IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.-7, Issue-3, March 2019 E-ISSN: 2347-2693

Roaming Agreements vis-a'-vis Identity Privacy

Hiten Choudhury

Dept .of Computer Science and Information Technology, Cotton University, Guwahati, Assam, India

Corresponding author: hiten.choudhury@cottonuniversity.ac.in

DOI: https://doi.org/10.26438/ijcse/v7i3.632635 | Available online at: www.ijcseonline.org

Accepted: 06/Mar/2019, Published: 31/Mar/2019

Abstract— Recent advancements in cellular networks have led to the demand of 'any-where' service - immaterial of the location of the user or the coverage area of the service provider. The increasing demand for providing subscribers with services beyond ones home service area necessitates the service providers to set up elaborate trust relationships and agreements amongst themselves, to ensure secured and reliable service to the genuine subscribers. This process however limits the ease and span of extending the services by a service provider. In addition, it is important that such services are provided without compromising the identity privacy of the subscriber. While identity privacy is an accepted requirement, vulnerability of the same remained across the generations. Newer threat like location tracking and comprehensive profiling - wherein data about movement, usage, etc., of a subscriber is amassed and linked to his/her identity to explore various attacks - has been identified. Much of the aforesaid limitations can be attributed to the trust model adopted by the cellular networks. In this article, we highlight the benefits of a trust model that may contribute towards reducing the complexities of a-priori agreements amongst service providers, for providing service beyond their territories in future mobile networks.

Keywords—Roaming agreements, Authentication, Anonymity, IMSI, Privacy

I. INTRODUCTION

The basic architectural framework for security is common across the cellular technologies - be it Global System for Mobile Communication (GSM): a popular 2G standard, or be it Long Term Evolution (LTE): a popular 4G standard. In this framework, three parties are involved, viz., the Mobile Station (MS), the Home Network (HN) and the Serving Network (SN). The MS that a subscriber owns is registered with a HN. The association between the MS and the HN is created from the moment the subscriber procures a Subscriber Identity Module (SIM) from the HN and fits it into his/her MS. The HN offers services to its registered MSs through SNs that are located within or outside its own service area. Communication between a MS and a SN happens through radio link, whereas communication between a SN and a HN happens through the wired medium. The radio link is considered vulnerable to various kinds of attacks by adversaries as it is too open by nature for comfort, whereas the wired link is considered to be secured [1]. The secure nature of the wired link is a result of trust relationship that exists between the SN and the HN. A HN assigns a unique permanent identity called the International Mobile Subscriber Identity (IMSI) to every MS for unique identification of the subscriber. The HN uses this identity for authentication, authorization and billing purposes. To ensure identity privacy to the subscribers, the IMSI should not be accessible to anybody except the MS and the HN.

With the increasing availability of sensitive services like mobile banking, mobile commerce, etc., over a plethora of mobile access devices operating over cellular networks, the importance of identity privacy has increased many folds. Identification of newer threats like location tracking and comprehensive profiling - wherein data about movement, usage, etc., of a subscriber is amassed and linked to his/her identity to explore various attacks - has made the situation more critical [2].

In the current security architecture, effort is made to protect the identity privacy of a subscriber by limiting the transmission of IMSI over the radio link through the use of temporary identities [3] [4]. After every successful mutual authentication between the MS and the SN, a temporary identity is allocated to the MS by the SN through a secured channel. The association between a temporary identity and the corresponding IMSI is maintained at the SN's local database. To have access to a particular service, an MS has to send a service request along with its temporary identity to the SN. The SN, in turn presents the corresponding IMSI to the HN - in order to obtain relevant authentication data for the MS. It then uses this authentication data in a challenge response mechanism to authenticate the requesting MS [5]. However, in spite of the efforts made, there are occasions where the

IMSI has to be transmitted over the insecure radio path in clear text for everyone to see [6] [7]. Unfortunately, such occasions may even be created by an adversary [8].

To ensure safety of the IMSI while it is stored at the SN's local database, adequate trust relationship needs to be established between the SN and the HN through negotiations and agreements. While this might not be an issue for SNs owned by the same service provider as the HN, elaborate agreements will be necessary if that is not the case. With the demand for 'anywhere' service, it is not possible to always ensure that the SNs providing the support belong to the same home service provider. Thus, a service provider will require roaming agreements with third party service providers to ensure the necessary level of trust amongst them. This being an a-priori requirement, will limit the extent of serviceable geography; especially with existing operators quitting the business and/or new operators coming up at different locations across the globe. In this article, we propose a trust model that has the potential to relax the trust relationship requirement amongst service providers, wherein the overhead of having a-priori agreements can be replaced by flexible on-the-fly and on-demand agreements. In addition, it has the potential to significantly enhance identity privacy of the subscribers.

The rest of the article is organized as follows: in section 2, we discuss the current trust model; in section 3, we present the proposed model; finally, we conclude in section 4.

II. CURRENT TRUST MODEL

In the current trust model, the following trust requirements with reference to the permanent identity of a subscriber exist:

1. **MS → HN:** As the MS is registered to, and has a direct service agreement with the HN; it trusts the HN with its IMSI.

2. **HN → SN:** Since the HN serves its subscribers through SNs; the HN should confer full trust in the SN with regards to the IMSI of a subscriber. This might require elaborate service agreements amongst them. For authentication, authorisation and billing purposes, the IMSI is exchanged unabated between the HN and the SN.

3. **MS → SN:** This trust relation is a transitive outcome of the previous two trust relations, because of which, the MS has to fully trust the SN with its IMSI and it transmits the IMSI immediately upon request from the SN.

The following vulnerabilities/limitations exist in the above model:

a. To fulfill the second trust requirement in the model (i.e., HN → SN), a-priori agreements needs to be set up. Thus, this trust requirement may deprive a roaming subscriber form services in a location where there is no service provider having a prior agreement with the subscriber's HN.

b. According to the third trust requirement (i.e., MS → SN), the IMSI has to be transmitted in clear text through the radio link any time when the SN requests for it. The SN has provision to make such a request when it cannot map the received temporary identity of an MS with the corresponding IMSI. Such a recovery mechanism provides an opening for a fake SN to compromise a subscriber's IMSI.

c. During the very first connection, there is no temporary identity by which a MS can be identified. In such a situation, taking advantage of the third trust requirement in the model (i.e., MS → SN), the SN requests the MS for its IMSI; in response to which the MS has to transmit its IMSI in clear text.

Roaming agreements with third party operators to provide service in a location where an operator has not set up its own infrastructure is a common practice. The trust model adopted by the cellular networks expect unconditional trust requirement on part of the subscribers. In today's context when multiple operators compete among each other for cellular air space, such trust relationship requirement imposes restriction and brings in overheads towards providing 'anywhere' service to the subscriber. Thus, there is need for a paradigm shift such that the requirement of trust on third party SNs is relaxed or even entirely eliminated.

III. PROPOSED TRUST MODEL

In this section, we propose a trust model that is based on the following observations:

a. To overcome the above vulnerabilities, the HN/MS should not have the need to trust the SN with the IMSI of the MS. provided the HN/MS have an alternate mechanism to uniquely identify the MS to the SN, and to allow the SN to acquire authentication data from the HN.

b. Due to low power and low computational capability of a MS, public key based solutions are not feasible for cellular networks [9].

c. With an alternate mechanism of identity presentation sans IMSI, the HN → SN trust relationship can be considerably relaxed.

The new trust model is more flexible compared to the state of the art model. In this, there is only one trust requirement, which is as follows:

1. **MS → HN:** The MS should trust only the HN with which it is registered and no one else. The IMSI should not be shared with any third party and under no circumstance should leave the MS or the HN.

For successful working of this model, a second set of temporary identities (say TI_{HN}), over and above those used between the MS and the SN (say TI_{SN}), are to be used between the MS and the HN, and these are to be generated and distributed by the HN. These temporary identities can be presented by MS to SN for initiating the connection process. Temporary identity (i.e., TI_{HN}) distribution mechanism should ideally be integrated with the authentication and key agreement procedure, to avoid extra communication latency.

Towards this, the HN may include TI_{HN} in that part of the authentication data which reaches the MS as a challenge via the SN. A TI_{HN} should be such that when presented by an MS, it should reveal the owner home network identity to the SN, so that the latter can approach the corresponding HN for authentication data. A mapping between TI_{HN} and the IMSI should be maintained at the HN. Such a mapping would help the HN to easily identify the corresponding IMSI when a TI_{HN} is presented to it. For convenience of identity presentation during the very first connection, the HN should insert a TI_{HN} (that is meant for one time usage) into the SIM's memory. During successive connections, the TI_{HN} that is received by the MS from the HN (during the previous successful authentication) is to be used. An implementation of this model that uses short lived temporary identities instead of the IMSI for setting up of MS-SN connection, is already proposed by the authors in [10] [11].

With this trust model, there will no longer be a requirement for prior trust agreement between the HN and the SN. Any SN available in the serving area will be able to serve the MS. This might also allow for auctioning of service (including QoS) by various SNs serving a given area based on their current load. The involvement of the HN in generation of temporary identities will ensure a process for billing of the services provided by the SN. Subscribers who wish to protect their data from being interpreted by the intermediate network elements may use end to end application layer based ciphering and integrity protection solutions [12] [13]. Moreover, cellular networks are gradually moving towards all-IP packet switched mode, where IPsec can be used to protect the IP packets [14] [15].

IV. CONCLUSION

In conclusion, if we relax the requirement of having to trust the SNs, it then opens up an opportunity to have on-demand/on-the-fly service agreements between the SN and the HN, instead of the current a-priori agreements. This would ensure that a subscriber will be serviceable in any location as long as there is at least one network serving that location. Moreover, this relaxation provides an additional benefit of enhanced identity privacy. With more and more service providers taking a plunge into the competitive cellular market, interoperability amongst them is a key issue. Thus, the benefits of a relaxed HN → SN trust requirement would be difficult to ignore in the foreseeable future.

REFERENCES

[1] 1. Xenakis C, Merakos L: Security in third generation mobile networks. Computer communications 2004, 27(7):638–650.

[2] 2. Whalen T: Mobile Devices and Location Privacy: Where Do We Go from Here? Security & Privacy, IEEE 2011, 9(6):61–62.

[3] 3. 3GPP: 3G Security;Security architecture. TS 33.102, 3rd Generation Partnership Project (3GPP) 2011, [http://www.3gpp.org/ftp/Specs/html-info/33102.htm].

[4] 4. 3GPP: 3GPP System Architecture Evolution (SAE); Security architecture. TS 33.401, 3rd Generation Partnership Project (3GPP) 2011, [http://www.3gpp.org/ftp/Specs/html-info/33401.htm].

[5] 5. Zhang M, Fang Y: Security analysis and enhancements of 3GPP authentication and key agreement protocol. Wireless Communications, IEEE Transactions on 2005, 4(2):734–742.

[6] 6. Koien G: An introduction to access security in UMTS. Wireless Communications, IEEE 2004, 11:8–18.

[7] 7. Sankaran C: Network access security in next-generation 3GPP systems: A tutorial. Communications Magazine, IEEE 2009, 47(2):84–91.

[8] 8. Meyer U, Wetzel S: A man-in-the-middle attack on UMTS. In Proceedings of the 3rd ACM workshop on Wireless security, ACM 2004:90–97.

[9] 9. Zhang Y, Zheng J, Ma M: Handbook of research on wireless security. Information Science Reference-Imprint of: IGI Publishing 2008.

[10] 10. Choudhury H, Roychoudhury B, Saikia D: End-to-End User Identity Confidentiality for UMTS Net-works. In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on, Volume 2, IEEE 2010:46–50.

[11] 11. Choudhury H, Roychoudhury B, Saikia D: UMTS user identity confidentiality: An end-to-end solution. In Wireless and Optical Communications Networks (WOCN), 2011 Eighth International Conference on, IEEE 2011:1–6.

[12] 12. Diab W, Tohme S: VPN solution for securing voice over third generation networks. In Internet Mul-timedia Services

Architecture and Applications, 2008. IMSAA 2008. 2nd International Conference on, IEEE 2008:1–6.

[13] 13. Xenakis C, Ntantogian C, Stavrakakis I: A network-assisted mobile VPN for securing users data in UMTS. Computer Communications 2008, 31(14):3315–3327.

[14] 14. Arkko J, Devarapalli V, Dupont F: Using IPsec to protect mobile IPv6 signaling between mobile nodes and home agents 2004, [http://trac.tools.ietf.org/html/rfc3776].

[15] 15. Xenakis C, Merakos L: IPsec-based end-to-end VPN deployment over UMTS. Computer Communications 2004, 27(17):1693–1708.

Authors Profile

Dr. Hiten Choudhury pursued Bachelor of Science in Physics from Cotton College, India in 1998 and Masters Degree in Computer Applications from Jorhat Engineering College, India in the year 2001. He received his Ph.D. in Computer Science and Enginering from Tezpur University, India in 2014. Currently he is working as Assistant Professor in Department of Computer Science and Information Technology, Cotton University, Asssam, India.

