Communications Security, Reliability and Interoperability Council

CSRIC

March 2018

WORKING GROUP 3

Network Reliability and Security Risk Reduction

Final Report – Recommendations to Mitigate Security Risks for Diameter Networks

Version 1.1 – March 14th 2018

Table of Contents

1 Executive Summary

As described in the CSRIC V Working Group 10 Report, while the overwhelming majority amount of traffic using the Signaling System 7 (SS7) protocol is legitimate, the SS7 network connecting hundreds of wireless networks globally is subject to potential exploitation by bad actors that improperly obtain valid credentials on the black market. Current research indicates that similar vulnerabilities demonstrated in SS7 networks may also apply to Diameter networks, used in 4G/LTE as well as AIN/charging networks.

The use cases found in SS7 may exist in Diameter as well, namely: location tracking; voice/SMS interception; subscriber denial of service (DoS); and account fraud/modification. In addition to these use cases, the Diameter protocol may be used for the interception of user data sessions. Previous research exposed the GPRS Tunneling Protocol (GTP) to be vulnerable in 3G networks, but the functions provided by GTP have been replaced by the Diameter protocol in 4G. The Diameter protocol also introduces the potential to spoof the identity of networks due to the way Diameter routes commands from hop-to-hop, which is unique to Diameter. Similar to SS7, nation state attacks are believed to be the largest threat, and such attackers can be highly sophisticated and well-funded.

The Diameter vulnerabilities are at the same stage that SS7 was at just a few years ago. While the research community has begun to demonstrate use cases that can be used to exploit Diameter vulnerabilities, few if any attacks have been identified in production networks to date. This can be attributed to the fact that Diameter is not widely deployed between networks today and that the vulnerability (as with SS7) is tied to roaming. Carriers have not, to date, entered into widespread LTE roaming agreement and, as such, attackers continue to focus on SS7. As LTE roaming becomes more prevalent, this may change and the industry will be ready to meet the threat.

Due to the similarities between SS7 and Diameter threats, the industry can use the successful "playbook" it employed to combat SS7 threats to protect Diameter.[1] These steps, which are further delineated in the recommendations in this report, include: blocking certain message types, as recommended by GSMA; employing monitoring platforms; and implementing advanced firewalls. The industry has already begun these efforts, well before wide-spread targeting of Diameter by nefarious intruders.

Specifically, mitigation includes the implementation of firewall rules and policies deployed at the network edge (implementation of such can be through a standalone firewall appliance or Diameter edge agent, or DEA). The GSMA has documented guidelines for defining these rules and policies in FS.19 and FS.21. The GSMA continues work on these guidelines and should be the principal reference for safeguarding networks.

The S6a interface (connecting to the network Home Subscriber Server, or HSS) is the first focus of any security plan and should be protected from outside abuse. There are other interfaces providing external access to network resources that should be protected as well, but the S6a provides access to Personally Identifiable Information (PII) and network specifics, making it the prime target of attacks.

[1] Following the release of the WG10 report in March 2017, the FCC encouraged carriers to implement the best practices recommended in the report, and industry publicly expressed support of the recommendations and noted that industry is implementing them.

Security zones should be implemented to ensure the vulnerabilities are containerized, and access to one domain in the network does not expose the entire network. Isolation of the DEA is one example of creating security zones.

Diameter networks can be protected, and in many cases there are much better tools for securing Diameter networks. This is perhaps one reason global operators are moving their interconnections to Diameter, in place of SS7. However, Diameter also introduces unique vulnerabilities that must be taken into consideration prior to implementing Diameter at the roaming interconnect.

Government, including the Department of Homeland Security (DHS), should continue to engage with industry about enhanced protections for certain government officials and potentially valuable targets. This may also include the use of commercially available media encryption technologies to secure their voice and data sessions.

In North America, there should be consideration given towards establishing a ‘Circle-of-Trust’ between operators, to help protect North American networks. Operators should work in collaboration towards this goal.

The industry should continue working with industry and standards organizations and adopt best practices and guidelines (such as those recommended by the GSMA) for Diameter security as part of their planning for 5G and IoT deployments. Further study will be needed for 5G specific security recommendations.

2 Introduction

Telecommunications service providers have long interconnected their networks to support long distance and international calling. These connections were made with a level of trust between the limited number of operators with SS7 networks. With the introduction of wireless, and particularly wireless roaming, these connections became more prolific, with wireless providers interconnecting networks all over the world. The wireless industry expanded those interconnections as they expanded their roaming agreements, allowing their subscribers to roam anywhere in the world where they had roaming agreements in place. This expanded use of SS7 has had great benefits, and the overwhelming majority of traffic is legitimate, but has also increased potential threats.

To eliminate the need for a network operator to negotiate with hundreds of other operators, aggregators were introduced to provide the connectivity across the entire ecosystem. These aggregators provide an important role in the roaming ecosystem, managing traffic between hundreds of networks globally.

As smartphones entered the picture, new partners were needed to deliver content such as ring tones and music. These partners are not network operators but have been granted access to the control plane of networks so they can deliver content to the subscribers in the network.

As we described in CSRIC V WG 10, SS7 credentials have become more readily available to bad actors on the black market, forcing the industry to view any SS7 traffic as potentially nefarious. While many networks in the US have taken significant steps to lock down their networks to prevent unauthorized access, many outside the US have not.

As operators move from SS7 to Diameter for their interconnect protocol, the same issues addressed in the WG10 report are applicable. However, Diameter introduces unique attack vectors and additional vulnerabilities not identified in SS7. Operators are beginning to address potential threats to Diameter, in advance of widespread roaming that may introduce potential threats.

This report outlines the technology, the threat assessment, and recommendations to mitigate risk through roaming connections.

2.1 CSRIC Structure

Communications Security, Reliability and Interoperability Council VI		
Working Group 1: Transition Path to NG911	**Working Group 2: Comprehensive Re-imagining of Emergency Alerting**	**Working Group 3: Network Reliability and Security Risk Reduction**
Chair: Mary Boyd, West Safety Services	***Chair:*** Farrokh Khatibi, Qualcomm	***Chair***: Travis Russell, Oracle
FCC Liaisons: Tim May and John Healy	***FCC Liaisons***: Steven Carpenter and Austin Randazzo	***FCC Liaisons***: Steven McKinnon and Vern Mosley

Table 1 – CSRIC VI Structure

2.2 Working Group 3 Team Members

Name	Company
- Chair Travis Russell, Director, Cyber Security	Oracle Communications
Shirley Bloomfield, CEO	NTCA–The Rural Broadband Association
Don Brittingham, VP, Public Safety Policy	Verizon Communications
Charlotte Field, SVP, Application Platform Operations	Charter Communications
Bob Gessner, Chairman	American Cable Association
Michael Iwanoff, SVP and CISO	iconectiv
Mohammad Khaled, Senior Security Specialist	Nokia Bell Labs
Jason Livingood, VP, Technology Policy & Standards	Comcast Cable
Jennifer Manner, VP Regulatory Affairs	EchoStar
Robert Mayer, VP – Industry and State Affairs	USTelecom
Susan Miller, President & CEO	Alliance for Telecom Industry Solutions (ATIS)
Drew Morin, Director, Federal Cyber Security Technology and Engineering Programs	T-Mobile
Sara Mosley, Acting CTO, OCC/NPP*	Department of Homeland Security
Greg Schumacher, Technology Development Strategist	Sprint Corporation
Lee Thibaudeau, CTO & VP of Engineering	Nsight
Tim Walden, SVP of Engineering and Construction	Century Link
Jeremy Larson, Network Manager	USConnect
Martin Dolly, Lead Member of Technical Staff	AT&T Services Inc.
John A. Marinho, VP Technology & Cybersecurity (editor)	CTIA

Table 2 - List of Working Group Members

2.3 Subject Matter Experts (SMEs), Acknowledgements:

- Alexandre De Oliveir, Post Luxembourg
- Sergey Mashukov, Michael Downs, Positive Technologies
- Cathal McDaid, AdaptiveMobile
- Dr. Silke Holtmann, Nokia Bell Labs

3 Acronym Glossary

3GPP	Third Generation Partnership Project
5G	Fifth Generation
AAA	Authentication, Authorization and Accounting
AF	Application Function
AIN	Advanced Intelligent Network
APN	Access Point Name
AVP	Attribute Value Pair
BBERF	Bearing Binding and Event Reporting Function
CAMEL	Customized Applications for Mobile networks Enhanced Logic
CDMA	Code Division Multiple Access
CGF	Charging Gateway Function
CSRIC	Communications Security, Reliability and Interoperability Council
DA	Diameter Agent
DCCA	Diameter Credit Control Application
DEA	Diameter Edge Agent
DHS	Department of Homeland Security
DNS	Domain Name System
DoS	Denial of Service
DRA	Diameter Routing Agent
DTLS	Datagram Transport Layer Security
EIR	Equipment Identity Register
EPC	Evolved Packet Core
EPS	Evolved Packet System
FCC	Federal Communications Commission
FASG	Fraud and Security Group
GMSC	Gateway Mobile Switching Center
GPRS	General Packet Radio System
GSM	Global System for Mobiles
GSMA	GSM Association
GTP	GPRS Tunneling Protocol
H-PCRF	Home - Policy and Charging Rules Function
HPLMN	Home Public Land Mobile Network
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
IETF	Internet Engineering Task Force
IoT	Internet of Things
IMEI	International Mobile Equipment Identity

IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-CAN	IP Connectivity Access Network
IPsec	Internet Protocol Security
IP-SM-GW	IP Short Messaging Gateway
IPX	Internet Protocol eXchange
IWF	InterWorking Function
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MAP	Mobile Application Part
MME	Mobility Management Entity
MS	Mobile Subscriber
MSC	Mobile Switching Center
MSISDN	Mobile Station Integrated Services Digital Network
NE	Network Element
OCS	Online Charging System function
PCC	Policy Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PDG	PDN Gateway
PDN	Packet Data Network
PGW	Packet Gateway
PII	Personally Identifiable Information
QoS	Quality of Service
RADIUS	Remote Access Dial-In User Service
RAN	Radio Access Network
RFC	Request for Comments
SCP	Service Control Point
SCTP	Stream Control Transmission Protocol
SGSN	Serving GPRS Node
SGW	Serving GPRS support node Gateway
SIP	Session Initiation Protocol
SM	Short Message
SME	Subject Matter Expert
SMS	Short Message Service
SMTP	Simple Mail Transport Protocol
SPR	Subscriber Profile Registry
SS7	Signaling System 7
SSP	Service Switching Point
STP	Signal Transfer Point
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram protocol
URL	Uniform Resource Locator
VoIP	Voice of IP
V-PCRF	Visited - Policy and Charging Rules Function

VPLMN	Visited Public Land Mobile Network
WG	Working Group

Note: The table is non-exhaustive and covers the main terms relevant to Diameter. It excludes the Diameter Interface descriptors presented in Section 4.3 below. Additional terms may be specified within the document.

4 Overview of Diameter

Diameter is the global standard signaling protocol used for telecommunications traffic for 4G and LTE networks. The IETF defined the Diameter base protocol in RFC 6733. The Diameter base protocol is intended to provide an Authentication, Authorization, and Accounting (AAA) framework for billing and charging networks. This base protocol was later expanded to include support for network access and IP mobility in both local and roaming situations. The 3GPP standards are many, depending on the application being supported through Diameter. IETF RFC 6733 defines the minimum mandatory set of AAA operations. The 3GPP then defined additional requirements for network access and mobility. The requirements implemented through Diameter include:

- Failover: Diameter supports application-layer acknowledgements and defines failover algorithms and the associated state machine.

- Transmission-level security: Diameter provides support for TLS/TCP and DTLS/SCTP, as well as IPsec.

- Reliable transport: Diameter runs over reliable transport mechanisms (TCP, Stream Control Transmission Protocol (SCTP))

- Agent support: Diameter defines agent behavior explicitly

- Server-initiated messages: support for server-initiated messages is mandatory in Diameter

- Transition support: considerable effort has been expended in enabling backward compatibility with RADIUS so that the two protocols may be deployed in the same network.

- Capability negotiation: Diameter includes support for error handling, capability negotiation, and mandatory/non-mandatory Attribute-Value Pairs (AVPs)

- Peer discovery and configuration: Through DNS, Diameter enables dynamic discovery of peers. Derivation of dynamic session keys is enabled via transmission-level security.

The base protocol defines the message format, which comprises a header and a set of data elements expressed as attribute-value pairs (AVPs). By expressing data as AVPs, applications using the Diameter protocol can be extended in the future without having to modify existing source code or data inputs; new information is simply added as a new AVP. The base protocol defines a set of commands and AVPs that can deliver the minimum set of signaling functions, such as peer discovery, capability exchange, proxying, loop detection and error handling. The base set of operations can be extended by Diameter applications through the addition of new commands and AVPs. For reliable transport, Diameter supports both SCTP and TCP transport protocols, and transport security is provided by the TLS/DTLS or IPsec protocol.

Diameter is a peer-to-peer protocol that uses a request-answer transaction format. A Diameter peer (or Diameter Node) can be a client, a server or a Diameter Agent (DA). A Diameter Client is a device at the edge of the network that performs access control. Examples of Diameter clients include MME (Mobility Management Entity) and PCEF (Policy and Charging Enforcement Function) in EPS architecture. A Diameter Server is one that handles authentication, authorization, and accounting requests for a particular realm. Examples of Diameter servers include HSS (Home Subscriber Server) and PCRF (Policy and Charging Rules Function) in EPS architecture.

In a typical EPS architecture, the Diameter node that receives the user connection request will act as the Diameter client. In most cases, a Diameter client will be a Network Access Server. After collecting user credentials, such as username and password, it will send an access request message to one Diameter node serving the request. For simplicity, we assume it is the Diameter server. The Diameter server authenticates the user based on the information provided. If the authentication process succeeds, the user's access privileges are included in the response message and sent back to the corresponding Diameter client. Otherwise, an access reject message is sent.

The Diameter architecture also supports nodes called Diameter agents that are positioned between clients and servers, and forward client requests to the appropriate server. There are four kinds of agents: relay, proxy, redirect and translation. A relay agent uses the header information and routing related AVPs of a message to choose the destination peer. A proxy agent can modify AVPs in the message, it forwards messages, and may use the AVPs to determine the destination or apply a policy – for example, to reject a request. Redirect agents return requests to the originating client, providing information on the appropriate next hop that can service the request. Translation agents translate messages from one protocol into another. This type of agent was originally defined to translate messages from AAA protocols, such as RADIUS, to Diameter. However, translation from LDAP and MAP to Diameter is also of interest.

The GSMA defined the Diameter Edge Agent (DEA). The role of the DEA is to provide access into a network domain, while securing that domain. This is where topology hiding, access control lists, and filtering of Diameter commands are implemented. The DEA should be implemented as a standalone node; for example, with an IP address in a separate sub-domain. For this example, the IP address of the DEA should never be within the same group as other network elements it is protecting.

The Diameter framework can be developed by extending existing applications or by creating new ones. An existing Diameter application can be extended through the addition of optional AVPs. To implement additional functionality, new Diameter applications need to be defined which may imply new command codes and new sets of mandatory AVPs. The 3GPP Ro protocol is an example of how an existing Diameter application – the IETF-specified Diameter Credit Control Application (DCCA) – has been extended with additional AVPs to support the exchange of charging information.

4.1 Connection and Session in Diameter

A connection is a physical link between two Diameter nodes. It is mandatory for the Diameter protocol to run over either TCP or SCTP. Compared with UDP, used in RADIUS, these two protocols include features that provide more reliable transport, which is critical for applications exchanging accounting-related information.

Compared with a connection, a session is a logical connection between two Diameter nodes, and can cross multiple connections. A session is characterized by a sequence of activities within a timeframe; it refers to the interactions between a Diameter client and a Diameter server in a given period. Each session in Diameter is associated with a client-generated Session-Id that is globally and eternally unique. The Session-Id is then used to identify a particular session during further communication.

Routing in Diameter is implemented hop-by-hop. At each Diameter node, the destination address is examined, and the node determines how to reach the destination through its own routing tables. The node will also insert the IP address of the node it received the Diameter message from, as part of the Route_Record AVP in the message header.

The Route_Record AVP is inserted at each hop, until received by the destination. The destination will then create an answer, and using the Route_Record AVP, send the answer back to the last node in the path, using the same path in which it was received.

There is no authentication for the originator of a Diameter message relative to roaming scenarios that may involve multiple "hops".

4.2 Security in Diameter

Like SS7, Diameter was founded on a basis of trust between carriers developed for use in a closed community. As noted in the CSRIC Working Group 10 report, Legacy Systems Risk Reductions, carriers interconnected their SS7 networks because they properly presumed that the information and messages they receive from other carriers are valid and for legitimate purposes. While the SS7 system has proven effective and reliable over a significant amount of time, the SS7 community has evolved over time as the industry and ecosystem expanded. Ultimately, the result is that with more coverage, more networks, and more participants, the attack surface for a bad actor to potentially exploit the SS7 community of trust has increased.[2] The same possibility exists for Diameter.

Widespread roaming is the primary cause of the threats in SS7. However, there are only a small number of LTE roaming agreements today. As a result, the industry's past focus has been on where the nefarious activity and research has been targeted - SS7. Industry is now turning its attention to Diameter and will be following the same playbook for addressing vulnerabilities on Diameter as on SS7: blocking; monitoring; and firewalls; inclusive of network hardening, security by design, etc.

Additional security mechanisms such as IPsec may also be deployed to secure connections between

[2] WG10 Final Report at 10. https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

peers. However, all Diameter base protocol implementations are required to support the use of TLS/TCP and DTLS/SCTP or IPsec. The security parameters for TLS/TCP and DTLS/SCTP or IPsec are configured independent of the Diameter protocol. Diameter peer to peer secure connections must be established prior to any Diameter message exchange. Once established, all Diameter messages will be sent through the TLS/TCP and DTLS/SCTP or IPsec connection.

4.3 The Role of Diameter in the EPS Architecture

Diameter has been chosen for evolving networks not just for meeting the above-mentioned AAA criteria, but also for providing transfer of Quality of Service (QoS) as well as bandwidth and rating policies, subscriber profiles, and other sensitive data. The presence of Diameter in the (Evolved Packet System) EPS is spread across various interfaces described below.

Interface	Node	Node
S6a	MME	HSS
S6b	PDG	AAA
S6c	PDG	AAA
S6d	HSS	SGSN
S9	H-PCRF	V-PCRF
S13	MME	EIR
S13’	MME	EIR
Gx	PCRF	PCEF
Gy	PCEF	OCS
Gz	PCEF	CGF
Sp	PCRF	SPR
Rx	PCEF	Application Function

4.3.1 Interface S6a

The interface S6a lies between the HSS (Home Subscriber Server) and the MME (Mobility Management Entity) for authentication and authorization. This interface has the following properties:

- Transport of subscriber related data.
- Transport of location information.
- Authorizing a user to grant access to EPS.
- Transport of authentication information.

4.3.2 Interface S6b

The reference point S6b lies between the PDG (PDN Gateway) and the 3GPP AAA Proxy/Server for mobility-related authentication. This interface has the following properties:

- Transport of commands to retrieve and store the mobility parameters.
- Transport of static QoS.

4.3.3 Interface S6c

The S6c interface enables the retrieval of routing information for the transfer of short messages, the report of status of the delivery status of a short message and the alerting of the SMS-SC between the HSS, the SMS-GMSC and the SMS Router. This interface has the following properties:

- Between the SMS-GMSC or the IP-SM-GW and the HSS to retrieve the routing information needed for routing the short message to the serving MSC or MME or SGSN.
- Between the SMS-GMSC and the SMS Router or the IP-SM-GW, and between the HSS and the SMS Router or the IP-SM-GW in order to enforce routing of the SM delivery via the HPLMN (Home Public Land Mobile Network) of the receiving MS.

4.3.4 Interface S6d

The interface S6d lies between the HSS and the SGSN (Serving GPRS Support Node) used to retrieve and store mobility-related parameters. This interface shares the same properties as those of S6a.

4.3.5 Interface S9

The reference point S9 lies between the H-PCRF (Home Network-Policy Charging and Rules Function) and the V-PCRF (Visited Network-Policy Charging and Rules Function) in the EPS network. This interface has the following properties that enable the H-PCRF:

- Dynamic PCC control, including both PCEF and, if applicable, BBERF (Bearer Binding and Event Reporting Function) in the VPLMN.
- Transport of IP-CAN-specific parameters from both the PCEF and, if applicable, the BBERF in the VPLMN.
- Serves Rx authorizations and event subscriptions from the AF in the VPLMN.

4.3.6 Interface S13

The reference point S13 lies between the MME and the EIR (Equipment Identity Register). This interface has the following property:

- Enables the ME Identity check procedure between the MME and the EIR.

4.3.7 Interface S13’

The reference point S13’ lies between the SGSN and the EIR and has the similar property as that of S13.

4.3.8 Interface Gx

The reference point Gx lies between the PCRF (Policy Charging and Rules Function) and the PCEF (Policy Control Enforcement Function) in the EPS network and enables the PCRF to have dynamic control over PCC behavior at the PCEF. This interface has the following properties:

- Enables the signaling of PCC decisions.
- Negotiation of IP-CAN bearer establishment mode.
- Termination of Gx session.

4.3.9 Interface Gy

The online charging reference point Gy lies between the PCEF and the OCS (Online Charging System Function). This reference point Gy provides the same functionalities as those of reference point Ro.

4.3.10 Interface Gz

The offline charging reference point Gz lies between the PCEF and the CGF. This reference point Gz provides the same functionalities as those of Rf in the EPS.

4.3.11 Interface Sp

The reference point Sp lies between the SPR (Subscription Profile Registry) and the PCRF (Policy Control and Charging Rules Function). This reference point provides following functionalities and is not limited to:

- Transfer of subscriber information related to IP-CAN based on subscriber Id.
- Unsolicited notifications about subscriber information change

4.3.12 Interface Rx

The reference point Rx lies between the AF and PCRF. This reference point provides the transport of application-level session information and is not limited to:

- IP filter information that identifies service data flow for the policy control.
- QoS control of media/application bandwidth.
- Notifications on IP-CAN bearer level events.

4.4 Diameter networks – wireless implementations

The Diameter protocol is the main protocol suite used for 4G core networks. It is the base protocol for billing, authorization, authentication, accounting and mobility management in both Home and Roaming networks. Diameter signaling provides information to network elements about whether a particular user is authorized to use specific services. The Diameter Routing Agent (DRA) manages communication among the network elements, eliminating the need for direct connections between network elements.

4.4.1 Wireless Architecture

The 4G/LTE wireless network consists of the Radio Access Network (RAN), and the Evolved Packet Core (EPC). The EPC can also be divided into the user plane and the control plane. The user plane supports the delivery of subscriber data sessions using specialized routers named the Serving GPRS Support Node Gateway (SGW) and the Packet Gateway (PGW).

The SGW is used for routing subscribers data sessions within the EPC, while the PGW is used for connecting to external packet networks (such as the Internet). Both the SGW and the PGW must communicate through the control plane to the other network elements in the EPC.

The other network elements include:

- The Home Subscriber Server (HSS)
- The Policy and Charging Rules Function (PCRF)
- The Subscriber Profile Registry (SPR)

The HSS is used for storing the subscriber profile in the home network, and is the most targeted network entity in the EPC because of the information it stores. All of the network elements in the EPC have an interface to the HSS so they can retrieve authentication and authorization information for a subscriber when a subscriber is roaming or using the network services.

Serving/visited networks access the HSS in the subscriber's home network when a subscriber of that network roams onto the visited network for the purpose of authorization and authentication so subscribers can receive the same services they get from their home networks while they are roaming.

The PCRF is used to define QoS and other permissions regarding a subscriber's use of the network. For example, the PCRF can define what types of data sessions a subscriber is allowed during specific periods of the day, as well as based on the device type they are using.

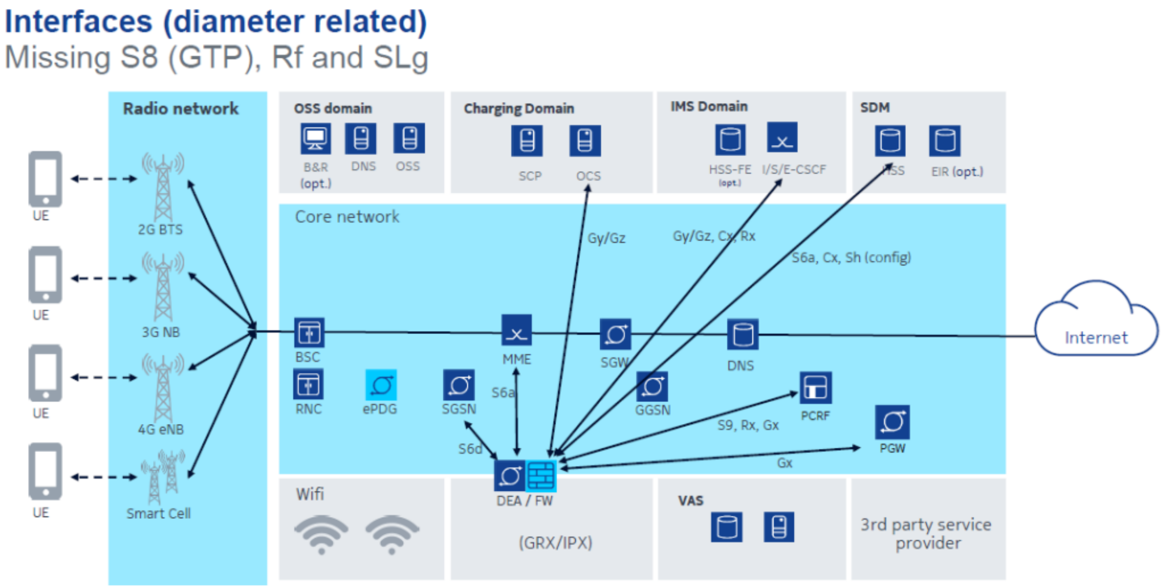
The PCRF is accessed by the SGW and PGW (policy control enforcement functions, or PCEFs) to retrieve the policy assigned to the subscriber, and to determine what privileges are to be granted to the subscriber based on a number of criteria, including:

- Subscriber
- Time of day
- Type of device
- Site being accessed (such as the URL or the Access Point Name or APN)

These aspects are mentioned here should an attacker gain access to the PCRF, where they could theoretically change the policy for specific subscribers (or group of subscribers).

When networks interconnect to support roaming, they typically use the IPX for the exchange of packets across networks. On the order of about 800 operators are officially recognized and a large number of service providers have wholesale business arrangements and lease out access. Large service providers (e.g. national carriers) often maintain direct connections with "peers". Also new players that come from the classical internet business and now offer connectivity services often just rent the connectivity service from a connectivity provider and do not make all roaming relationships themselves (e.g., Apple SIM). An IPX provider may aggregate access with other operators that could traverse several IPX providers from source to destination.

The figure below gives an overview of the relevant Diameter based interfaces which are typically used in wireless networks:



Interfaces (diameter related)

Missing S8 (GTP), Rf and SLg

Figure 1 – Diameter Interfaces

4.4.2 Relevant standards and protocols

The Diameter protocol was developed by the IETF as a replacement for the RADIUS protocol. The RADIUS protocol is used primarily for authentication, authorization, and accounting (AAA) in packet networks, however, RADIUS has many issues that drove its replacement.

The original document, RFC 3588 was replaced with RFC 6733, which added some additional recommendations for security as well as clarification on some aspects of 3588. Note that the RFC 6733 serves as the base protocol document, defining the basic functions of the Diameter protocol. Because the protocol was developed for charging networks, the base protocol focuses on procedures in the charging domain, and not in wireless networks. For this reason, the 3GPP defined additional standards for using the Diameter protocol in wireless networks, including charging in wireless networks. In addition to charging, the Diameter is used for Mobility Management, Location, and QoS Policy Applications.

IETF RFC 6733	Diameter Base Protocol
IETF RFC 6408	Diameter Straightforward-Naming Authority Pointer (S-NAPTR) Usage
IETF RFC 7683	Diameter Overload Conveyance Indication
IETF RFC 3403	Dynamic Delegation Discovery System (DDDS) Part Three: The Domain Name System (DNS) Database
3GPP TS 29.336	HSS interfaces S6m, S6n, and S6t (for IoT)
3GPP TS 33.210	3G Security; Network Domain Security
3GPP TS 29.229	Cx/Dx Interfaces
3GPP TS 29.213	Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping
3GPP TS 29.272	Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol
3GPP TS 29.329	Sh interface based on Diameter Protocol, Protocol Details
3GPP TS 29.215	Policy and Charging Control (PCC) over S9 reference point; Stage 3
3GPP TS 29.338	Diameter based protocols to support Short Message Service (SMS) capable Mobile Management Entities (MMEs)
3GPP TR 28.305	InterWorking Function (IWF) between MAP based and Diameter based interfaces
3GPP TS 23.003	Technical Specification Group Core Network and Terminals; Numbering, addressing and identification
3GPP TR 29.805	InterWorking Function (IWF) between MAP based and Diameter based interfaces
3GPP TS 23.078	Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase 4; Stage 2
3GPP TS 32.251	Telecommunication management; Charging management; Packet Switched (PS) domain charging
3GPP TS 29.173	Location Services (LCS); Diameter-based SLh interface for Control Plane LCS
3GPP TS 29.172	Location Services (LCS); Evolved Packet Core (EPC) LCS Protocol (ELP) between the Gateway Mobile Location Centre (GMLC) and the Mobile Management Entity (MME); SLg interface
3GPP TS 33.116	Security Assurance Specification(SCAS) for the MME network product class
3GPP TS 33.117	Catalogue of general security assurance requirements
3GPP TS 33.916	Security Assurance Methodology (SCAS) for 3GPP network products
3GPP TS 33.250	Security Assurance Specification for PGW network product class

Table of Diameter standards applicable to this report

The Diameter network consists of many different network elements. Each of these network elements is connected via interfaces, and it is these interfaces that are identified in the 3GPP standards. They are referred to as applications, and each interface is given an application identifier (such as S6a, denoting the interface between the MME and the HSS).

Within 3GPP, there are typically three sets of documents defining each of the interfaces. The first document will describe the overall purpose of the application. The second provides more details regarding the commands defined for the application, and the third even more details regarding all of the Attribute Value Pairs (AVPs) defined for each command.

3GPP profiles the IETF RFC for wireless network applications, therefore there are also some inconsistencies between RFC 6733 and the 3GPP standards. Some commands defined by the IETF are ignored by the 3GPP, as well as 3GPP specific AVPs defined. It is therefore important to understand which application you are looking to understand, and you select the correct 3GPP document for that interface. The 3GPP standards will identify which commands and AVPs they ignore, and which new commands and AVPs they have introduced specifically for wireless applications.

The 3GPP continues to define new applications for the Diameter protocol, for use in 3G as well as 4G networks. As 5G is defined, there will be additional applications defined for use in 5G.

4.4.3 Wireless Security Practices

Given its experience with SS7, there is considerable knowledge about how to address Diameter issues. For example, following the release of the WG10 Final report in March 2017, the FCC encouraged carriers to implement the best practices recommended in WG10.[3] Industry publicly expressed support of the recommendations and noted that industry is implementing them.[4] For Diameter, there are key network functions (e.g., MME), interfaces (e.g., S6a, S9), protocol messages and communications (e.g., hop-by-hop) that need to be addressed by security technology and operational processes.

The 3GPP standards forum has defined network security assurance requirements and a methodology for evaluating a vendor’s network product development practices and the network product’s lifecycle management processes (Technical Specs 33.116, 33.117 and 33.916). It includes protecting the network element’s availability and integrity, user authentication and authorization, session management, logging and securely configuring the operating system and web-based management services.

The GSMA FASG has produced practical and useable security recommendations that address the protecting against attacks against Diameter[5]. It has considered the security problems that can occur throughout the different IP and Diameter protocol layers and at critical boundary and internal interfaces.

In a Diameter-based network, all Network Elements (NEs) are connected via an IP interface, typically with SCTP transport. The interfaces that may most likely be attacked that use the Diameter protocol are S6a, which provides connectivity between the HSS and the MME; S6c, which provides connectivity between the HSS and

[3] https://apps.fcc.gov/edocs_public/attachmatch/DA-17-799A1.pdf

[4] https://www.ctia.org/docs/default-source/default-document-library/ss7-statement-2017-final.pdf

[5] FS.19 – Diameter Interconnection Security; FS.21-Interconnection Signaling Security Recommendations

the central SMS functions; S9 which provides connectivity between the home PCRF and the visited PCRF: and SGd, which provides connectivity between the MME and SMSC. These and other interfaces can be abused unless protections (e.g., topology hiding) are in place and controls are employed to detect and mitigate incursions on these interfaces.

Most Diameter communications are based on a hop-by-hop routing whereby messages respond to the previous node in the chain versus the original sender. Passive monitoring of interconnect signaling traffic to detect illegitimate traffic, and active testing and auditing of the signaling infrastructure to increase the operator's understanding of its network vulnerabilities, are valuable tools in developing a security strategy as they are for SS7. The WG10 final report also noted the value of these practices.

Diameter firewalls, SS7 firewalls, and traffic filters (e.g., whitelisting allowable messages at edge devices while blacklisting unacceptable messages) are effective deterrents to many kinds of attacks, particularly when they are implemented at network edges, before potential malicious traffic has the chance to enter the core network. Filtering should be done at all layers to provide message protection, application and command level security, SMS layer protection, and lower layer protection.

Similar to what is being done to protect SS7 networks, advanced data analytics that combine subscriber data with signaling data can be used to detect new forms of attack as well as identifying specific targets such as individuals, or organizations.

As telecommunications network providers implement security in the form of filtering, and firewall capabilities, the question of where that functionality will be hosted becomes an issue that needs careful consideration. At one extreme is the architectural option to place all functionality into a single NE; such as a combination IWF (Interworking Function)/firewall/standalone firewall appliance/event monitor/filter/etc.; while at the other extreme is the option to break functionality out into many discreet NEs.

The first option offers the ease of all-in-one service, with associated higher costs;

- Additional network elements,
- Added latency,
- Higher administrative overhead to manage the appliances,
- Increased chances of failure of one or more capabilities in response to bad software updates for a single, perhaps unrelated, capability in the same box, and
- Possible corruption of the whole device by malicious attackers or careless insiders.

The second offers protection against some of those all-in-one disaster scenarios at the expense of more complex provisioning, and perhaps de-conflicting interactions among the security services, particularly if they are offered by different vendors or run variants of standard protocols. The advantages, disadvantages, and trade-offs of implementing security are all important factors that must be considered as part of the security architecture, costing, and operations planning and implementation. Good security architecture dictates defense in depth as the best overall choice for security implementations. Both approaches outlined above are viable.

Many operators have already implemented filtering on their STPs and DEAs, as well as the HLR/HSS. This did not add complexity (or network elements) to the network. It did add complexity to the provisioning of those nodes, but at a smaller cost than an external appliance. The standalone firewall appliance, on the other hand, adds complexity as well as latency.

The growing complexity of the networks and variety of interconnected entities combined with increasing sophistication and determination of network attackers mean that more processing time must be dedicated to protecting those networks and their traffic. It is therefore worth considering the role of trust and "rules" for relying on trusted partners, networks, and network interconnections. In 3GPP, there have been initial contributions towards defining circles of trust for network boundaries. Trusting traffic from an adjacent network service provider (due to an SLA or other considerations) must be tempered by the knowledge that the adjacent network may trust its own adjacencies to differing degrees that might be incompatible with the first network's expectations. There could also be rogue operators, who may "front" adversarial networks in a trusted environment.

Though a couple of standard efforts in the IETF and GSMA have been initiated to define end-to-end application level encryption, none of these have been completed. It is recommended that networks use hop-by-hop IPSec encryption. Both 3GPP and the GSMA said IPSec is required for Diameter network encryption.

4.5 Diameter networks – wireline implementations

The Diameter protocol is used in wireline networks as well as wireless networks; however, the use in wireline is predominantly for charging (and could be used for AIN applications).

4.5.1 Wireline architecture

The Diameter protocol was originally designed to replace the RADIUS protocol used in telecommunications networks for charging functions in the back office. The IETF defined specific interfaces between the network elements responsible for subscriber sessions for the purpose of recording user sessions. The interfaces connect these network elements to the charging domain where the usage is recorded for billing.

In this capacity, the protocol can be found in wireline networks. However, given that wireline subscribers are not mobile, many of the network functions defined by the 3GPP are not necessary, and therefore the Diameter protocol is fairly limited in its implementation in wireline networks.

The use cases discussed in this report do not apply to wireline, nor has any research been published on vulnerabilities in wireline networks. However, as reported by CSRIC V WG10, the vulnerability is in connecting two networks using the SS7 or the Diameter protocol. Therefore, wireline networks should not be ruled out as vulnerable.

4.5.2 Wireline Security Practices

The wireline network is composed of traditional telecommunications network elements, SS7 signaling interfaces and associated messaging and the evolution to IP-based networking. These network elements include the Signal Transfer Points (STPs), Service Switching Points (SSPs), and Service Control Points (SCPs). Working Group 10 identified the wide variety of attack vectors for an attacker to potentially gain both domestic and international access to the signaling plane, take advantage of the trust relationships between interconnected service providers, abuse the SS7 protocols for reconnaissance and exploitation purposes and compromise the network elements and their databases. These attacks can impact both the individual and groups of subscribers.

The advent of Voice over IP (VoIP) has brought the Session Initiation Protocol (SIP) into the wireline network as well as the need to interface with new generation mobile technology and services. This interworking has brought the Diameter protocol to interface with the embedded base of SS7-based signaling networks.

SS7 is a much bigger target of attack than is Diameter, which is still in its infancy as a network protocol. As Diameter's presence grows beyond network element and application interfaces to interconnection. Diameter attacks will likely increase.

4.6 Interworking Functions

The interworking between SS7 and Diameter messaging has now become a key area of security focus. Security needs to address the different Interworking Function (IWF) architectural options, new IWF network functional elements and the actual filtering of SS7 and Diameter signaling messages so that attacks are not propagated from one network environment to another network environment. For example, LTE-based service providers may need to support interconnection to SS7/MAP-based networks to enable roaming by using IWF functions to convert signaling messages and mapping the AVPs. Failure to mitigate these attacks could result in SS7 vulnerabilities enabling subscriber profile discovery and unauthorized modifications, targeted subscriber location queries and billing fraud on Diameter based networks.

Because the transition from 2G/3G networks to LTE/EPC will not happen overnight, SS7 and Diameter will coexist for the next ten to twenty years, which means that IWF functions will be a major network component for some time to come.

5 Diameter Threat Assessment

This section discusses threats, attack methodology, interdependencies, and impacts that may result from compromising the Diameter signaling network.

5.1 Introduction

The telecommunications network infrastructure is composed of different subsystems to support end-to-end services. These trusted subsystems include the endpoints (e.g., smartphones, cars), access network (e.g., radio cell towers), core network (e.g., switches and databases) and interconnection points between service providers (e.g., STPs, Diameter Edge Agents - DEAs, Gateways). These different network elements, protocol stacks, service functions, and databases are targets of attacks with different intentions, resulting in various impacts to the infrastructure, services, and subscribers.

The working group considered reported vulnerabilities (e.g., that have been discovered by industry or security researchers) and reports of exploitation, if any. Industry is taking steps to coordinate and research the reported vulnerabilities, while being cognizant that the overwhelming amount of Diameter traffic is legitimate.

Figure 2 provides a traditional end-to-end view on security threats to Mobile Networks:

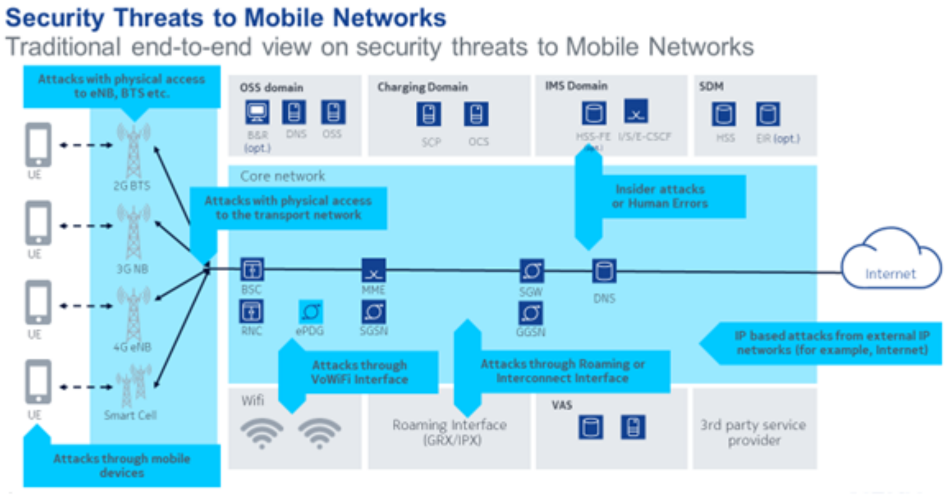

Security Threats to Mobile Networks
Traditional end-to-end view on security threats to Mobile Networks
Attacks with physical access to eNB, BTS etc.
OSS domain
B&R (opt.)
DNS
OSS
Charging Domain
SCP
OCS
IMS Domain
HSS-FE
I/S/E-CSCF
SDM
HSS
EIR (opt.)
UE
UE
UE
UE
2G BTS
3G NB
4G eNB
Smart Cell
Core network
Attacks with physical access to the transport network
Insider attacks or Human Errors
BSC
MME
SGW
DNS
Internet
RNC
ePDG
SGSN
GGSN
IP based attacks from external IP networks (for example, Internet)
Attacks through VoWiFi Interface
Attacks through Roaming or Interconnect Interface
Wifi
Roaming Interface (GRX/IPX)
VAS
3rd party service provider
Attacks through mobile devices

Figure 2 – Security Threats to Mobile Networks

The threat assessment content for this section was initially sourced from a series of subject matter expert (SME) presentations to the CSRIC Working Group members and augmented by additional research information provided by working group members. The SMEs that presented to the CSRIC WG3 members included:

- Segey Mashukov and Michaell Downs, Positive Technologies
- Alexandre De Oliveir, Post Luxembourg
- Cathal McDaid, AdaptiveMobile
- Dr. Silke Holtmanns, Nokia Bell Labs

Travis Russell, Director, Cybersecurity at Oracle Corporation and Chair of WG3 provided a presentation on the threats to Diameter signaling based on his previous research.

5.2. Assessment

5.2.1 Comparison of Threat Environment between SS7 and Diameter

As described in the CSRIC V WG10 report, the SS7 Network was originally founded on the basis of trust between members of a small closed community of carriers. Carriers interconnected their SS7 networks because they properly presumed that the information and messages they receive from other carriers are valid and for legitimate purposes, and the system has proven effective and reliable over a significant amount of time. However, the SS7 Community has evolved over time as the industry and ecosystem expanded, yielding several consequences:

- The growth in mobility use and widespread global roaming has increased the number of carriers with access to the SS7 network.
- The assumptive trust nature of the network being a closed community was true when SS7 was first deployed. After the global trend in deregulation of the telecommunications sector, in the U.S. exemplified by the Telecommunications Act of 1996, deregulation removed many of the restrictions on access and, in

fact, mandated the opening up of networks. While this is a good thing for an array of reasons, it did result in certain complications, one of which is the barrier to gain access to SS7 was dramatically lowered.

- Access to SS7 networks has increased over the past few decades, in some instances, by design, as telecommunications networks and network functions were opened up to more competition, and were adapted to novel uses and new services, like Application to user SMS services (e.g., for financial information, flight information, password recovery etc.).

Ultimately, the result is that with more coverage, more networks, and more participants, the attack surface for a bad actor to potentially exploit this community of trust has increased.[6]

When the industry began using IP as a transport in 2000, the ability to connect networks became much easier, requiring an inexpensive logical connection rather than an expensive special circuit. As a result, content providers and other partners gained access into the control plane to support subscribers as they roamed from network to network, or even to simply provide content.

Attackers could also gain access to the control plane through negotiated connections they purchased from complicit and rogue operators and/or content providers. This potential vulnerability exists in the Diameter protocol as it too provides the same services as SS7, in the 4G/LTE domain. To date, researchers have not published on actual attacks to Diameter, but they have demonstrated the vulnerabilities, thus as the attack surface grows, so does the likelihood of Diameter attacks. This is likely because the potential vulnerability is related to widespread roaming over SS7. To date, there are not widespread LTE roaming agreement and, as such, the working group assesses that bad actors continue to target SS7.

Bad actors are able to use SS7 access, along with legitimate network identifiers purchased through the rogue service providers to gain access to any network worldwide from remote locations. Diameter adds a new attack vector due to its routing mechanism; spoofing a network is possible in the Diameter protocol.

Like SS7, the Diameter protocol was built upon a trust model. Initially, Diameter was designed as a replacement for the Remote Access Dial-Up User Service (RADIUS) in charging networks, and was expanded to include the many services and applications needed in wireless networks. While discussions around end-to-end encryption have long been discussed even for SS7 networks, the industry has yet to define any such standards that meet the needs of operators worldwide (easy to implement, is not cost prohibitive, and does not impact performance).

Diameter was not initially developed as a telecommunication signaling protocol. The Diameter protocol suite was developed by the IETF to facilitate authentication and billing. The 3GPP adopted Diameter as a replacement signaling protocol to SS7 for use in 4G networks. Diameter suffers from the same breakdown of the trust model that has occurred with SS7. It is possible to get access through an Internet Protocol eXchange (IPX), the interconnect between different IP based telecommunications networks, by posing as an information service and using spoofing to implement an attack. This is similar to purchasing access to the SS7 network through one operator and then traversing into partner networks over the intercarrier exchange posing as a legitimate platform in the network.[7]

[6] WG 10 Final Report at 6. https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

[7] “Diameter Security Overview” subject matter expert presentation by Positive Technologies, October 2017

The motivations behind potential attacks in Diameter are no different than what was discovered in SS7. As in SS7, attacks are most likely to be focused on location tracking, call and text interception, data interception, DoS, and account fraud. However, these are simply the known use cases and others may manifest as Diameter implementations increase.

While the use cases generally remain the same, there are a number of factors that are influencing the current threat environment. Diameter offers a much smaller attack surface since SS7 is still the dominant signaling technology deployed in telecommunication networks globally. A comparative analysis done by an expert of operator traffic over a representative time period identified SS7 traffic traversing over 200 countries compared to only 60 countries for Diameter. The same sample set identified 35 times more discrete SS7 traffic sources than Diameter sources. As a result, the profit motivated attacker is more likely to spend time and resources to exploit vulnerabilities of SS7 than Diameter. The exception to this is in cases where CDMA is the technology used. Diameter may be more attractive as an attack vector because there is little to no research on attacking CDMA and many of the operators using CDMA and other non-GSM technologies are moving to Diameter for their interconnects. The end result is that more Diameter networks are expected to deploy as some operators in Europe are now accelerating their implementation plans for Diameter at the edge.

Diameter attacks tend to be more complicated and sophisticated than SS7 attacks. This knowledge gap is likely to gradually close as research is becoming more readily available on possible Diameter attacks.

It is anticipated that attacks in Diameter networks may eventually become more prolific than SS7 over time as Diameter deployments increase. SS7 is a difficult technology to learn and requires years of expertise to fully understand. Conversely, Diameter is a text-based protocol based on HTTP and SMTP, two well-known and broadly implemented Internet protocols. Access and knowledge of the underlying protocols are more widespread.

While some researchers claim visibility to “suspicious traffic” in Diameter networks, there lacks any superlative evidence that these are indeed attacks rather than configuration issues. The general types of Diameter attacks - tracking, interception, spoofing, DoS, and fraud - are described in more detail in the sections that follow. Still, with much fewer Diameter implementations at the edge of the network, there remains to be seen any actual Diameter breaches discovered in the wild.

However, as noted above, the industry has already learned from its security controls implemented in the SS7 network and is not starting from scratch for Diameter. As Diameter is implemented between more networks as the roaming interface, the need for these same controls in Diameter will be paramount. In general terms, the types of Diameter attacks are similar to those seen in SS7 and focus on tracking, interception, disruption, and fraud and are described more in the sections that follow.

5.2.2. Diameter Attacks

There are two phases to any attack; discovery and attack. During the discovery phase, the location of the subscriber is retrieved, along with the subscriber IMSI and subscription details. This information is then used for the next phase of call or text interception. While the location tracking and other attacks are often described separately as individual use cases, they are in reality key parts of a bigger exploit as well.

5.2.3 Location tracking

First, it is helpful to understand exactly what location tracking is, and is not. Location tracking in the SS7/Diameter sense does not provide granular location data for a consumer. The information retrieved through location tracking is therefore limited to cellID or serving MSC/MSS address, which in itself may disclose the city or general area within a city for a target, but not specific GPS coordinates as seen with other attack vectors (such as malware on a device where these coordinates can be retrieved). Even this information can be harmful though, depending on the subscriber. VIPs and government officials need to be especially wary of this possibility.

Location tracking through the SS7 network is one of the main attacks. Location tracking through Diameter is seeming to be a similarly conceptualized process with the same impacts as it was in SS7. This breaching method is expected to continue to be a threat to Diameter signaling as the attacks are fairly “simple” to produce results against an unprotected network. Location tracking is the process of attaining individualized information of subscribers’ locations to develop pattern maps of the target’s whereabouts. The impacts of location tracking most commonly lead to the collection of location coordinates of a subscribers’ locations which is considered confidential subscriber information and an explicit violation of Personal Data Protection Laws.

In Diameter, the HSS can be queried over the S6a interface using User Data Request (UDR) to return IMSI information. The attacker then has ability to utilize Diameter commands over the S6a interface and retrieve cell ID (CID or ECI) and location codes (TAC or LAC). If the cell ID and/or location codes are revealed, the attacker has the ability to determine the location of the cell tower through publicly available websites. The attacker can also use the Send Routing Information for Short Message (SRR) to the HSS masquerading as an SMSc in the visited network, using the S6c interface. This will yield similar results. There are several other ways for retrieving this information, so not every attack is the same. Attackers will use a variety of methods depending on the response received from the network they are attacking.

5.2.4 Call and messaging intercept

Call and data interception is a more complicated attack and requires quite significant expertise and might not be possible for all networks, due to implementation and configuration specific approaches. As a consequence, this sort of attack is typically not done by unsophisticated attackers. On the other hand, the sophisticated attackers are well funded and build a shareable attack-toolbox to use and combine different approaches. This is a similar model to what occurred with SS7 attacks over the past few years.

Call and text interception is done by redirecting a call or message away from the serving network, by masquerading as a roaming partner now serving the target subscriber. The attacker redirects the traffic to their own target destination to eavesdrop on the call, read and answer the text messages, and even complete the call loop as a man-in-the-middle.

To initiate an SMS intercept, the attacker first uses the Send Routing Info for SM Request (SRR) over the S6c interface to the HSS. This message is intended to query for the current serving MME and IMSI of the targeted subscriber from the HSS. Once this information is obtained from the Send Routing Info for SM Answer (SRA), the attacker can then use the Update Location Request (ULR) over the S6a interface to update the HSS to provision the spoofed MME as servicing the target customer's IMSI. When the subscriber sends a text message to the SMS-C, the SMS-C platform queries the HSS for the serving MME and receives the spoofed MME address. The SMS-C then forwards the message to the attackers MME. The message flow for this example of an intercept attack is depicted in the figure below[8].

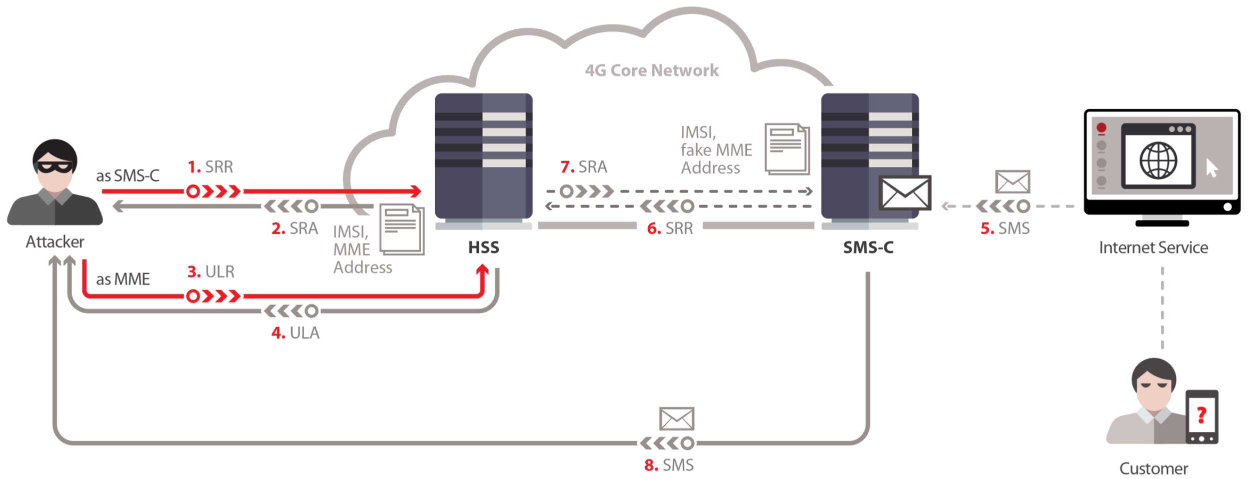


Figure 3 - Example Message flow for intercept of SMS messages

There are different implementations of SMS over NAS (Non-Access Stratum) signaling. This seems to depict an attack based on the least commonly deployed architecture currently in which the SMSC interacts with the MME directly without an MSC/VLR and the SGs interface being involved.

Call and message interception are serious threats to subscribers. In many cases, confirmation/verification codes from social networks, banks, etc. are sent via SMS to the subscriber and attackers can capture and exploit these confirmation messages using this Diameter attack. Attackers also have the ability to forward calls to record and/or listen to conversations using a similar intercept approach. There is an example of this attack in the SS7 domain. In 2017, numerous subscribers of O2 Germany found their bank accounts drained after attackers transferred funds from their hacked bank accounts to the attackers' bank accounts. [9] When the banks sent a text message for two-factor authentication, the attackers were able to use SS7 to intercept the text message and use the sent code to authorize the bank transfers. This is a good example of a complex, multi-tiered attack using the signaling network of wireless networks.

[8] Sourced from "Diameter Security Overview" subject matter expert presentation by Positive Technologies, October 2017

[9] http://securityaffairs.co/wordpress/58735/hacking/ss7-protocol-cyber-heists.html.

5.2.5 Network spoofing

The objective of network spoofing is for the attacker system to pose as a legitimate roaming partner network or platform in order to gain access to the target network. Once this access is granted, the attacker is then in a better position to execute many of the other exploits already noted in this section – interception, DDoS, location tracking, etc. In order to execute a network spoofing exploit, the attacker needs to gather information on architecture and interconnects. The GSMA IR.21 provides much of this information for the configuration of legitimate roaming interconnects. Other methods include exploitation of the IPX Domain Name Service (DNS) to provide network specific addressing and topology information; sending the Authentication Information Request (AIR) with a legitimate IMSI to the HSS which will respond with its name and other network topology information; or even the “good faith” purchase of Diameter access from a service provider that is then misused. This information is used to then pose as legitimate roaming partner platforms to gain access to the target network.

In Diameter networks, commands are routed one hop at a time. Each hop is determined based on where the message originated (Origin) and the destination. There is no concept of end-to-end routing in Diameter at each routing node. When a Diameter agent receives a request, the agent examines the origin, and saves the session ID associated with the request as well as the address of the adjacent node that forwarded the request (not the originator, but the adjacent node). The agent then forwards the request on to the next hop in the path to the destination. This next agent repeats a similar process, recording the address of the node that forwarded the request. The session ID serves as the reference in message routing. The address of the adjacent node that forwarded the packet is also recorded with the session ID so the answer can be routed using the same path.

When the answer is received, each node looks at the session ID to identify the node that sent the request. The answer is then forwarded back to that node using the same path from which the request was received.

The origin address is not integrity checked or protected during the transport. This method of Network Spoofing is depicted in the figure below.

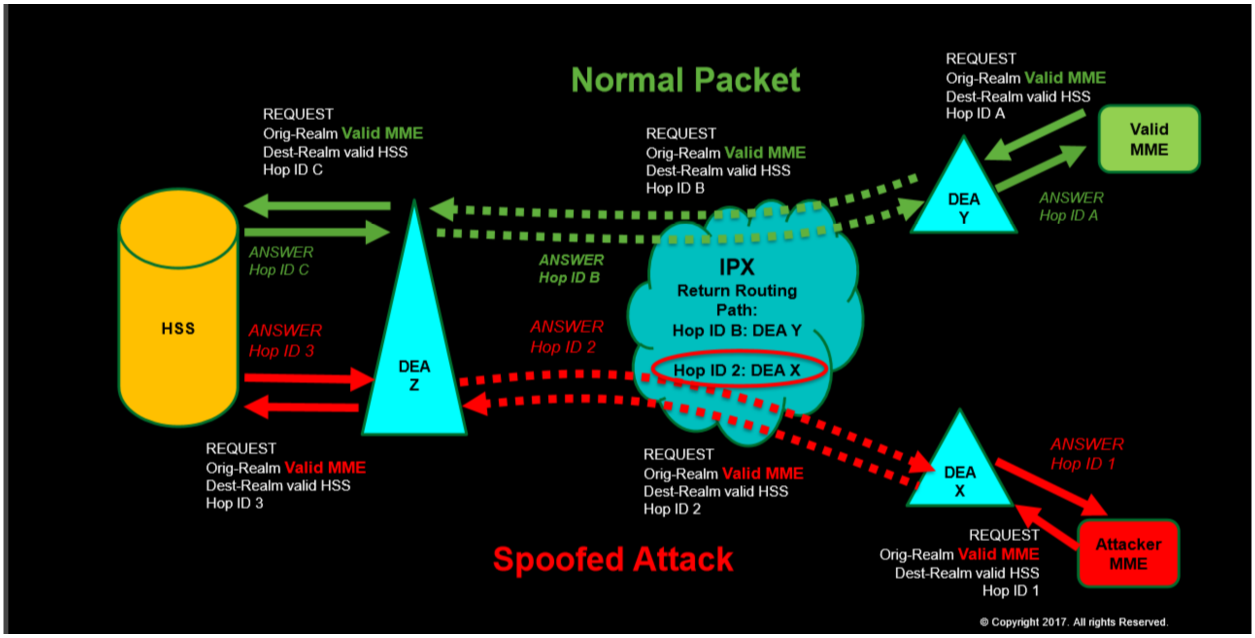


Figure 4 - Spoofing Vulnerability through Hop-to-Hop Authentication[10]

Vendors and operators consider this to be the biggest threat to Diameter networks, and something that was not identified in the SS7 studies because of the end-to-end routing used in SS7. As long as attackers are able to spoof a network node to gain access into the roaming ecosystem, it will be very difficult to detect and mitigate potential attacks.

5.2.6 Denial of Service (DoS) attacks in Diameter

There are two types of denial of service attacks identified in researcher claims (and reported in the CSRIC V WG10 report). Network DoS attacks usually target the HSS by sending a flood of requests to the HSS (such as Reset) overwhelming the capacity of the HSS, and resulting in an outage. As subscribers attempt to register in the network, they are denied because the HSS is unable to receive the authentication requests, and services for the entire network are shut down.

Another type of DoS attack focuses on groups or individual subscribers. The intent of these attacks is to purge their subscriber profiles from the VLR. When this happens, the subscriber is unable to use their device until they either move to another cell site (which will initiate the Update Location Request and re-register the device with the VLR/HSS) or they turn the device off and back on again.

An example of a subscriber-based DoS attack begins with the attacker posing as the HSS and sending an Insert-Subscriber-Data- Request (IDR) with IMSI of the subscriber through the S6a interface. The IDR specifies that the subscriber is connected to a fake MME. This results in MME services blocked for the subscriber since the network identifies it as connected to the fake MME. Figure 5 below showcases a visualized procedure of DoS affecting a subscriber through Diameter.

[10] Sourced from "Diameter Security Research" subject matter expert presentation by Cathad McDaid, Chief Intelligence Officer, AdaptiveMobile Security, November 2017

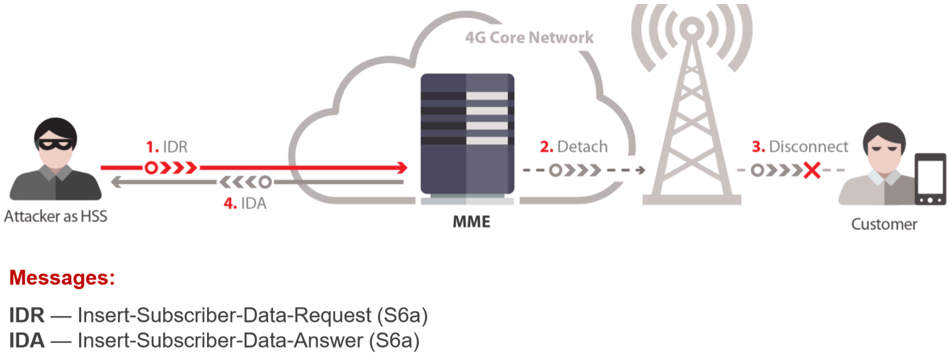


Figure 5 - Example of a DoS Subscriber Attack[11]

Denial of Service subscriber attacks can target both individuals and groups of individuals (such as groups of first responders). When a subscriber is blocked from network services, the impact is temporary. If the subscriber turns the device off and back on again, or moves to another tower, the device will re-register with the network and normally correct the manipulated profile.

Such attacks do not require an answer message, i.e., the attacker sends traffic to overwhelm the receiver and does not need to track the flooded requests.

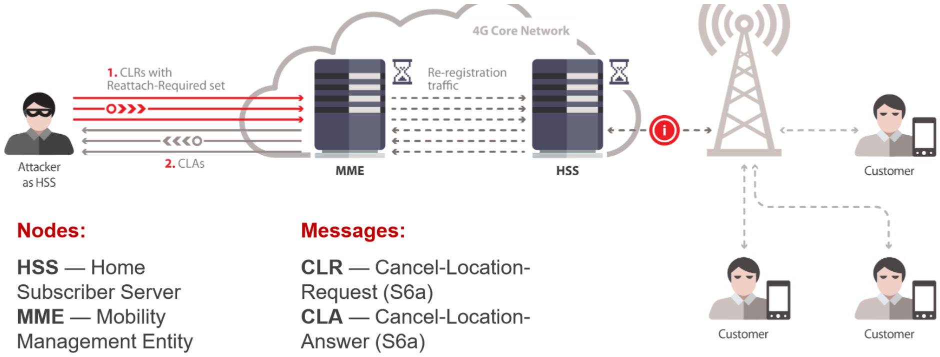

4G Core Network
1. CLRs with Reattach-Required set
Re-registration traffic
2. CLAs
Attacker as HSS
MME
HSS
Customer
Customer
Customer
Nodes:
HSS — Home Subscriber Server
MME — Mobility Management Entity
Messages:
CLR — Cancel-Location-Request (S6a)
CLA — Cancel-Location-Answer (S6a)

Figure 6 - Example of a DoS Network Attack[12]

The implications and effects of DoS attacks can lead to expansive outcomes for the end-user. Subscriber DoS can disrupt the service and display end-user subscribers as temporarily "unavailable" (until next registration). Subscriber DoS can also lead to reputational damage for the user itself. For further clarity, Figure 7 below, Types of DoS Attacks in Diameter, provides a summary of the various forms of DoS attacks, and its formulation requisites, procedure, and consequences.

[11] Sourced from "Diameter Security Overview" subject matter expert presentation by Positive Technologies, October 2017

[12] Sourced from "Diameter Security Overview" subject matter expert presentation by Positive Technologies, October 2017

5.2.7 Fraud attacks in Diameter

In a fraud attack, the attacker impersonates a legitimate subscriber to gain access to services typically to avoid being charged for this access. The attacker uses the Insert Subscriber Data Request (IDR) message over the S6a or S6d interface to inject or update subscriber profile data on the MME and HSS.

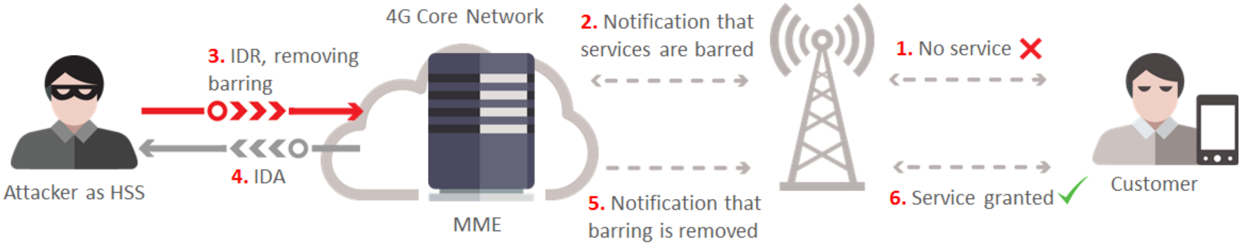


Figure 7 - Example of Fraud via S6a IDR

The fraud risk should be considered likely. First, profit motivated attackers may change the subscriber profile to get a “happy-flat-rate” and then re-sell the access. The second reason is that the subscriber profile is stored in many nodes and some of them are needed to be accessible from the IPX (e.g., MME / SGSN).

In addition to the attacker changing the subscriber profile for fraudulent purposes, this vulnerability is also part of intercepting a voice call. By attacking the charging system, attackers can modify the call forwarding parameters on a subscription so calls are diverted to their device. This is used for listening in on the call, but they also must complete the call as a man-in-the-middle attack.

This is analogous with the SS7 call intercept scenario that used the CAMEL protocol for attacking the charging system. With the Diameter protocol, the attack becomes simpler, because only one protocol is required.

5.3 Summary Threat Assessment

There is a clear market for interconnection based attacks due to the richness of data available from the cellular networks. In 2014 the HackingTeam claimed in a customer communication that they are working on similar capabilities as they have for SS7 also on Diameter / LTE.[13] Data acquisition service companies and darknet companies are highly customer oriented, and it is just an evolution of their services offering. The subject matter experts reported on the first detected location tracking attacks using the Diameter protocol to a running live network[14].

Insecure network configurations could make attacks easier and the interconnection network "approachable/visible" from the Internet and thereby hackable. It is assumed that Internet style attacks via Diameter will target the cellular core network (e.g., ransomware and related blackmailing). We have already seen the impact of platform vulnerabilities, e.g., with processor vulnerabilities and operating systems (e.g., Meltdown[15]). Regardless of configuration of platform risks, precautions should be taken to ensure the ability to isolate a compromised element. For example, the DEA should be isolated from the rest of the core network. This could mean putting it on its own subnet so if the DEA is compromised, it cannot be used to "hop-scotch" across the network via IP (a configuration issue).

It should be assumed, that the network may be accessed without authorization at some point. Given such an event, mitigation should be such that nothing breaks and services are resilient. In the event services go fully down, recovery plans, clear chain of commands, recovery procedures and emergency drills are essential mechanisms to reduce the outage time to a minimum and accelerate recovery with minimum damage and loss.

[13] https://wikileaks.org/hackingteam/emails/emailid/133908

[14] https://wiki.aalto.fi/download/attachments/112176170/Cellular%20Location%20Tracking%20Attacks.pdf?version=1&modificationDate=1464017180942&api=v2

[15] https://blog.malwarebytes.com/security-world/2018/01/meltdown-and-spectre-what-you-need-to-know/

6 Diameter evolution – 5G

The same network functions found in 3G and 4G will exist in 5G as well. While the architecture has changed to a Service Based Architecture (SBA), the same capabilities must exist to support roaming sessions.

One major change in 5G is the use of the protocol HTTP2 as a transport for JSON and RESTful protocols. These protocols will be used for signaling in the new architecture, however, there will remain legacy Diameter interfaces as well.

A pure 5G Core System (i.e., 5GC) relies on HTTP2 interfaces, except for some legacy interfaces: Diameter/MAP is supported on the interface between the SMS-GMSC/IWMSC and HSS, SMS-GSMC/IWMSC and SMSF. IMS related interfaces are also still applicable and will still be Diameter (e.g., Rx, Sh, Cx, Dx)

For the 5G architecture option 3, where the 5G radio terminates a Gateway (g)Nb into the existing 4G EPC, all of the EPC diameter interfaces are maintained.

Even though many operators are announcing their plans to deploy 5G networks, the reality is most will elect to deploy 5G at the RAN and use the existing 4G core network. This means Diameter will continue to support the network for some time. Likewise, 5G handsets MUST support 4G (LTE), requiring Diameter networks to support those sessions.

7 Findings and Recommendations

Like Signaling System 7 (SS7), Diameter is recognized as a critical component of the United States telecommunications infrastructure supporting both wireline and mobile services and subscribers. These technologies have become targets of both domestic and international attackers with different motivations and create different risks for both service companies and subscribers. The attacks have exploited the legacy trust ecosystem that has been in place for many years. The increased interconnection among different types of service companies, and changing business and geo-political factors have also played a role in increasing the frequency and volume of targeted attacks. The result is that with more coverage, more networks, and more participants, the probability that bad actors will exploit this community of trust increased as noted in the CSRIC V Working Group 10 Report.[16]

7.1 Findings

As found in CSRIC V, WG10, there are many similar measures that can be taken for Diameter security as in SS7. Key to protecting the network is monitoring and analytics. Without visibility to both the ingress and the egress network traffic, it will be impossible to detect network breaches and mitigate attacks.

Likewise, good network hygiene is important. This consists of access control, as found in the GSMA recommendations found in FS.19, FS.21, and IR.88. Managing access with a least privilege policy should be implemented for every network connection.

Mobile networks are complex. There are thousands of nodes, servers, different protocol stacks, different software releases and different vendors. In such large networks, implementation mistakes or misconfigurations of nodes may happen. Possible misconfigurations increase network vulnerabilities.

Network infrastructure vendors commonly perform testing of network nodes; i.e. testing to ensure that nodes are compliant with industry standards and behave according to specifications. Specifications are created for interworking purposes and this testing is focused on features and performance. Other testing approaches include what happens if “incorrect” data is sent or if too much data is sent. These break testing techniques include edge condition testing to stress the platform (or network), One example of this testing, commonly known as fuzz testing, involves sending massive amounts of random data (“fuzz”) to the target platform in an attempt to uncover coding flaws.

However, even when hardened network nodes are deployed, configuration mistakes could lead to new attack vectors. When firewalls and network gateways (such as DEAs) are deployed, security assessments should be used to ensure that the configurations are proper, and that erroneous or rogue traffic cannot pass through. The GSMA provides guidelines for testing of these nodes. The CSRIC concludes that ongoing security assessment of the network signaling infrastructure to detect and mitigate possible threat vectors, consistent with best practices and standards is required.

The roaming ecosystem continues to be the primary attack vector, and special care should be taken to protect these relationships.

[16] https://www.fcc.gov/file/12153/download

Contracts should also be revisited, to ensure there is language to prevent roaming partners, content providers and OTT providers from exploiting their connections. The GSMA Wholesale Agreements & Solutions group (WAS) has created language to be used by member companies to address this.

7.1.1 Implementation of IPSec and TLS/DTLS

The use of the IPSec protocol has been considered previously in CSRIC. This report documents the fact that Diameter message routing is managed on a hop-by-hop versus end-to-end basis. Implementing IPSec as an end-to-end security wrapper poses significant technical and procedural challenges. Further, the vulnerabilities in Diameter discussed in Section 5 of this report are not the result of ”in flight” exploitation of traffic. The vulnerabilities are exploited by a rogue platform that is authenticated at the ”border” of the network under attack. Even if using IPSec for end-to-end encryption were determined to be feasible, it would require a very significant systemic peer-wise effort on multiple hops in order to ensure end-to-end security where most operators in the ”hop” chain are not bound to the FCC or US based practices. It could also compromise the security of current implementations of CALEA and other Lawful Intercept practices.Therefore it is considered at this time that IPSec for Diameter at interconnection points would have very low impact and very limited benefits, noncommensurate with the broader impacts, complexity implications and requisite investment.

The topic of end-to-end encryption and authentication should be revisited in 5G. Given the standards are currently in development and the principal transport for signaling is HTTP2 on TLS, this should be easier than previous attempts at retrofitting existing networks and technologies to support authentication. However, end-to-end encryption introduces other challenges for network operators, and the mechanism must be such that it does not prevent transit networks from being able to identify rogue traffic.

IoT brings about new challenges for networks. Broadband IoT (BB-IoT) can be used to create a DoS attack on networks simply through the infection of devices with botnet malware. However, 3GPP has defined Narrowband IoT (NB-IoT) using the Diameter protocol for delivering its payload. A new network function has been introduced for 4G and 5G networks for terminating all NB-IoT traffic and managing access by these devices to prevent DoS attacks from affecting the Diameter network, but this is a new function that has not yet made its way into all networks. All operators should consider the benefits of the new Services Capabilities Exposure Function (SCEF) as a means of controlling NB-IoT traffic, and isolating it from the rest of the Diameter network.

The CSRIC concludes that ongoing security assessment of the network signaling infrastructure to detect and mitigate possible threat vectors, consistent with best practices and standards is required.

Consistent with Cybersecurity Risk Management and Best Practices from CSRIC Working Group 4[17] and recommendations from subject matter experts, it is recommended that industry evaluate Diameter ”peer” relationships based on the GSMA guidelines and recommended service level terms. Message filtering based on GSMA recommendations are viewed as having the most significant mitigating impact.
The CSRIC concludes the continued use and leverage of existing industry consumer advisories and recommendations for the use of end-to-end encryption is appropriate and beneficial. Consumers and VIPs should be encouraged to use commercially available applications for securing their communications as defined in these recommendations.

[17] https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

7.2 Final CSRIC Working Group Recommendations

7.2.1 Recommendations for the FCC

The CSRIC recommends the FCC and its federal government partners, including the Department of Homeland Security (DHS), continue to engage with industry on Diameter security issues and share information and threat intelligence about Diameter threats (e.g., FCC consider convening a workshop with industry and government stakeholders to highlight the Diameter CSRIC Report and industry best practices).

The CSRIC recommends the FCC and its federal government partners, and specifically DHS, engage with industry about the possibility of enhanced protections for Very Important Persons (VIPs), including which government employees would be considered VIPs. Further, the CSRIC recommends that the government, in coordination with industry as appropriate, should also provide education and awareness to VIPs about best practices[18] to mitigate security threats (See Section 8 Appendix).

The CSRIC recommends the FCC and its federal government partners develop procedures to accelerate the declassification of actionable threat information such that it can be shared with industry in a timely manner.

7.2.2 Recommendations for industry

7.2.2.1 US Critical infrastructure protection

Consistent with Cybersecurity Risk Management and Best Practices from CSRIC Working Gorup 4[19] and recommendations from subject matter experts, it is recommended that industry evaluate Diameter ”peer” relationships based on the GSMA guidelines and recommended service level terms. Message filtering based on GSMA recommendations are viewed as having the most significant mitigating impact.

7.2.2.2 GSMA Security Best Practices and Guidelines

The CSRIC recommends that industry use the GSMA security best practices and guidelines to secure signaling interconnections for Diameter as described in Section 4.

7.2.2.3 Threat Information Sharing

The CSRIC recommends and endorses continuing efforts to improve information sharing of threat intelligence[20] that can be used to adapt monitoring, filtering and data analytics, see Section 4.

7.2.2.4 Diameter in Emerging 5G Networks

The CSRIC recommends that the industry continue to participate in industry and standards forums and adopt the

[18] CTIA. Protecting Your Data on Your Mobile Device. https://www.ctia.org/consumer-tips/protecting-your-data-on-your-mobile-device (March 2018)

[19] https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf

[20] CSRIC WORKING GROUP 5: CYBER SECURITY INFORMATION SHARING
https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf

GSMA recommended controls to address emerging security risks as part of their overall 5G and IoT security approach as outlined in Section 6 and 7.

7.2.2.5 Subscriber Media Encryption Support and User Authentication

The CSRIC recommends that industry encourage the use of available media encryption technologies, for both voice and data communications, in particular for highly sensitive and critical applications or for Very Important Persons (VIPs) that may often be targeted by bad-actors. Over the long-term CSRIC recommends continued tracking and assessment of advancements in end-to-end user authentication, media integrity protection and media encryption techniques.

7.2.2.6 Security Assessments

The CSRIC recommends and endorses security assessments as a tool to be applied and used based on specific network architectures, CSRIC further recommends continued risk management based on the unique requirements of each network and the corresponding unique test results.

7.2.2.7 Network Administration

CSRIC Recommends that Network Administrators implement secure domains, and if they serve multiple countries, each country should be operating in its own domain. Security domains are interconnected through security gateways (SEGs). Security gateways are deployed at the network boundaries to protect against attacks and unauthorized access. CSRIC Recommends that a security gateway is implemented with limited access to network resources, to limit attack surfaces. The security gateway is only used to protect the control plane and not the user plane.[21]

7.2.2.8 North America Circle of Trust

For North America, consideration should be given to a Circle-of-Trust initiative. This initiative should include discussion of collaboration to help meet potential threats. All operators in the region must agree on this, and measures could be implemented to increase visibility to traffic in and out of those networks.

[21] “LTE Signaling With Diameter,” Russell, Travis; McGraw-Hill, NY 2016

8. Appendix: Sample Industry References (Links)

a. http://www.verizonenterprise.com/products/mobility/enterprise-mobility-management-security/voice-cypher/
b. http://www.verizonenterprise.com/industry/public_sector/public_safety/docs/vz_network_security_wp.pdf
c. https://www.t-systems.com/us/en/solutions/security/solutions/mobile-encryption-app/cell-phone-encryption-391684
d. https://www.t-mobile.com/company/privacy-resources/your-privacy-choices/marketing-choice.html
e. http://about.att.com/sites/cybersecurity?source=IC2Y0H0000000000L&wtExtndSource=cyberaware
f. http://about.att.com/sites/cybersecurity/ae/hce
g. https://www.att.com/esupport/article.html#!/wireless/KM1010136
h. https://www.att.com/support/fraud-and-security.html
i. https://business.sprint.com/blog/top-5-data-loss-prevention-practices/
j. http://es.sprint.com/sdshop2/en/solutions/managed_services/encrypted_email.shtml