Privacy in LTE networks

Siddharth Prakash Rao
Aalto University
Espoo, Finland
siddharth.rao@aalto.fi

Bhanu Teja Kotte
Bell Labs Nokia
Espoo, Finland
bhanu.kotte@nokia.com

Silke Holtmanns
Bell Labs Nokia
Espoo, Finland
silke.holtmanns@nokia.com

ABSTRACT

Ever since the public revelation of global surveillance and the exploits targeting the mobile communication backend, the general awareness of user privacy in telecommunication industry has increased. Misusing the technical features of mobile core network technology - specifically the Signalling System 7 (SS7) has disclosed numerous ways to locate the mobile users and intercept the voice calls or text messages. These events had led the mobile network operator to focus more on protecting the privacy of user meta-data and signaling communication.

With relatively more security and privacy features, Diameter protocol - the successor of SS7 in Long Term Evolution (LTE) networks are believed to guarantee more protection to end-users. In this paper, we argue that the default considerations of Diameter are not sufficient enough to offer privacy to the mobile user, particularly when it comes to location tracking. We will discuss the possibilities of the persistence of location tracking attacks from SS7 to Diameter. We also recommend the mobile network operators to review their security mechanisms based on the countermeasures that we present. In short, this paper provides a comprehensive overview of Diameter protocol to claim – *Without the appropriate measures, the Diameter-based LTE networks are as vulnerable as SS7-based GSM networks at least in terms of location tracking.*

CCS Concepts

•**Networks** → **Mobile networks;** *Mobile and wireless security;* •**Security and privacy** → *Security protocols; Mobile and wireless security;*

Keywords

Diameter, Interconnection, Location tracking, Security, Privacy, SS7

1. INTRODUCTION

With recent advancements in cellular technologies, the mobile phones have become more prevalent than ever before. Mobile phones have become a tool for surfing the Internet, sending text messages and apps to aid every part of day-to-day life, beyond its primary communication service of phone calls. The mobile phones were not intended to provide any kind of privacy and security to the end-users when it was designed. Considering the emerging threats, the telecommunication standardization organizations (such as GSMA, ETSI, and 3GPP) have included security features iteratively in every generation of mobile technologies. In spite of all those measures, mobile phones offer less control over privacy in comparison with personal computers, especially in terms of revealing its physical location.

Unlike the Internet-based communication where staying invisible without revealing the actual physical location of the end-users is possible, in the mobile networks such concept is far from reality as of now [17]. This shortcoming is partly due to the design of mobile communication technologies which mandates the announcement of whereabouts[1] of the mobile device to perceive continuous cellular services. The basic working mechanism allows the mobile operators know the physical location of the users at any point of time when the phone is switched on.

Undoubtedly the location data of the mobile phone users are considered to be personal information. However, the advancements in recent positioning technologies have built a strong market for location-based services. In these cases, the location data is used with the consent of the users to provide valuable services. Contrary to the emerging market of location-based services, illegitimate access to the location information has been one of the prime targets of mass surveillance [21]. In particular, the possibility of exploiting the mobile communication backend *i.e.* the signaling systems such as Signalling System 7 (SS7) to collect/track the location data on a large scale has raised serious privacy concerns.

Illegitimate location tracking in SS7-based Global System for Mobile communication (GSM) networks have been in debate over the past two years and telecommunication security is building solutions to defend the network against them. However, Diameter – the successor of SS7 is believed to offer more security to the LTE networks and privacy to the end-users. Even though Diameter offers a relatively large number of security features, location tracking is still a persistent

[1]Mobile phones periodically broadcast radio signals to attach themselves to the mobile operator's network.

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China

DOI 10.4108/eai.18-6-2016.2264393

threat. In this paper, we review the security and privacy consideration of Diameter protocol and claim that the default measures in Diameter make the network as vulnerable as SS7 in terms of offering protection against illegitimate location tracking.

Key contributions: This paper gives an overview of state-of-the-art Diameter security usage and its problems in modern LTE network. It draws upon a wide range of existing literature and our ongoing work [28] related to Diameter security. The primary contribution of this paper is the detailed review of Diameter protocol to point out the practical and deployment related deficiencies in its current security considerations. Secondly, we will discuss the possible persistence of location tracking attacks from SS7 protocol to Diameter. Thirdly, we propose two different categories of potential countermeasures to defend the location privacy of mobile users without being forced to deploy a full-scale public key infrastructure on the interconnection network.

Organization of the paper: In section 2, we will describe the background architecture of LTE networks by describing the underlying components and interfaces. In section 4, we will review the Diameter protocol in order to discuss the security considerations (4.1) and shortcomings (6.1). A high-level description of the SS7 protocol and the related location privacy breaching attacks can be found in section 3. In section 5, we will summarize the location disclosure attacks based on the latest development in LTE security as part of our ongoing work. We propose some of the potential countermeasures to strengthen the LTE network in section 6. Finally, we end our discussion with the concluding remarks in section 7.

2. BACKGROUND

With the evolution of the 2G (GSM) and 3G (UMTS) cellular networks towards 4G (LTE) networks, the Signalling System No. 7 (SS7) based core network communication is gradually replaced by Diameter based IP network. The core of an LTE network is known as Evolved Packet Core (EPC) whose simplified representation is shown in figure 1. The Home Location Register (HLR) and Mobile Switching Center (MSC) known from the GSM network evolved to be the Home Subscriber Server (HSS) and Mobility Management Entity (MME) respectively in the Diameter-based LTE networks.

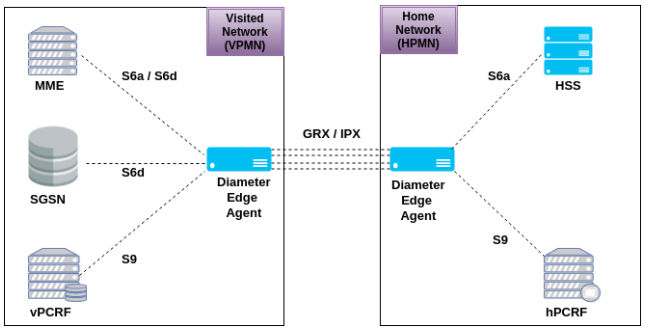

Figure 1: LTE roaming architecture.

1. Mobility Management Entity (MME) controls mobility management in the signaling network beyond radio communication. As with the serving gateway, a typical network might contain a handful of MMEs, each of which serves a certain geographical region. The MME also communicate with other nodes of the network (*e.g* HSS) by means of signaling messages that are internal to the EPC.

2. Home Subscriber Server (HSS) is a central database which contains information about all the subscribers of a network operator. It holds subscription related data such as subscriber profile, data access restrictions and roaming. The HSS may also integrate the Authentication Center (AuC), which generates the encryption tuples that are used for encrypting the over-the-air communication.

3. The home Policy Charging and Rule Function (hPCRF) enables billing and thereby collects the charging records for a user. When the subscriber is in a visited network, the same functionality is handled by the visited Policy Charging and Rule Function (vPCRF).

4. Diameter supports scalability, resilience and maintainability by using different types of Diameter Agents (DA) such as Diameter Routing Agents (DRA) and Diameter Edge Agents (DEA). DRA [4] is a centralized configuration repository which provides real-time routing capabilities to ensure that the message packets are routed among the correct nodes within an LTE network. On the other hand, DEA serves as a centralized entry point to an operator's network from the global interconnection. To protect an operator network from attacks coming via the interconnection interface, the DEA is ideally the first line of defense.

5. Diameter has a base protocol defined by the Internet Engineering Task Force (IETF), based upon which the application specific interfaces for establishing Diameter connection between different nodes are defined. The 3rd Generation Partnership Project (3GPP) standardized many of those interfaces[2] such as Cx, Dh, Dx, Rf, Ro, S6a, S6d, S9 and Sh. Some of the key interfaces (as shown in figure 1) are as follows: S6a/S6d interface connects HSS and MME as per TS 29.272 [12]; Sh interface is between an IMS application server and the HSS [6]; S9 provides standard communication interface between the hPCRF and vPCRF [3]; S6c interface [2] connects the HSS and the central SMS Centre.

The core networks of operators are connected by IP Packet eXchange(IPX) or GPRS[3] Roaming eXchange (GRX) interconnection. These interconnections offer backbone infrastructure to various service providers[4] and communication providers enabling them to provide services all over the world. The interconnection is the technical foundation to enable roaming worldwide. This interconnection network was built at a time when there were few trustworthy state-owned operators. They used the SS7 protocol to communicate with each other, due to the closed nature of the network at that time, no security was built. However, the closed nature of the core network has been opened up in recent years due to

[2]3GPP uses alphanumerics (*e.g.* S6a) to designate standard interfaces between the nodes.
[3]GPRS stands for the *General Packet Radio Service*
[4]All service providers including the mobile network operators can be connected to IPX/GPX via roaming hubs.

changes in legislations and this has resulted in exploitation of the vulnerabilities of signaling systems. Several attacks were published on the SS7 network and also for the Diameter network [30]. The amount of service providers having access to the interconnection network has increased substantially (*e.g.* SIP/VoIP based services), and not all of those service providers can be considered as trustworthy. Even though many network operators monitor the traffic coming from the interconnection network and apply suitable filters, the number of network providers who are aware of the risks are relatively high. GSMA is actively working on studying and countering potential Diameter based attacks, as Diameter replicates many functional elements from the SS7 protocol.

A detailed guideline about the security requirements and filtering approaches for the service providers to use the global interconnection can be found in IR.77 [23]. Furthermore, the service operators can also use the guidelines issued by GSMA (GSM Association) (*e.g.* IR.88 [26], IR.34 [22] and [24]) for installing filters and firewalls to strengthen their network which is exposed to the global interconnection network. We will describe general and mobile network specific security considerations of Diameter protocol in section 4.

3. RELATED WORK

The first location tracking attack was presented by Engel at the 25th Chaos Computer Club Conference in 2008 [18]. Even though the granularity of the location tracked using this attack is quite coarse, it successfully disclosed the vulnerabilities of SS7 interconnection network. The attack misuses the legitimate procedures in the short message service (SMS). More specifically, it uses the Message Application Protocol (MAP) [13] *Send Routing Information for SM* message to pose as an SMS Center (SMSC). By sending the victim's mobile phone number (MSISDN), it obtains the International Mobile Subscriber Identity (IMSI) and the identity of the Mobile Switching Center (MSC) that is currently serving the mobile. The MSC identity gives a rough location of the user upto the granularity of state or county of a country.

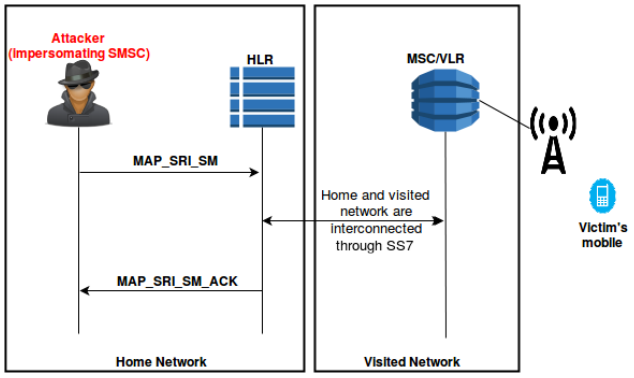

Figure 2: MSC level tracking using SRI SM

In May and August 2014 Positive Technologies published some of the cell level trackings [32] along with several other attacks. Later in December 2015, Engel [19] presented more concrete cell level tracking attacks. The attack in context uses the operator network internal *Any Time Interrogation* (ATI) message which returns the Cell ID, which gives a quite accurate user position in densely populated areas. Since ATI is normally a network internal command, many security aware operators now filter this message at the edge of their network. There are variations of a cell level location tracking attack such as a hybrid attack using SMS and CAMEL protocol [32] or Location Based Service (LBS) messages [19].

Further details and evolution of the attacks discussed in this section can be found in our survey paper [33].

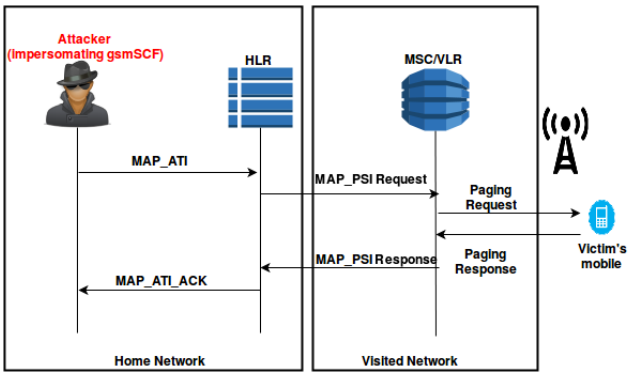

Figure 3: Cell level Tracking using *MAP ATI*

Some operators confirmed that their networks receive unauthorized location tracking messages (which we described in this section) over the roaming network interfaces. Ideally in such cases, they have to either filter those messages or return bogus locations if blocking is not possible. However, such straightforward mechanisms may not be implemented due to stringent roaming agreements with the partners and some of the messages are expected from the partner networks over the interconnection. Context-based filtering mechanisms to differentiate the attacks from legitimate scenarios are still not often used in the telecommunication industry.

4. REVIEW OF DIAMETER PROTOCOL

The communication between the nodes of an LTE network is facilitated by Diameter protocol suite which as an evolution of the MAP protocol of SS7 application stack. The Diameter protocol was originally designed to provide a framework for Authentication, Authorization and Accounting (AAA) to overcome the limitations [29] of its predecessor - RADIUS [34]. However, 3GPP has standardized the use of Diameter in cellular core network communication to support mobility, IP Multimedia Subsystem (IMS) and to extend the functionalities of SS7 over an all-IP network. Since any node that supports Diameter can initiate a request (behaving as a client) or receive requests from other nodes (behaving as a server), Diameter is considered to be a peer-to-peer (P2P) communication protocol. The P2P communication nature of Diameter replaces the hierarchy of the nodes within the network, which makes Diameter a suitable protocol for a broad range of emerging technologies such as Mobile IP and the Internet of Things (IoT).

4.1 Security considerations in Diameter

Due to increased requirement of security concerns in the communication protocols built on top of IP networks, Diameter has been designed to provide the several security features. In spite of the security features provided by Diameter, the actual security offered will completely rely on its

complete and correct implementation of Diameter. 3GPP standards assume that nodes on either side of the interconnection can be trusted as these nodes reside within the domain of trusted operator network. Ideally, the communication between the nodes beyond interconnection is secured individually as per Network Domain Security NDS/IP Security [1] using TLS or IPSec by the operators. In practice, this proves to be a business challenge as the operators often do not connect their nodes directly with their partners over interconnection, but they utilize the roaming hubs in order to provide their customers with a large base of roaming partners. The implementation of security features over the roaming hubs raises reliability concerns as the communication between Diameter nodes connected by the roaming hubs may not be using NDS/IP Security.

Below are some of the security features offered by Diameter protocol for LTE networks.

In-built Global Title Translation (GTT): Every node within the core of an operator's network is uniquely identified by their Global Titles (GTs). The operators tend to use and assign ranges of GTs to their nodes. Therefore, an attacker who has knowledge of one valid GT *e.g.* of SMSC, can start a brute force probing attack to learn the GTs of other core network nodes. This has been one of the main reasons for the attacks that abuse the SS7 interconnection as the GTs expose the critical nodes of the core network nodes to the partner or attackers from outside the home network.

In this realm, the Global Title Translation functionality provides protection to the core network nodes by reducing the need for explicitly disclosing the GTs of the nodes of the entire network in the routing tables of a communication message. GTT hides the topology of critical infrastructures such as HLR/HSS and EIR, by provisioning internal routing tables within the nodes rather than the communication message. The concept of GTT is implemented by default in Diameter suite, particularly in HSS. Along with mutual node authentication, GTT protects the core network against port scanning and impersonation attacks.

Dynamic peer discovery: Diameter is capable of dynamic peer discovery methods using which a Diameter client can discover the next hop node or all the nodes (peers) that appear during a specific communication. In a nutshell, any Diameter server/agent broadcasts the application and security level that they support, so that the neighboring nodes can dynamically discover the appropriate peers based on either SRVLOC (Service Location Protocol) [27] or DNS Service Protocol [14]. Every time a new peer is identified, relevant information about the peer location (addresses) and routing configurations along with the application and service that the peers support will be stored in peer tables and peer routing tables respectively. The dynamic peer discovery of Diameter protocol in terms of local storage of application-specific routing information adds another level of security as an attacker cannot learn the routing paths or addresses of critical nodes. Dynamic peer discovery makes the configuration of networks much easier since the sender does not need to be aware of the internal addresses.

Topology hiding: The aforementioned GTT and dynamic peer discovery help in *topology hiding* [12] in terms of hiding the address of the critical infrastructure (*e.g.* HSS, EIR) as well as the routing paths. When an interconnection message is sent outside the home network, the DEA replaces the internal (actual) address of the network node with a generic address which can only be resolved by itself. This helps to hide the global IP addresses from the view of an attacker or illegitimate partner who is trying to gain access to the core network via interconnection. Such topology hiding offered by Diameter prevents an attacker from penetrating deeper into the network using vulnerable ports, mapping the periphery of the network and executing a potential man-in-the-middle (MitM) attacks.

Cryptographic protection: Contrary to SS7 which offers no inbuilt security to the communication between the core network nodes, Diameter provides cryptographic protection in several ways [20]. The Diameter protocol provisions secure connection between the nodes of the core network using IP Security (IPSec) or Transport Layer Security (TLS) to authenticate and encrypt the internal traffic. It offers session-based (end-to-end) and connection-based (hop-to-hop) security measures. Furthermore, it uses TLS handshake protocol [16] which in turn utilizes the X.509 certificates [15] and asymmetric cryptography to authenticate between the nodes. Diameter also supports the use of Network Access Identifier (NAI), Challenge Handshake Authentication Protocol (CHAP), Extensible Authentication Protocol (EAP) and Password Authentication Protocol (PAP) to enhance the security of authentication procedures.

4.2 Shortcomings of Diameter security

With the strong support for AAA and other security considerations as we discussed in the previous section, Diameter appears to provide more security to the core network nodes and enhance the end-user privacy compared to SS7. Due to this, there is the perception that *"Diameter provides security by default"*. However, several business and interoperability factors influence the actual implementation and hence the level of security in the LTE networks. In addition to the generic security issues discussed in [35] (which is more related to air interface vulnerabilities), we will now discuss some of the shortcomings which enables an attacker to breach the location privacy of LTE end-users.

Gap between standardization and implementation: The 3GPP standard for Diameter base protocol [20] strongly recommends the use of IPSec for intra-operator communication and TLS[5] for inter-operator communication. Even though the IPSec/TLS has been standardized in Diameter based communication, using them is not obligatory. Furthermore, the nodes in a Diameter based network have no means to verify the usage of IPSec/TLS [31] while communicating with their peers because there is no standard procedure as of now. In practice, it can be seen that many operators do not secure their home LTE network to reduce the overhead of implementing the non-mandatory functionalities and this definitely shows their ignorance to recognize the threats from the interconnection. It should be noted that while we focus mostly on the attacks coming over the interconnection interface, the same attacks can also be launched from a compromised core network node directly. Sometimes the core network nodes (that run telnet or ftp protocol) are visible on the Internet, and the attackers can compromise them to further launch their attacks.

Reachability is decided by the applications: Diam-

[5]TLS is used when the underlying network uses TCP in the transport layer. However, Diameter also supports SCTP instead of TCP, and in this case, the transport layer security is facilitated by Datagram TLS (DTLS).

eter is an application based P2P protocol and hence, the communication messages (data packets) that a Diameter node sends is dependant on the application rather than the network configuration[6]. Since the application decides the penetration or reachability of the signaling messages, the attacker can impersonate at the application level and penetrate deeper into the core network. The application driven penetration capabilities make Diameter vulnerable to spoofing or impersonation attacks, particularly if an attacker succeeds to intercept the interconnection traffic. An attacker can easily misuse such automatic mechanism to exploit the vulnerabilities without detailed knowledge of the network topology.

Imposed overhead due to encryption: Diameter relies on the use of X.509 certificate and Public Key Infrastructure (PKI) for authentication. The common problems of PKI such as the distribution of public keys, the management of certificates and the verification of certificate revocation continue to create the security administration overhead in core networks. Additionally, the piggybacking of acknowledgement messages in the transport layer (via TCP or SCTP) induces more encrypted traffic in the upper layers, which requires bandwidth. As the interconnection network is a global network, the financial overhead of certificate distribution, maintainable of certificate revocation list, management of central PKI system becomes a serious problem. For the same reason, operators with less capital expenditure ignore to safeguard their nodes with PKI.

Problems due to strong fail-over algorithms: Diameter base protocol [20] has provisions for various failover [36] and error-handling algorithms to provide descriptive feedbacks in the case of system or network failures. These algorithms are initiated by the client when it has not received any answers for a certain amount of time [29]. An attacker can impersonate a Diameter client to flood the peers by sending bogus traffic of the fail-over algorithms. Even though the receiving peers can recognize the traffic as bogus or faulty (if the peer filters such), the fail-over algorithms attempt to process the traffic to provide useful feedback, which eventually results in a Denial of Service (DoS) attack. We can argue that the Diameter protocol is vulnerable to DoS attacks.

Support for legacy systems at the interconnection: The upgrade of the network from GSM (SS7) to LTE (Diameter) is a gradual process as most of the operators update their network infrastructure gradually to avoid service interruption. Due to this, the current interconnection network contains nodes that support either SS7/Diameter or both, making it an inhomogeneous set-up. For interoperability reasons with their partners, the edge nodes and the nodes themselves often have the ability to translate between Diameter and SS7 protocols, which is done using Interworking Functions (IWF) [10] [11].These inhomogeneous set-up enables an attacker poses as a roaming partner having an SS7 network and therefore, it forces the new LTE network to use less secure legacy communication messages. Additionally, the IWF provides an easy means of porting the SS7-based attacks to Diameter-based LTE networks. The attacks exploiting lack of security measures in the interconnection due to interoperability can be found in detail in our research article on IWF insecurity [28].

[6]This implies that the routing paths, intermediate nodes and the handling of the messages depend on the application.

5. LOCATION TRACKING ATTACKS IN LTE NETWORKS

For the practical realization of the attacks, we assume that an attacker has the acces to global interconnection network[7], and the targeted operator does not perform any IP address filtering or layer matching. It is important to note that even with appropriate filtering mechanisms (more details will be provided in 6) some of the attacks that we discuss in this section might still work.

5.1 IMSI retrieval (Preparation phase)

Short Message Service (SMS) is transmission of messages up to 140 bytes between mobile stations in a sore and forward mechanism. The Mobile Terminated Short Message Service (MT-SMS) protocol comprises of two parts: first where the SMS is submitted to Short Message Service Center (SMSC) by the sender; second is the delivery of that message to the recipient from SMSC. Basic message workflow in MT-SMS protocol as per [9] is as follows:

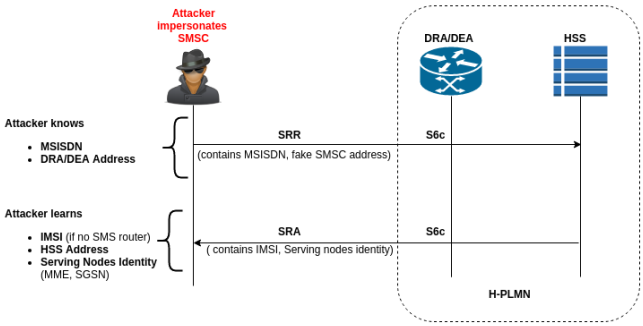

Figure 4: Obtaining IMSI using SRR

1. Message submission by the sender (Mobile Originating part)
   - The address of SMSC is usually stored in the SIM card. When the sender sends a Short Message (SM), the message along with SMSC address will be transmitted to the MME.
   - Based on the SMSC address specified, MME imparts Mobile Originated ForwardSM (MO ForwardSM) message to the SMSC.
   - If the SM is successfully delivered (stored in SMSC), it is acknowledged by SMS submit report message i.e. MO ForwardSM ACK.
2. Message delivery by SMSC to the destination (Mobile terminating part)
   - To deliver the short message to the destination, SMSC has to know the MME location and IMSI of the recipient which is stored in the HSS.
   - SMSC sends Diameter Send Routing Info For SM Request (SRR) [2] message to the HSS to query the serving MME identity and IMSI of the recipient.

[7]There are several ways to gain access to the interconnection network. However, the detailed description of those methods are beyond the scope of this paper.

- HSS encapsulates IMSI and serving MME Diameter identity in Diameter Send Routing Info For SM Answer (SRA) [2] message and sends it back to the sender's SMSC. Based on this information, sender's SMSC routes the short messge to the recipient MME which in turns delivers it to the receiving phone.

Attack: An attacker with an interconnection access can misuse the above protocol to identify the IMSI and identity of the subscriber's serving MME. The SRR Diameter message on the S6c [2] interface is used between the SMSC and the HSS to retrieve the routing information needed for routing the short message to the serving MME. The request must contain a mandatory SC-Address AVP whose value is the SMSC address. The request must also contain the MSISDN to identify the subscriber. A successful SRA message will contain the Serving-Node AVP which in turn contains the Diameter identity and the Diameter realm of the MME and SGSN (if present). The SRA will also contain the IMSI if no SMS router is deployed, if it is deployed, the attack potentially fails, depending on configuration aspects. The attack sequence is shown in the Figure 4.

5.2 Location Tracking using IDR

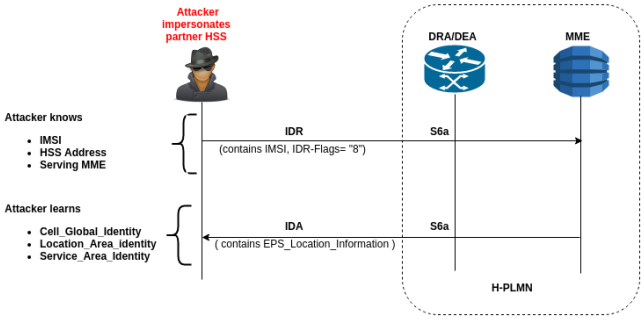

Figure 5: Location Tracking using IDR

An HSS can request the EPS Location information of a UE from the MME using the *Insert-Subscriber-Data-Request* (IDR). The *EPS location information* is the LTE network radio location where the user was last registered. The IDR request must contains two Diameter AVPs. The first is username whose value is the IMSI and the second AVP is *IDR-FLags*. The IDR-Flags is an unsigned 32-bit integer and contains a bit mask. Each bit corresponds to a different parameter [12]. The third bit corresponds to *EPS Location Information Request*, when set, indicates the MME that the HSS is requesting location information. The fourth bit corresponds to *Current Location Request*, when set, indicates the MME to provide the most current location information. The *Current Location Request* bit can be used only in conjunction with the *EPS Location Information Request* bit.

An MME receiving the IDR-Flags with *EPS Location Information Request* bit set, returns the *EPS Location Information* AVP. This AVP, in turn, contains three more AVPs: Cell-Global-Identity, Location-Area-Identity, Service-Area-Identity which identifies the location of a subscriber. If the Current Location Request bit is set and the UE is in idle mode, then the MME pages the UE in order to return the most up-to-date corresponding user location.

Attack: An attacker with access to the roaming interconnection network can impersonate the partner HSS and send the IDR to identify the location of a subscriber. The MME receiving the message assumes that the request is from the subscriber's home network HSS and sends the requested information back. The Figure 5 shows the attack sequence. It should be noted, that the IDR message is a quite powerful tool for an attacker, as it allows general modification of the subscriber profile in the MME and the subscriber information contains e.g. service restrictions, group memberships *etc.*

5.3 Location Tracking using UDR

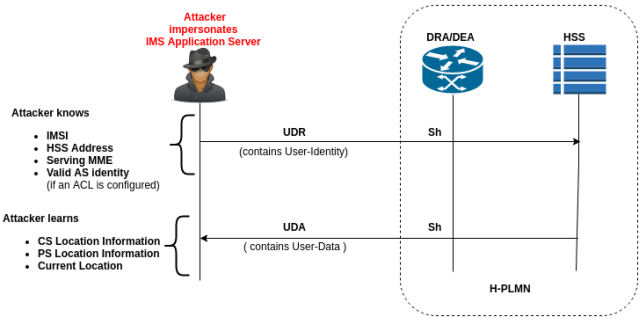

Figure 6: Location Tracking using UDR

The *User-Data-Request* (UDR) Diameter message is used on the Sh interface between an IP Multimedia Subsystem (IMS) application server and the HSS. Sh interface is defined in 3GPP TS 29.329 [6], and is one of the key interfaces for the operators to provide IMS services to their subscribers. The UDR message does not require an IMSI to be present according to standards, but some configurations may require the presence of the IMSI. The User-Data AVP in the answer contains the location information of a particular subscriber such as the Circuit-Switched (CS) Location Information, Packet-Switched (PS) Location Information, Current Location. The returned information depends on the HSS implementation and on the available data. In most cases, the CS location information will be available and contains the Location Area ID and Cell ID which identifies where the subscriber is currently located or where it was last located.

Attack: An attacker impersonates an IMS Application Server and sends the UDR message to the HSS. The HSS receiving the message assumes that the request is from a valid AS and sends the requested information back. If the HSS has an access control list implemented, then the attacker would need to either be in control of a legitimate AS or know and spoof the identity of an AS. The Figure 6 shows the attack sequence. The Sh interface is usually only a network internal interface, but if the edge nodes or the nodes do not deploy proper interface separation, then an attacker can send a Sh message over an S6a interface.

6. COUNTERMEASURES

One of the main reasons for the attacks that we discussed in section 5 is the gap between the security standardization and deployment. At the time of writing this paper, the detailed guidelines for operators to improvise the security of their roaming interconnection is available in [25]. In this section, we will discuss two categories of countermeasures which may vary in terms of cost and effectiveness. We

strongly recommend considering both categories while deploying protection mechanism to the existing infrastructure.

6.1 Standardized security measures

As we discussed earlier in section , the Diameter protocol fails to provide security when the partners on the end nodes of an IPSec/TLS tunnel are untrusted. Mobile network operators from the developed countries often sell their outdated infrastructure to developing countries where the capital expenditure for telecommunication services is limited. In those countries, there is no strict legislations or knowledge to protect the end-user privacy. Therefore, as with many older IT equipment, it is much more vulnerable and can be misused to launch attacks on other networks. Furthermore, the trust related issues are even more challenging in the global IPX interconnection roaming hubs where there are no specific entities and policies to manage the certificates (and the related costs) within the interconnection network. These challenges can be solved by improvising the business practices and policies along with strengthening the technical security measures.

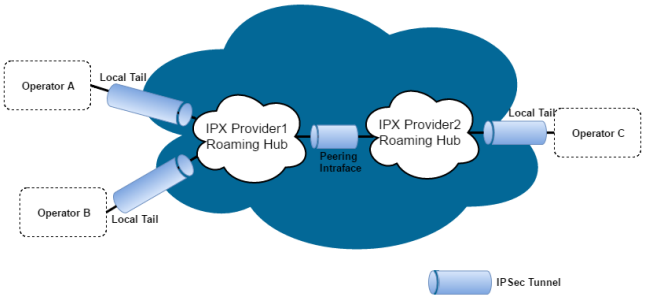

Figure 7: Diameter security

However, when the end nodes can be trusted, IPSec tunneling as part of Diameter specification standard [1] provides sufficient protection to the interconnection network. As represented in the figure 7, Diameter provides hop-to-hop connection based security and end-to-end session based security if implemented correctly, but IPSec or TLS offers no protection if the end-point is already compromised.

Exploiting the SMS protocol commands to sniff the victim's IMSI along with his operator's network topology has been a persistent attacking method since SS7. Those commands (*e.g.* SRR) cannot be simply blocked as they are used for user services. However, such exploits can be avoided if the operators correctly implement the *SMS Home Routing* mechanism as per the standard [7]. The aforementioned mechanism also provides protection from spam[8] SMS messages. Another security measure that we recommend is to harden network nodes according to the ongoing work of 3GPP as per [8] and [5], which provide protection approaches against the compromising of nodes. Nevertheless, there will always be partners that have not yet fully put their PKI in place and even if all service provider connected to the interconnection network have the financial resources and enthusiasm to secure the connections it will take the time to upgrade such a huge network. Therefore, it is important to have also other security measures in place as an additional defense line.

[8]Countries like China suffer severely from SMS spamming.

6.2 Efficient filtering mechanisms

Since some of the messages used for the attacks that we described in section 5 are part of regular communication, directly blocking those messages would interrupt the cellular services. The first approach is, that the nodes residing on the edge have proper interface separation i.e. they know if a message is for a Sh or S6a interface. Efficient filtering mechanisms based on the smart combination of cross-layer verification, IP-address-based blocking, origin/realm host checking, message details, attribute value pair verification and advanced access control methods are recommended the LTE networks against the location privacy breach attacks.

First of all, the operators should whitelist their partners based on the protocols, IP address of the nodes or origin and host realm, support for requested applications and required permissions. Such whitelisting is highly recommended due to the increased risk for the support for interoperability of lower generation networks of the partners. Secondly, the operators should thoroughly monitor their network traffic in real time. They should include robust statistical traffic analysis methods to detect any unusual or abnormal behaviour of the network nodes. Furthermore, the traffic from suspected nodes should be directed to honey-pots for further investigation to finally block the nodes.

One of the key advantages of using strong access control policies in the nodes - particularly in DEA/DRA is, even if the attacker bypasses sender origin filtering, the node would not respond beyond its configured functionalities. On the other hand, the cross-layer verification in the hop-by-hop routes of Diameter helps to verify the origin of a message such that the operators can automatically block[9] the messages originated from illicit nodes.

The above-mentioned filtering mechanisms might be available in the firewalls available in the market. However, it is very important to configure the firewall policies to effectively defend the LTE network against the attacks that we discussed in this paper.

7. CONCLUSION

In this paper, we provided a comprehensive review of security and privacy considerations of Diameter protocol. We discussed the possible exploits in Diameter which enable an attacker to illegitimately track the location of the mobile users in the LTE network. We argue that without appropriate countermeasures in place, the threats in terms of location privacy breaches are persistent in Diameter from their predecessor SS7. The default security and privacy guaranteed by the Diameter is not sufficient to make LTE as an attack-resistant network. While the roaming interconnections ensure cost-efficient way to provide cellular services on a global scale, it is important to deploy additional measures in the interconnection network to protect the privacy of the users.

8. ACKNOWLEDGMENTS

The authors would like to thank the members of GSMA RIFS group and Diameter protocol experts from Bell Labs - Nokia for their drive to improve the security of the global interconnection network. The authors would also like to

[9]This method works only if the sender's identity (*i.e.* Origin-realm AVP) is not replaced by the intermediate routers

thank the Finnish CyberTrust Project for financially supporting this research to improve the global communication security.

9. REFERENCES

[1] 3GPP. 3G security; Network Domain Security (NDS); IP network layer security. TS 33.210, 3rd Generation Partnership Project (3GPP).

[2] 3GPP. Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs). TS 29.338, 3rd Generation Partnership Project (3GPP).

[3] 3GPP. Policy and Charging Control (PCC) over S9 reference point; Stage 3. TS 29.215, 3rd Generation Partnership Project (3GPP).

[4] 3GPP. Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping. TS 29.213, 3rd Generation Partnership Project (3GPP).

[5] 3GPP. Security assurance scheme for 3GPP network products for 3GPP network product classes. TR 33.916, 3rd Generation Partnership Project (3GPP).

[6] 3GPP. Sh interface based on the Diameter protocol; Protocol details. TS 29.329, 3rd Generation Partnership Project (3GPP).

[7] 3GPP. Study into routeing of MT-SMs via the HPLMN. TS 23.840, 3rd Generation Partnership Project (3GPP).

[8] 3GPP. Study on security assurance methodology for 3GPP network products. TR 33.805, 3rd Generation Partnership Project (3GPP).

[9] 3GPP. Technical realization of the Short Message Service (SMS). TS 03.40, 3rd Generation Partnership Project (3GPP).

[10] 3GPP. InterWorking Function (IWF) between MAP based and Diameter based interfaces. TS 29.305, 3rd Generation Partnership Project (3GPP), Sept. 2008.

[11] 3GPP. InterWorking Function (IWF) between MAP based and Diameter based interfaces. TR 29.805, 3rd Generation Partnership Project (3GPP), July 2008.

[12] 3GPP. MME Related Interfaces Based on Diameter Protocol. TS 29.272, 3rd Generation Partnership Project (3GPP), Sept. 2008.

[13] 3GPP. Mobile Application Part (MAP) specification. TS 29.002, 3rd Generation Partnership Project (3GPP), Sept. 2008.

[14] S. Cheshire and M. Krochmal. Rfc 6763, dns-based service discovery. *Internet Engineering Task Force*, 2013.

[15] M. Cooper, Y. Dzambasow, P. Hesse, S. Joseph, and R. Nicholas. Internet x. 509 public key infrastructure: Certification path building. Technical report, 2005.

[16] T. Dierks. The transport layer security (tls) protocol version 1.2. 2008.

[17] Electronic Frontier Foundation. Surveillance Self Defense: The Problem with Mobile Phones. "https://ssd.eff.org/en/module/problem-mobile-phones", 2015.

[18] T. Engel. Locating mobile phones using signalling system 7. In *25th Chaos communication congress*, 2008.

[19] T. Engel. Ss7: Locate. track. manipulate. 2014.

[20] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn. Diameter base protocol. *IETF (The Internet Engineering Task Force) Request for Comments*, 6733, 2012.

[21] B. Gellman and A. Soltani. Nsa tracking cellphone locations worldwide, snowden documents show. *The Washington Post*, 4, 2013.

[22] GSMA. (IR.34) Guidelines for IPX Provider Networks (Previously Inter-Service Provider IP Backbone Guidelines V11.11. "https://perma.cc/P65P-42ET", 2015.

[23] GSMA. (IR.77) Inter-operator IP backbone security requirements for service providers and inter-operator IP backbone providers V3.0, 2015. (GSMA internal document).

[24] GSMA. SS7 and SIGTRAN Networks Security Issues V 2.0, 2015. (Available only to GSMA members).

[25] GSMA. SS7 Interconnect Security Monitoring Guidelines V 1.0, 2015. (Available only to GSMA members).

[26] GSMA. (IR.88) LTE and EPC Roaming Guidelines V14.0. http://www.gsma.com/newsroom/wp-content/uploads//IR.88-v14.04.pdf, 2016.

[27] E. Guttman, C. Perkins, and J. Kempf. Rfc 2609: Service templates and service: Schemes. *Network Working Group, The Internet Society*, 1999.

[28] S. Holtmanns, S. P. Rao, and I. Oliver. User location tracking attacks for lte networks using the interworking functionality. In *IFIP Networking Conference (IFIP Networking)*, 2016. (To appear).

[29] A. Hosia. Comparison between radius and diameter. *changes*, 1:2, 2003.

[30] A. D. Oliveira. Assaulting IPX Diameter roaming network. http://www.slideshare.net/yodresh/assaulting-diameter-ipxnetwork, 2016.

[31] L. Philippe. Diameter vs ss7 from a security perspective. http://labs.p1sec.com/2013/07/28/346/, 2013.

[32] S. Puzankov and D. Kurbatov. How to intercept a conversation held on the other side of the planet, 2014.

[33] S. P. Rao, S. Holtmanns, I. Oliver, and T. Aura. We know where you are! utilising the telecoms core network for user tracking. In *The 8th International Conference on Cyber Conflict (CyCon 2016)*, 2016. (To appear).

[34] C. Rigney, S. Willens, A. Rubens, and W. Simpson. Remote Authentication Dial In User Service (RADIUS). RFC 2865 (Draft Standard), June 2000.

[35] N. Seddigh, B. Nandy, R. Makkar, and J.-F. Beaumont. Security advances and challenges in 4g wireless networks. In *Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on*, pages 62–71. IEEE, 2010.

[36] S. K. Yoo, H. G. Kim, and S. W. Sohn. Enhancement of failover using application layer watchdog and sctp heartbeat in diameter. In *Mobile Communications*, pages 239–246. Springer, 2003.