ORACLE COMMUNICATIONS

Multi-Layer Security Protection for Signaling Networks

All-IP Invites Innovation, but also More Vulnerabilities

ORACLE WHITE PAPER | JANUARY 2016

ORACLE

Table of Contents

Introduction

The sanctity of mobile operators' networks and brands will depend greatly on their ability to deliver QoS guarantees to roaming and interconnect partners, while simultaneously protecting increasingly multimedia-savvy and socially connected subscribers. The challenge is that the all-IP architecture making mobile networks innovative and monetizable as digital lifestyle-enabling ecosystems are also making them more vulnerable to a multitude of security threats including: Denial of Service (DoS) attacks, IP address, malware, man-in-the-middle (MITM) attacks, botnets, identity theft, and service theft, to name a few.

In LTE, the environment can be even more "unpalatable" since operators have to distribute and manage user- and control- plane traffic across new partners through interconnect and roaming arrangements with others: service providers, developer communities, content and over-the-top (OTT) application providers, and network service providers. Since partners could unwittingly harbor malware and viruses among their payloads, "secure" environments are harder to come by as mobile cloud, OTT-driven applications and social media strategies evolve. To address security and roaming use cases, most operators have hunkered down at the IP layer with different types of encryption and firewall approaches – mostly leveraging IPSec and Transport Layer Security (TLS) security standards for security gateways, network routers, mobile VPN devices, and desktop VPN clients. Many mobile operators have investigated the IETF mandates for encryption in LTE networks, and are considering security measures and recommendations coming out of the GSM Association's Signaling Security Working Group (Sig SG) for both SS7 and Diameter networks.

While these courses of action can be effective – as devices and the core networks are the most heavily targeted areas for security threats – they will not be enough in and of themselves as the focus shifts beyond access and transport networks. Equal attention will be needed at the Signaling and Service Layers, which increasingly tie directly to operators' network assets, partner relationships, and subscriber privacy and loyalty. Consider, for instance, that in LTE networks no less than 100 percent of revenue- generating traffic becomes dependent on Diameter signaling. In multi-device/multi-screen environments, the Diameter protocol has to be appreciated and protected for its power to orchestrate critical communication among policy servers (PCRFs), charging systems, subscriber databases and many policy enforcement functions, such as packet gateways, deep packet inspection, application servers, and mobility management functions.

Diameter signaling will be so innate that Diameter traffic is expected to grow rapidly in the years to come. In fact, global diameter growth is accelerating at such a high rate that it could surpass global IP traffic growth in the near future, according to Oracle Communications LTE Diameter Signaling Index[1]. Though Diameter is powerful in what it can engender for revenue purposes, Diameter networks require enhanced security, as the all-IP nature of LTE exposes them to the risks inherent in the Internet.

This paper describes the measures that operators can implement to secure IP-based Diameter networks, namely:

- Access Control Lists (ACLs)
- Topology Hiding
- Congestion Control
- Protecting the Subscriber through Encryption

It looks at these measures in the context of how operators can achieve optimal management of the control plane, partners, equipment, processes and expectations. It also explains how Diameter Signaling Routers (DSR) in the core can play a crucial security role when complemented by several layers of security at the transport and the control/application layers. A multi-layer security approach should include the elements below, all of which should be considered at the inception of LTE and Diameter deployments. Once security breaches are detected, it is more difficult to implement all necessary components of an end-to-end security strategy.

Access Control List

For the reasons described at the beginning of this paper, no network can be considered a truly trusted network. It is the inherent complexity of today's interconnect and roaming use cases that will prove most impactful in terms of security policy in LTE networks, as the level of control typical with SS7 can no longer be expected. Data- and content-driven services – whether mobile voice, email, mobile data, mobile video, IMS-based services, or web services – cannot flourish in a closed environment.

In SS7 networks, routing messages into the signaling network is accomplished through generic addressing to a gateway signal transfer point (STP). The actual address of the network entity (the point code) is not advertised outside of the network. Global Title Translation (GTT) provides only the address to the gateway STP for further routing into the network. It becomes the responsibility of the STP to then route the message to the correct internal

[1] Oracle Communications Diameter Signaling Index Report at Oracle.com/diameter-signaling/router

address. The physical address is not relevant in this case, because in Time Division Multiplex (TDM) networks, network elements are interconnected via a dedicated circuit assigned to a port within the element itself. Routing tables then dictate to which port (or circuit) to send the signaling message.

In an IP network, however, network elements are interconnected through routers. The routers use an IP address to determine the next hop and to determine the final destination. If the IP address of an internal element is known, any network can gain access to the IP domain and send a signaling message to the IP address of an internal node. When this happens, the IP address of the originator is also provided. This is critical in LTE networks for the prevention of unauthorized access to the LTE core. An Access Control List (ACL) can be used to determine if the originating or sending IP address is known to the network. If the IP address is not known, and therefore not entered in the ACL, then access to the network is denied, and the message is discarded.

ACLs are common in data center networks today, and are effective in preventing access from unknown partners or rogue sites. However, in a multi-layer approach, the management of access by IP addressing alone is fortified with application layer security. Thus, DSR prevents unauthorized access by denying access to any network element that is not recognized, so that only known peers are allowed a session. In addition, the ability to filter messages on any AVP allows discarding messages that are not permitted in the network

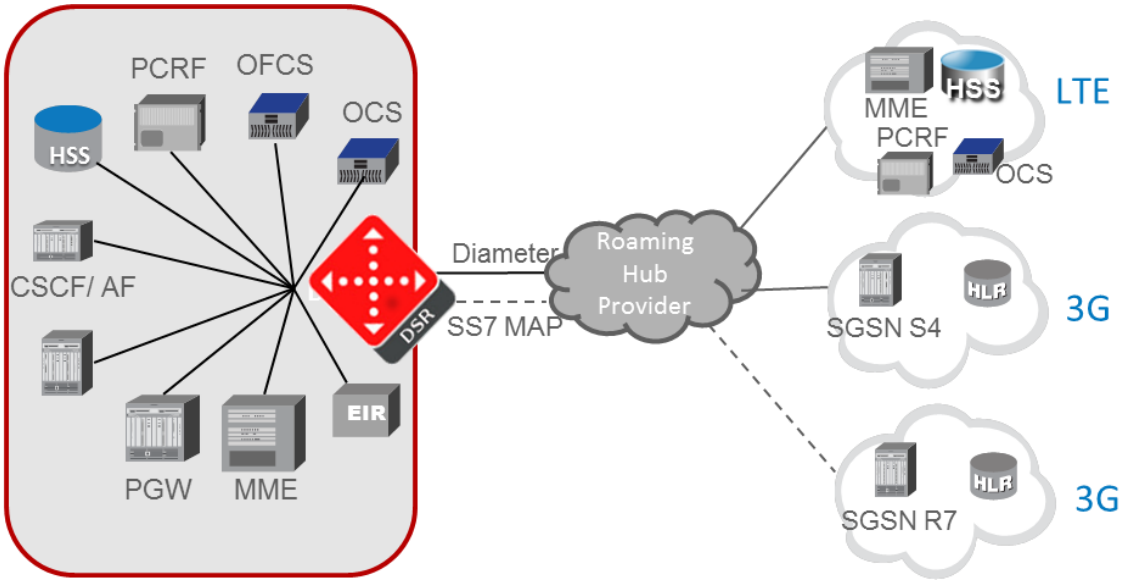

Figure 1.Oracle Communications DSR Roaming Proxy with Access Control List

Topology Hiding

It becomes easier in LTE for peer networks to learn the topology of home networks, potentially exposing the network to DOS and causing signaling surges that can flood Home Subscriber Servers (HSSs) and Mobility Management Entities (MMEs) with messages. By learning about the type and number of MMEs or HSSs deployed in a network, illicit sources can launch attacks targeted to specific nodes in home networks or gain sensitive network and subscriber data. This can also be an unintentional result from some type of event.

The first level of prevention is to hide details about the network topology. This is accomplished through topology hiding. When topology hiding is invoked, the host and realm names can be altered in such a way that they cannot be used to learn the network topology. To be effective, host names should never be advertised outside of the network. Some operators believe they must identify their host names for roaming agreements, but in fact this practice opens the network to more vulnerability. Topology hiding offers a different approach for interconnection by assigning multiple generic host names so that outside networks cannot learn about the identities or nodes used in networks.

The Diameter Edge Agent (DEA) is responsible for changing the host name of an outgoing message prior to sending to another network. The DEA uses a pool of host names previously assigned to the originating network element and randomly selects one of the generic host names from that pool. The DEA also maintains the session ID so it can associate any Answer command received back from another entity. When an incoming message is received, the DEA is responsible for determining the real host name assigned to the generic host name in the message, and forwarding to the correct host name.

This method prevents outside networks from learning the identities used in the network, and makes it more difficult to determine how many nodes are in the network since every host name is assigned multiple generic host names. If the concern is that someone could send a rogue message into the network using a generic host name and the real realm name, it must be remembered that the IP address of the originator must be present in the ACL in order to be granted access into the network. This can be implemented for all entities in the network, using mediation at the DEA. Mediation allows the DEA to substitute fields in the Attribute Value Pair (AVP) with values defined by the mediation table. For that reason, the cost of this type of implementation is minimal when compared to more "stateful" approaches.

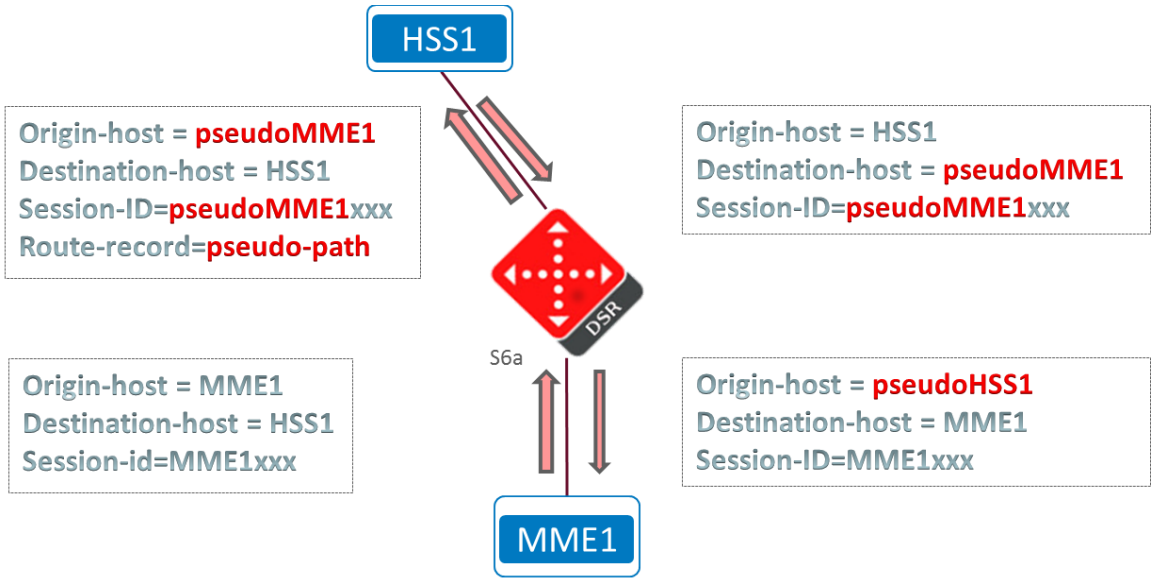

Figure 2.Oracle Communications DSR Topology Hiding

Congestion Control

Another important security consideration is congestion control. By using a centralized DSR, the operator can prevent signaling storms from reaching end nodes, such as the HSS. Since this is typically the intent of a DOS, having a mechanism for handling the DOS – should one occur – is a wise part of any security strategy.

When an attack occurs, and signaling levels reach a predetermined threshold, the DSR/DEA must slow down the flow of signaling messages to their destination. That can be accomplished by either discarding messages or throttling the flow of lower-priority signaling messages, which can then prevent a signaling storm. If congestion control is implemented at the end point, it loses its effectiveness, as the signaling already reaches its destination, leaving no choice but to discard the signaling messages and deny service. When congestion control is implemented in the core, signaling messages can be redirected to other redundant nodes, effectively load balancing wherever possible, and lessening the impact of the attack.

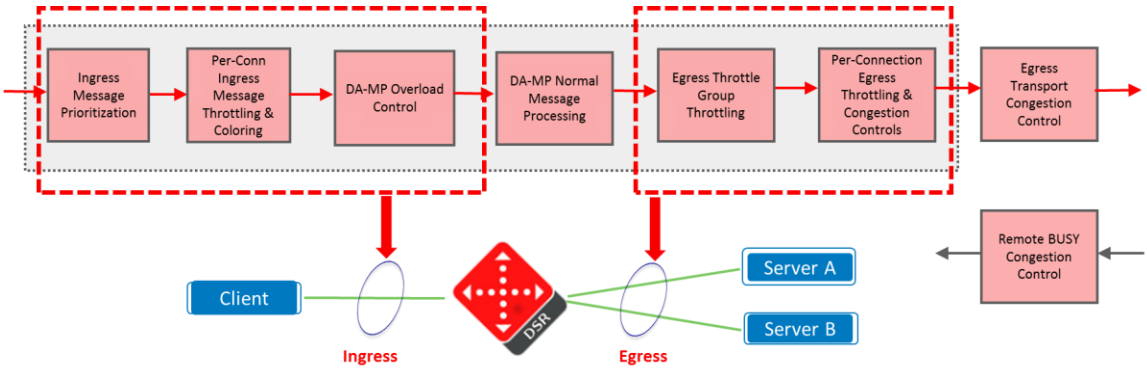

Figure 3.Oracle Communications DSR Overload and Congestion Control

Protecting the Subscriber through Encryption

Protecting subscriber data and privacy is one of the most important responsibilities a mobile operator assumes. The operator's success in protecting subscriber data and privacy links directly to loyalty, trust and profitability. In essence, subscriber data is the most important "payload," especially now that analytics and subscriber data management (SDM) have grown in importance for monetizing mobile data and personalizing services.

Protecting that data is more important now that mobile operators are looking at ways to broker the precious subscriber information in their possession to third-party advertisers and application and content providers, and as they look for ways to become "digital lifestyle providers" and subscriber "identity brokers" to third parties. The identity of a subscriber and the daily transactions undertaken by that subscriber have more meaning now than they did in the voice world. There is much that can be learned about subscriber behaviors through their daily transactions: what Internet sites they visit, who they send emails and messaging to, the location of the device, even the time of day during which they perform certain online tasks. All become valuable subscriber data that can be monetized.

As new ways to monetize subscriber data emerge, so do new security risks. With the increased use of smartphones for financial transactions, the risks will continue to rise. As that happens, encryption will be the most effective means

for protecting data, but its weaknesses should be acknowledged. For one, network monitoring through the use of probes is no longer as effective, because probes do not possess encryption keys. This makes monitoring of networks for performance and troubleshooting difficult. It can be assumed that this is the reason the industry has not been quick to implement TLS throughout networks. While TLS has remained part of the Diameter Base Specifications, few networks have actually implemented it. Another encryption method that has been recommended by the GSM Association at the DEA is IPSec. Encrypting the signaling between network connections is paramount to preventing man-in-the-middle attacks, eavesdropping on signaling sessions, and other common forms of intrusion in IP domains. While it is difficult to implement encryption within the network, encryption should be a requirement when interconnecting with another service provider.

Conclusion

4G/LTE networks provide bandwidth that dramatically enhances the subscriber experience and drive greater use of the advanced capabilities of modern smartphones. Mobile access through smartphones to the vast world-wide-web of information and services exposes networks to greater threats than ever before. With 2.5G and 3G networks, most sophisticated access was driven by laptops with wireless cards. These offered relatively few risks, as the users were typically business travelers accessing their corporate network via VPN connections. Now, however, every smartphone can access the Internet and expose networks to the best and worst it has to offer, including malware.

LTE adds an all-IP core infrastructure which brings with it new vulnerabilities to the most critical assets in network. Because Diameter is the protocol used throughout the core, protecting the core through centralized DSRs is one of the best means to ensure network and subscriber security. There are several levels of security that must be implemented, both at the transport and the control/application layers. This means several different mechanisms supported through the DSR/DEA should be leveraged.

The most basic of these mechanisms is the Access Control List (ACL), which dictates which IP addresses are granted access into the network. Hiding the topology of the network prevents attackers from launching targeted DOS attacks on specific nodes within the network through Diameter signaling flood. In instances where the host name is not known, specific nodes cannot be reached. Even if the host name is known, access is denied when the IP address of the originator is not absent from the ACL.

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

ORACLE

CONNECT WITH US

blogs.oracle.com/oracle
facebook.com/oracle
twitter.com/oracle
oracle.com

Integrated Cloud Applications & Platform Services

White Paper Multi-layer Security Protection for Signaling Networks
January 2016
Author: Travis Russell
Contributing Authors: Francisca Segovia