Integrity Key (IK) are established between U and V. These two keys enable communication over the otherwise vulnerable radio link (between U and V) to happen in a secured and reliable way.

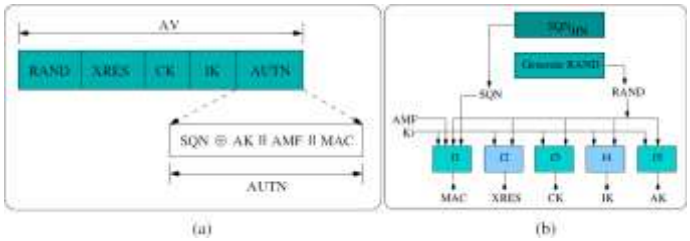

Figure 2. AV generation.

Since, identity presentation during an AKA precedes all other security, in the first stage, U is forced to send its identity (IMSI) in clear text to V through the vulnerable wireless link between them. This makes identity privacy of the subscriber vulnerable to eavesdroppers in wireless link.

In order to provide identity privacy to the subscribers in prominent global mobility systems like UMTS, LTE, etc., the permanent identity (i.e., the IMSI) of the subscriber is replaced by pseudonyms. Instead of the IMSI, short lived pseudonyms are used for identity presentation. Pseudonyms are allotted to U by V. A mapping between a pseudonym and its corresponding IMSI is maintained by V, so that V can resolve it back to corresponding IMSI when required. While allocating pseudonyms, the following is ensured:

- A pseudonym should not have any correlation with any previously generated pseudonym.
- It should not be possible for anyone except V to resolve the corresponding IMSI from a given pseudonym.
- A pseudonym is allotted to U only after a secured channel is established between U and V.

IV. IDENTITY PRIVACY VULNERABILITIES IN GLOBAL MOBILITY NETWORKS

In spite of the pseudonym based security mechanism used for identity privacy (discussed in Section III), there are situations when the identity privacy of a subscriber becomes vulnerable. Such situations are as follows:

- ***U*is switched on for the first time and has not yet received a pseudonym:** In such a situation, it is forced to present its identity by transmitting its IMSI in clear-text through the radio link.

- ***V* cannot map a presented pseudonym to its corresponding IMSI:** In such a situation (that may arise due to reasons like database failure, etc.), ***V*** has a provision to request ***U*** for its IMSI. Such a request requires ***U*** to transmit its IMSI in clear-text through the radio link.

- A new ***V*** cannot contact the old ***V*** for the pseudonym-to-IMSI mapping of a roaming subscriber: When a subscriber moves into the region of a new ***V*** (say *Vn*), ***U*** will present its identity to *Vn* through the pseudonym allocated to it by the previous ***V*** (say *Vo*). In order to request for a new set of AV from ***H***, *Vn* will need to have knowledge of the IMSI. Normally, this will be obtained by presenting the pseudonym to *Vo*. However, in case *Vo* cannot be contacted, *Vn* will be forced to ask ***U*** for its IMSI. The later will then have to be transmitted in clear-text over the radio link by ***U***. This vulnerability can in fact be exploited by an attacker who can masquerade as a new ***V***.

V. RELATED WORK

In the early days of mobile communications, when researchers started recognizing identity privacy as an important security issue, several schemes and protocols were proposed to improve identity privacy of the subscriber over the radio access link between U and V. Some of these schemes and protocols are the ones proposed by Asokan [10], Lin et al. [11], Horn et al. [12], Park et al. [13], Barbeau et al. [7], Juang et al. [14], Forsberg et al. [15], etc. A basic assumption in these proposals is that V is trustworthy.

In present day context, where V can practically be forged or compromised, such trust is difficult. Realizing this, researchers are now concentrating on providing identity privacy to the subscriber over the entire path between U and H. In these solutions, the need to protect the identity privacy of a subscriber from even V is well recognized.

Several schemes and protocols that envisage protecting the identity privacy of the subscriber form Vin global mobility networks are proposed. In many of these proposals, asymmetric key cryptography is used, viz., the protocols proposed by Samfat et al. [16], Godor et al. [17][18], Yang et al. [19], Li et al. [20], He et al. [21], Feng et al. [22], etc. In many proposals, a hybrid approach is adopted, where a combination of both asymmetric key and symmetric key crypto systems are used. Some of these protocols are the ones proposed by, He et al. [23], Varadharajan et al. [24], Al-Fayoumi et al. [25], Zhu et al. [26], Koien et al. [27], etc. Recently, many schemes were proposed, where computationally light techniques that use symmetric key based crypto systems, hash functions, XOR operations, temporary identities, alias, etc., are used. Some of these protocols are the ones proposed by Sattarzadeh et al. [28], Tang et al. [29], Pereniguez et al. [30], He et al. [31], Zhou et al. [32], He et al. [33], Chen et al. [34], Liu et al. [35], Jiang et al. [36], etc.

VI. ROAMING AGREEMENTS SIMPLIFIED

Recent research conducted to enhance identity privacy in global mobility networks, as discussed in Section V, envisage protecting the subscribers' identity from visited networks (V) which may even be forged or compromised. In this, the author of this paper perceives a supplementary benefit, which is that of simplification in the roaming agreement procedure between mobile operators.

Roaming agreements/pacts with third party operators to provide service in a location where an operator has not set up its own infrastructure is a common practice. Such agreements allow a subscriber of one operator to use the access service of another operator when inside the latter's coverage area.

The current status of identity privacy in global mobility networks requires establishing the following trust relationships with respect to its subscribers' identity, i.e., the IMSI (Fig. 3).

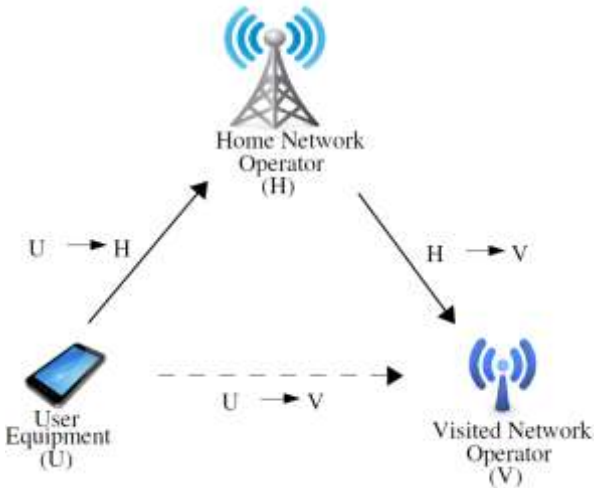

Figure 3. Current trust model.

1. U → H: As the U is registered with H, it trusts H with its IMSI.
2. H → V: H confers full trust in V with regards to the IMSI of the subscriber.
3. U → V: This trust relation is a transitive outcome of the previous two trust relations, because of which, the U also has to trust V with its IMSI.

Here, the first trust relationship requirement is unavoidable. However, the other two trust relationships requirements are due to the operator's obligation towards the subscribers to ensure adequate identity privacy while they are roaming within the coverage area of another operator. To establish such trust relationships, it becomes necessary for the home network operator to have elaborate negotiations or agreements with the visited network operator. Such negotiations, limits the ease and span of extending services beyond an operator's own circle/zone. A visited network operator, with which there is no prior roaming agreement, cannot be trusted by the home network operator when it comes to its subscribers' identity privacy.

With the increase in demand for any-time any-where service, there is need for a paradigm shift, such that the requirement of

trust on the visited network operator is relaxed. Recent research in the field of identity privacy that envisages protecting the subscribers' identity even from V fulfils this requirement. With this new approach, the need to trust V with the identity of the subscriber is eliminated. Thus, the only trust relationship that an operator is expected to take care of with respect to the subscriber's identity is the following (Fig. 4).

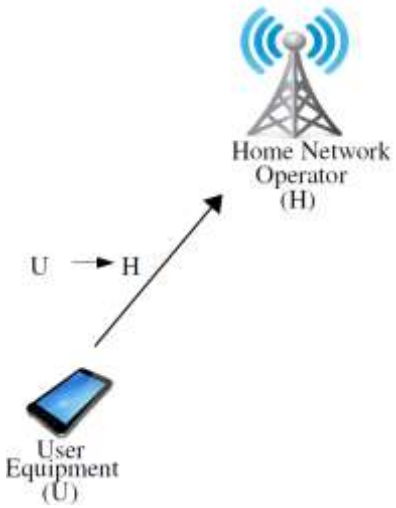

Figure 4. Simplified trust model.

1. U → H: As the U is registered with H, it trusts H with its IMSI.

Therefore, this new approach to enhance identity privacy of the subscriber in global mobility networks would be a step towards enabling the home network operator to have simplified negotiations/agreements with the other network operators.

VII. CONCLUSION

In today's context, when mobile operators strive to provide wider coverage, roaming agreements/pacts with third party operators to provide service in a location where an operator has not set up its own infrastructure is a common practice. Roaming allows a subscriber of one operator to use the access service of another operator when inside the latter's coverage area. Recent research to enhance identity privacy in global mobility networks envisages protecting the identity of the subscriber even from the visited network operator. If this becomes a reality in practice, it would remove the need for the home network operator to trust the visited network operator with the subscriber's identity. This relaxation is perceived to simplify roaming agreements. In this paper, an effort was made to elaborate on this possibility.

REFERENCES

[1] Whalen, T. Mobile devices and location privacy: Where do we go from here? IEEE Security & Privacy 9(6), 61-62, 2011.

[2] TWB. Mobile phone access reaches three quarters of planet's population, The World Bank Press Release. http://www.worldbank.org/en/news/2012/07/17/mobile-phone-access-reaches-three-quarters-planets-population, 2012.

[3] 3GPP. Numbering, addressing and identification, Technical Specification. http://www.3gpp.org/ftp/Specs/html-info/23003.htm, 2012.

[4] Liu, Z. Y. et al. A fast suffix matching method in network processor, in IEEE International Conference on Computational Intelligence and Security (CIS' 08), Suzhou, China, 405-410.

[5] Barbeau, M. & Robert, J. M. Perfect identity concealment in UMTS over radio access links, in IEEE International Conference on Wireless And Mobile Computing, Networking And Communications (WiMob 2005), Montreal, Canada, 72-77.

[6] Boman, K. et al. UMTS security, Electronics & Communication Engineering Journal 14(5), 191-204, 2002.

[7] Niemi, V., Nyberg, K. & Wiley, J. UMTS Security, Wiley, United States, 2003.

[8] Koien, G. M. An introduction to access security in UMTS, IEEE Wireless Communications 11(1), 8-18, 2004.

[9] Xenakis, C. & Merakos, L. Security in third generation mobile networks, Computer communications 27(7), 638-650, 2004.

[10 Asokan, N. Anonymity in a mobile computing environment, in IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1994), Santa Cruz, CA, 200-204.

[11] Lin, H. Y. & Harn, L. Authentication protocols for personal communication systems, ACM SIGCOMM Computer Communication Review 25(4), 256-261, 1995.

[12] Horn, G. & Preneel, B. Authentication and payment in future mobile systems, in European Symposium on Research in Computer Security (ESORICS' 98), Louvain-la-Neuve, Belgium, 277-293.

[13] Park, J. et al. Wireless authentication protocol preserving user anonymity, in Symposium on Cryptography and Information Security (SCIS 2001), Oiso, Japan, 159-164.

[14] Juang, W. S. &Wu, J. L. Efficient 3GPP authentication and key agreement with robust user privacy protection, in IEEE Wireless Communications and Networking Conference (WCNC 2007), Kowloon, Hong Kong, 2720-2725.

[15] Forsberg, D. et al. Enhancing security and privacy in 3GPP E-UTRAN radio interface, in IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2007), Athens, Greece, 1-5.

[16] Samfat, D. et al. Anonymity and untraceability in mobile networks, in ACM International Conference on Mobile Computing and Networking (MobiCom' 95), Berkeley, California, USA, 26-36.

[17] Godor, G. et al. Novel authentication algorithm of future networks, in IEEE International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies (ICNICONSMCL' 06), Mauritius, 80-80.

[18] Godor, G. & Imre, S. Novel authentication algorithm - public key based cryptography in mobile phone systems, International Journal of Computer Science and Network Security 6(2B), 126-134, 2006.

[19] Yang, G. et al. Anonymous and authenticated key exchange for roaming networks, IEEE Transactions on Wireless Communications 6(9), 3461-3472, 2007.

[20] Li, X. & Wang, Y. Security enhanced authentication and key agreement protocol for LTE/SAE network, in IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM'11), Wuhan, China, 1-4.

[21] He, D. et al. Privacy-preserving universal authentication protocol for wireless communications, IEEE Transactions on Wireless Communications 10(2), 431-436, 2011.

[22] Feng, T. et al. Anonymous identity authentication scheme in wireless roaming communication, in IEEE International Conference on Computing Technology and Information Management (ICCM 2012), Berlin, Germany, 124-129.

[23] He, Q. et al. The quest for personal control over mobile location privacy, IEEE Communications Magazine 42(5), 130-136, 2004.

[24] Varadharajan, V. & Mu, Y. Preserving privacy in mobile communications: A hybrid method, in IEEE International Conference on Personal Wireless Communications (ICPWC 1997), Mumbai, India, 532-536.

[25] Al-Fayoumi, M. et al. A new hybrid approach of symmetric/asymmetric authentication protocol for future mobile networks, in IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMOB 2007), New York, USA, 29-29.

[26] Zhu, J. & Ma, J. A new authentication scheme with anonymity for wireless environments, IEEE Transactions on Consumer Electronics 50(1), 231-235, 2004.

[27] Koien, G. & Oleshchuk, V. Location privacy for cellular systems; Analysis and solution, in International Workshop on Privacy Enhancing Technologies (PET 2005), Cavtat, Croatia, 40-58.

[28] Sattarzadeh, B. et al. Improved user identity confidentiality for UMTS mobile networks, in IEEE European Conference on Universal Multiservice Networks (ECUMN '07), Toulouse, France, 401-409.

[29] Tang, C. & Wu, D. O. Mobile privacy in wireless networks-revisited, IEEE Transactions on Wireless Communications 7(3), 1035-1042, 2008.

[30] Pereniguez, F. et al. Privacy-enhanced fast re-authentication for EAP-based next generation network, Computer Communications 33(14), 1682-1694, 2010.

[31] He, D. et al. A strong user authentication scheme with smart cards for wireless communications, Computer Communications 34(3), 367-374, 2011.

[32] Zhou, T. & Xu, J. Provable secure authentication protocol with anonymity for roaming service in global mobility networks, Computer Networks 55(1), 205-213, 2011.

[33] He, D. et al. Design and validation of an efficient authentication scheme with anonymity for roaming service in global mobility networks, Wireless Personal Communications 61(2), 465-476, 2011.

[34] Chen, C. et al. Lightweight and provably secure user authentication with anonymity for the global mobility network, International Journal of Communication Systems 24(3), 347-362, 2011.

[35] Liu, H. & Liang, M. Privacy preserving registration protocol for mobile network, International Journal of Communication Systems. http://onlinelibrary.wiley.com/doi/10.1002/dac.2426/full, 2012.

[36] Jiang, Q. et al. An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks, Wireless Personal Communications 68(4), 1-15, 20

AUTHOR'S BIOGRAPHY

Hiten Choudhury is an Assistant Professor in the Dept. of Computer Science and Information Technology at Cotton University, Guwahati, India. He has a Ph.D in Computer Science and Engineering from Tezpur University (India). His areas of current research interest include wireless network security, authentication protocols, security in IoT and security in vehicular networks.