Communications Security, Reliability and Interoperability Council

CSRIC

March, 2017

WORKING GROUP 10

Legacy Systems Risk Reductions

Final Report

Table of Contents

Contents

1 Executive Summary

The Signaling System 7 (SS7) and Diameter are recognized as critical components 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 creating 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 has increased.

A new Working Group (WG) was created in June, 2016 to study this problem and develop recommendations for the FCC and industry to mitigate the risks. This CSRIC Working Group has assessed different attack vectors that have been documented and discussed in different settings including blogs, conferences, and standards, as well as industry and government forums. The Risk Assessment considered reported vulnerabilities (e.g., that have been discovered by industry or security researchers) and reports of exploitation. Industry is taking steps to coordinate and research the reported vulnerabilities and exploits, while being cognizant that the overwhelming amount of SS7 traffic is legitimate. As a result, carriers need to be measured as they implement steps and solutions in order to avoid collateral network impacts.

The WG membership consists of a wide range of participants including service companies, suppliers, technology experts, and the US Government. While the WG was only convened halfway through the CSRIC V establishment period, there has been extensive activity and ongoing analysis by the WG of available SS7 attack methodology information, briefings from Subject Matter Experts and the review of current and emerging industry best practices to address the evolving threats.

A Risk Assessment report[1] was completed prior to this Final report that captures background on the SS7 technology and Diameter protocols, potential targets, prominent attack methodologies and their potential impacts, as well as some key best practices and countermeasures to address the threats.

In this final report the WG provides specific recommendations for industry as well as recommended areas of further study for future FCC CSRIC efforts (See Section 5).

[1] CSRIC Legacy System Risk Reduction Working Group, Interim Report – Risk Assessment and Summary Public Report, December 2016.

2 Introduction

In the Technology Transitions Order of August 2015[2], the Commission notes that "communications networks are rapidly transitioning away from the historic provision of time-division multiplexed (TDM) services running on copper to new, all-Internet Protocol (IP) multimedia networks." The intermingling of legacy communications technologies with advanced communications technologies introduces new threat vectors and cyber risk. Recently, this issue has gained greater attention in light of the security threats to Signaling System 7 (SS7) and its IP-based version SIGTRAN, a signaling protocol supporting call setup, routing, exchange, and billing functions in communications networks by sending messages between fixed and mobile communications service providers. The scale of SS7, which is the de facto standard for carriers all over the world, means that every network subscriber could be vulnerable to these security risks, elevating concerns among stakeholders in the communications sector.

As part of a series of requests to the Communication Security, Reliability, Interoperability Council (CSRIC), the Commission asked the CSRIC V to examine vulnerabilities associated with the SS7 protocol and other key related communications protocols (e.g., Diameter). CSRIC V Working Group 10 was tasked to assess existing and potential threats and current defensive mechanisms and make recommendations to the FCC and industry on how to best address security challenges present in SS7 and other communications protocols used between communications networks, as well as their exposure and impact on the transition to next generation networks.

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) V Working Groups			
Working Group 1 **Evolving 911 Services** **Co-Chairs:** Susan Sherwood & Jeff Cohen **FCC Liaisons:** Tim May & John Healy	**Working Group 2** **Wireless Emergency Alert** **Co-Chairs:** Francisco Sánchez & Farrokh Khatibi **FCC Liaisons:** Chris Anderson, James Wiley & Gregory Cooke	**Working Group 3** **Emergency Alert System** **Co-Chairs:** Steven Johnson & Kelly Williams **FCC Liaison:** Gregory Cooke	**Working Group 4A** **Communications Infrastructure Resiliency** **Co-Chairs:** Kent Bressie & Catherine Creese **FCC Liaison:** Jerry Stanshine & Michael Connelly
Working Group 4B **Network Timing Single Source Risk Reduction** **Chair:** Jennifer Manner **FCC Liaison:** Emil Cherian	**Working Group 5** **Cybersecurity Information Sharing** **Co-Chairs:** Rod Rasmussen, Christopher Boyer, Brian Allen **FCC Liaisons:** Greg Intoccia & Vern Mosely	**Working Group 6** **Secure Hardware & Software** **Co-Chairs:** Brian Scarpelli & Joel Molinoff **FCC Liaisons:** Steven McKinnon & Emily Talaga	**Working Group 7** **Cybersecurity Workforce** **Co-Chairs:** Bill Boni & Drew Morin **FCC Liaison:** Erika Olsen

[2] Federal Communications Commission Technology Transition, GN Docket No. 13-5, August 7, 2015, https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-97A1.pdf

Working Group 8 **Priority Services** **Co-Chairs:** William Reidway & Thomas Anderson **FCC Liaisons:** Tim Perrier & Ken Burnley	**Working Group 9** **Wi-Fi Security** **Chair:** Brian Daly **FCC Liaisons:** Peter Shroyer & Kurian Jacob	**Working Group 10** **Legacy Systems Risk Reduction** **Co-Chairs:** John Kimmins & Danny McPherson **FCC Liaison:** Steven McKinnon

Table 1 - Working Group Structure

2.2 Working Group 10 Team Members

Working Group 10 consists of the members listed below.

Name	Company
Kathy Blasco	DHS
Kevin Briggs	DHS
Shawn Clark	Comcast
Martin Dolly	ATIS
Mark Easley	AT&T
Joshua Franklin	NIST
John Gallagher	Sprint
Mohammad Khaled	Nokia
John Kimmins – Co-Chair	iconectiv
Philip Linse	CenturyLink
Tim Lorello	Seculore Solutions LLC
John Marinho – Lead Editor	CTIA
Danny McPherson – Co-Chair	Verisign
Drew Morin	T-Mobile
Donald Morris-Jones	DHS
Dave Nolan	DHS
Nilesh Ranjan	T-Mobile
Travis Russell	Oracle Communications
Xiaomei Wang	Verizon Wireless
Kathy Whitbeck	Nsight

Table 2 - List of Working Group Members

Subject Matter Experts (SMEs), Acknowledgements:
Nokia Bell Labs, Silke Holtmanns
Security Research Labs, Karsten Nohl
Adaptive Mobile, Brian Collins

3 Overview of SS7 – Summary Assessment, Background

Signaling System 7 (SS7) is the global standard signaling protocol dating back over three decades and is used for telecommunications traffic for most of the world's public switched telephone network (PSTN) calls, including wireline, legacy 2G and 3G cellular networks. After years of rapid growth in mobile communications, the scale of SS7 approaches Internet proportions. Today, networks based on SS7 protocols manage the circuit-switched links among hundreds of carriers for wireline and wireless services and operators serving the majority of the 7.46 billion mobile subscribers worldwide as of June 2016.[3]

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 Short Message Service (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.

As discussed in the Risk Assessment Report, SS7 is applied to both wireline and wireless networks. The SS7 protocol consists of several layers. The lower layer, Message Transfer Part (MTP) is used for transporting SS7 messages over Time Division Multiplexing (TDM) circuits, while SIGTRAN (Signaling Transport) is used for transporting SS7 messages over IP. The ISDN User Part (ISUP) is used for setting up and tearing down telephone calls between switches. For database queries, the Services Connection Control Part (SCCP) and Transaction Capabilities Application Part (TCAP) are used. These are the basic protocols used in today's SS7 networks. Figure 1 illustrates the SS7 protocol stack when operating over TDM.

[3] 5G Americas, Global Mobile Subscribers and Market Shared b Technology, Ovum estimates global mobile subscribership of 7.46 billion as of June 2016, http://www.4gamericas.org/en/resources/statistics/statistics-global/

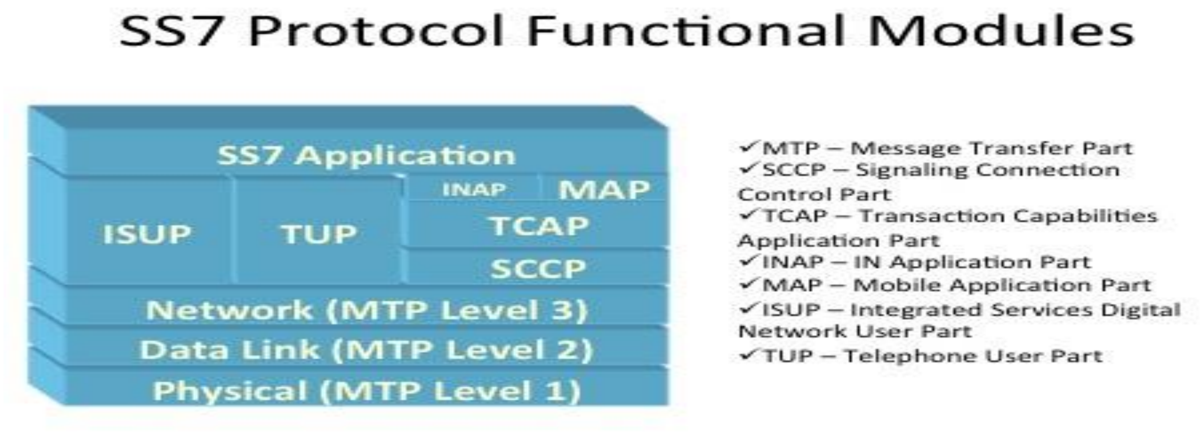

SS7 Protocol Functional Modules
SS7 Application
ISUP
TUP
INAP
MAP
TCAP
SCCP
Network (MTP Level 3)
Data Link (MTP Level 2)
Physical (MTP Level 1)
✓MTP – Message Transfer Part
✓SCCP – Signaling Connection Control Part
✓TCAP – Transaction Capabilities Application Part
✓INAP – IN Application Part
✓MAP – Mobile Application Part
✓ISUP – Integrated Services Digital Network User Part
✓TUP – Telephone User Part

Figure 1: SS7 Protocol Stack over TDM

When cellular networks were first developed, the ability for switches to access databases became a critical function for authenticating subscribers and determining the permissions a subscriber would have in the network. A new protocol was developed for supporting wireless services, called the Mobile Application Part (MAP).

3.1 Application to Wireline Networks

Wireline (fixed) networks depend on SS7 primarily for the connection of voice calls. However, numbering services such as 800, 411, 911, and Number Portability rely heavily on the SS7 network for routing such calls to their proper destinations. There are many other services provided by wireline service providers that are not possible without the SS7 network. Calling Name Display, E.164 Number Mapping (ENUM), and other Intelligent Network (IN) based services are also commonplace.

3.1.1 Generic Architectural View

A wireline telephony network is significantly simpler than wireless counterparts, especially where VoIP is not supported. Figure 2 illustrates a simple wireline SS7 network. The Service Switching Point (SSP) is the voice switch. Note that the Signal Transfer Point (STP) can be deployed as a Local STP (LSTP) or Regional STP (RSTP) depending on the network topology.

The various databases used in the network to support services are referred to as Service Control Points (SCPs) and provide further instructions to the switches as to how to handle calls. This includes routing of calls to a different destination than what was originally intended (e.g., call forwarding). This network architecture is referred to as the Intelligent Network (IN) in international standards, and the Advanced Intelligent Network (AIN) in North America.

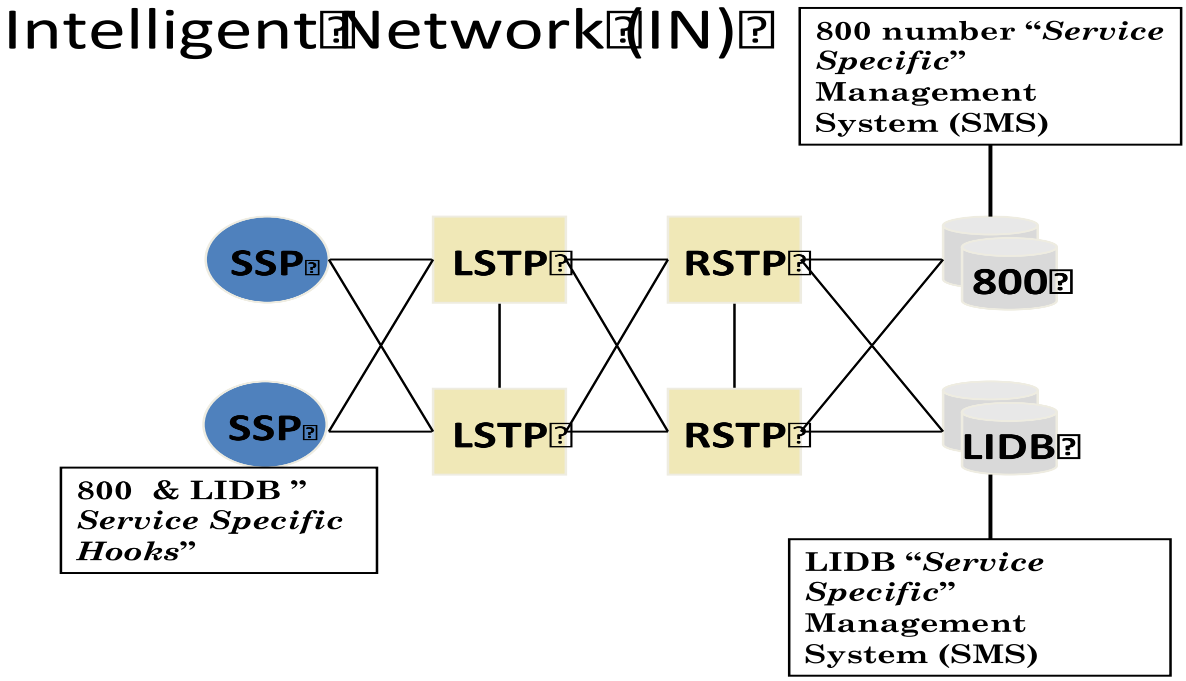

Intelligent Network (IN)
800 number "*Service Specific*" Management System (SMS)
SSP
SSP
LSTP
LSTP
RSTP
RSTP
800
LIDB
800 & LIDB " *Service Specific Hooks*"
LIDB "*Service Specific*" Management System (SMS)

Figure 2: Intelligent Network (IN) - A Fixed Wireline SS7 Network

3.1.2 Relevant Standards & Protocols

Wireline networks do not use the Mobile Application Part (MAP) of SS7 as this protocol was developed solely for the support of various wireless services. However, they do use SS7 and the IN protocol for transactional sessions.

3.1.3 Security Practices

Over the years, the Alliance for Telecommunications Industry Solutions (ATIS) standards forum has developed security requirements for protecting the control and management planes for the public telecommunications network. As with wireless networks, interconnect policies should be established for every network interconnect. While researchers have not yet demonstrated exploits in wireline networks, or provided empirical evidence thereof, it should be assumed that these networks are vulnerable like their wireless counterparts. For those networks that have not implemented protections, access to the control plane of a participant SS7 network may result in an array of attack vectors as discussed in the Risk Assessment.

3.1.4 Transition to New Technology

Wireline networks are also moving to IP-based architecture, using the Session Initiation Protocol (SIP) protocol to replace ISUP for the connection of calls. Diameter would then be used for all 'transaction related' traffic in the network by providing charging records and replacing the IN component (Diameter was originally developed to replace the older Remote Authentication Dial-In Service (RADIUS) protocol in charging networks). Many operators have already made this transition to Voice over Internet Protocol (VoIP) architectures, which brings an additional set of attack vectors and vulnerabilities into considerations, albeit outside the scope of this report. Figure 4 illustrates the evolution of signaling protocols.

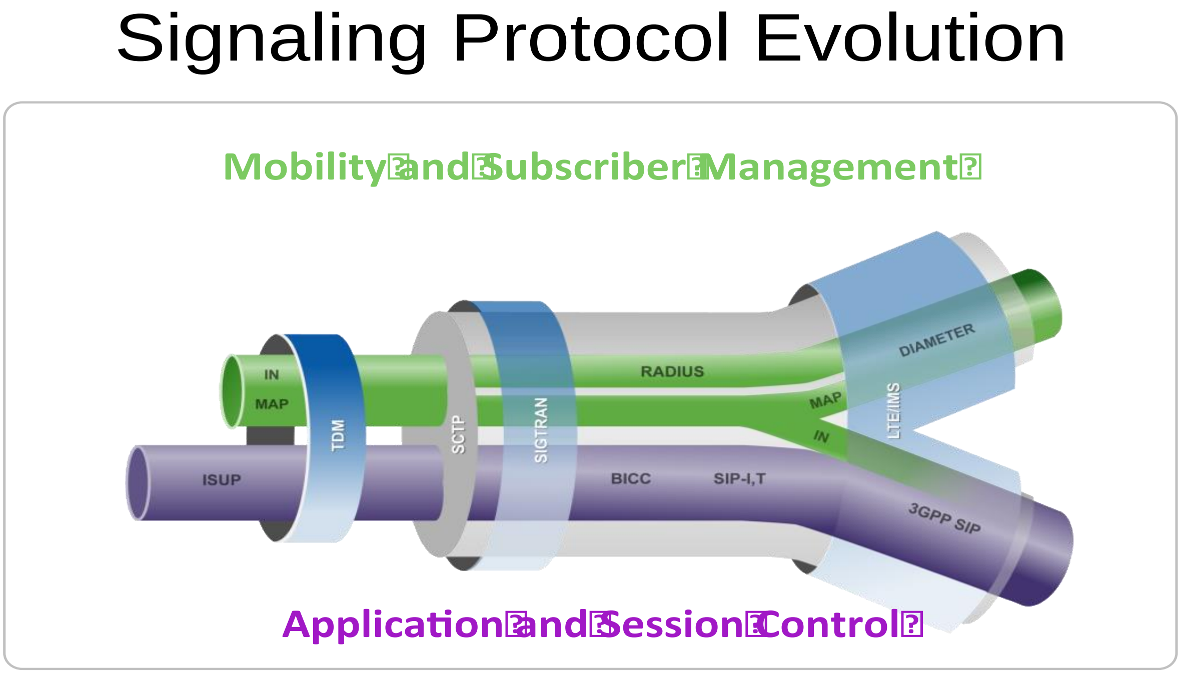

Signaling Protocol Evolution
Mobility and Subscriber Management
IN
MAP
TDM
ISUP
SCTP
SIGTRAN
RADIUS
BICC
SIP-I,T
MAP
IN
LTE/IMS
DIAMETER
3GPP SIP
Application and Session Control

Figure 4: Evolution of Signaling Protocols (Illustration courtesy of Oracle Communications)

3.2 Application to Mobile Network

3.2.1 Generic Architectural Overview

SS7 and the GSM MAP protocols are used as an interexchange (IPX) mechanism to coordinate global roaming between mobile network operators. 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 often maintain direct connections with “peers” while small operators use wholesale connectivity services. Also new players that come from the classical Internet business and now offer connectivity service often just rent the connectivity service from a connectivity provider and do not make all roaming contracts themselves e.g. Apple SIM. An IPX provider may aggregate access with other operators that could traverse several IPX providers from source to destination.

3.2.2 Relevant Standards & Protocols

The primary protocol used by the research community to demonstrate potential vulnerabilities discussed in this report are part of the SS7 protocol suite. Specifically, the MAP component has been used to effectuate these exploits: however, these vulnerabilities are not limited to the SS7 protocol suite. As previously discussed, the fact that access to networks is possible through any number of complicit or compromised operators means that all telecommunications protocols used to interconnect networks are potentially at risk. This includes SIP interconnects, as well as Diameter. The Intelligent Network (IN) and Advanced Intelligent Network (AIN) protocols, which are also part of the SS7 suite, should be considered for future assessment.

3.2.3 Security Practices

Key Standardization Forum for Network Security

The 3rd Generation Partnership Project (3GPP) and the International Telecommunication Union (ITU) defines global telecommunications standards while more national organizations (e.g., ATIS and American National Standards Institute [ANSI]) provide implementations of these standards for national networks. The 3GPP covers cellular telecommunications network technologies including radio access, core network and service capabilities. 3GPP has been studying the security of next generation systems to support existing and new multi-media services. The new network architectures need to be more flexible, scalable, secure and extensible to support different traffic characteristics and a variety of users and service requirements. The work is focusing on securing the user, management and control planes to protect the interfaces, network elements and data flows.

Key Industry Forum for Signaling Interconnection Security

The GSMA organization is a global mobile industry trade association. Among its many industry functions the GSMA coordinates roaming across the globe. It facilitates the needed information exchange to allow operators to connect to each other. It offers for example, legal documents related to roaming, protocol usage information, certification, technical operator network descriptions repository and many other enablers for roaming. The GSMA has about 800 operator members. The GSMA has many focused subgroups, in particular it has a Packet Group that deals with protocol implementation and a Fraud and Security Group[4], which has a subgroup focused on interconnection security.

Since the global mobile network in the past was a closed network, there was little need for security experts to secure the network interconnection. This resulted in the fact that today there are only a handful of interconnection security experts in the world that focus on protection of networks on the interconnect interface between operators. Interconnection security requires a combination of expert security and telecommunication protocol knowledge. The largest group in the world with an intersection of such experts is found in the GSMA security groups.

GSMA has produced several standard guideline documents designed to help mobile operators detect and protect their networks from malicious SS7 activity. Several of the key documents are identified and referenced in the Risk Assessment Report. It is worth noting that these documents are only available to GSMA members at this time.[5]

[4] GSMA Fraud and Security Group, http://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group

[5] Questions about these security documents can be directed to Mr. James Moran, jmoran@gsma.com.

4 Summary Conclusions from Risk Assessment Report

The Working Group conducted a risk assessment of the risks to carriers, individual subscribers and critical infrastructure services from exploiting the SS7 signaling infrastructures, and possible implications to the Diameter protocol. There is reported evidence of attacks being launched against U.S. carriers by exploiting the available signaling functionality and trusted interconnection that the U.S. telecommunications infrastructure is built on. The Risk Assessment report is a view of the current risk.

Based on feedback and review with industry subject matter experts the need was identified to establish a picture of what is going on in the U.S. that would correspond to monitoring networks for ”unauthorized commands”, based on GSMA FS.11 and corresponding network statistics.

The major telecommunications carriers and suppliers have recognized the current risks and have been implementing various countermeasures to analyze and block specific attacks or suspicious traffic. As noted in this report and the risk assessment, because the overwhelming amount of SS7 traffic is legitimate, carriers need to be measured as they implement solutions in order to avoid collateral network impacts. We have identified recommendations in the next section from Working Group members and SMEs that are actively working with U.S. and international telecom infrastructures and in standards forums. The following are preliminary views from the Risk Assessment report.

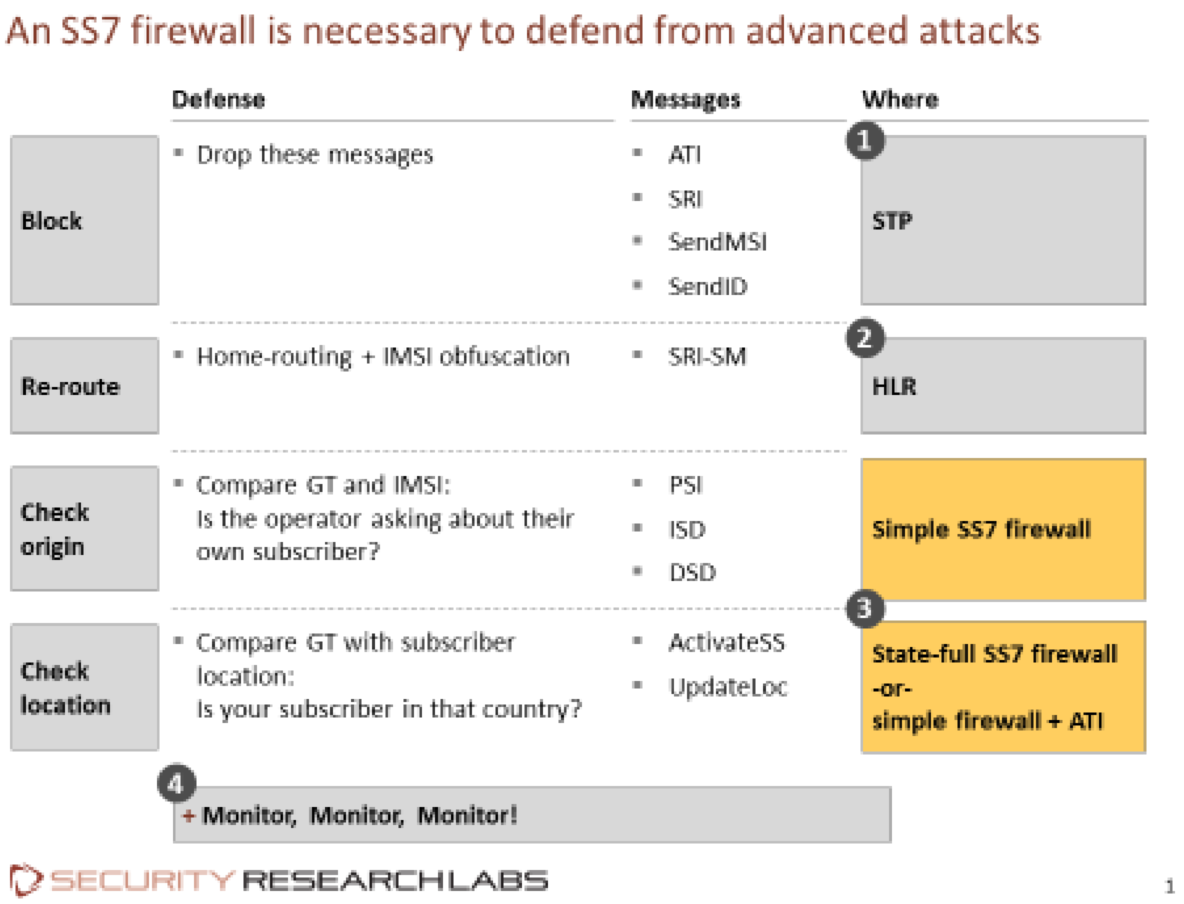
4.1 Interconnection Monitoring and Filtering

The experts recommended that industry carefully evaluate ”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.

GSMA SS7 firewall rules, FS.11, IR.82 (as far as applicable), are the most relevant documents. The experts identified the most likely filtering point as the STPs or in proximity to the STP. The Home Location Register (HLR) is also a ”rich” target and needs similar protections. The MSC/xGSN/VLR are identifed as likely ”at-risk nodes”. In addition, network elements need to be audited to ensure subscriber profiles have not been modified.

The experts further observed that depending on the existing node capabilities, filtering may be doable with ”configuration & tuning” within the network itself. It was further recommended by the experts that the vast majority of the current SS7 threats that address three (3) attack scenarios (Track, Intercept, Fraud), rely on ten (10) SS7 messages that can be rejected using four (4) defense measures: STP, HLR, SS7 firewall functionality (if needed), and monitoring and filtering. Nevertheless, it should be noted, when attackers no longer have access to the desired information they will likely attempt to adapt and may thereby target other SS7 message scenarios.

The scenarios and messages are outlined below in Figure 5. The depicted functional and architectural configurations are examples of possible control points within the service provider network.



An SS7 firewall is necessary to defend from advanced attacks

	Defense	Messages	Where
Block	Drop these messages	ATI SRI SendMSI SendID	1 **STP**
Re-route	Home-routing + IMSI obfuscation	SRI-SM	2 **HLR**
Check origin	Compare GT and IMSI: Is the operator asking about their own subscriber?	PSI ISD DSD	**Simple SS7 firewall**
Check location	Compare GT with subscriber location: Is your subscriber in that country?	ActivateSS UpdateLoc	3 **State-full SS7 firewall** **-or-** **simple firewall + ATI**

4 **+ Monitor, Monitor, Monitor!**

SECURITY RESEARCHLABS

1

Figure 5: SS7 Firewalls and Advanced Attacks (Courtesy: Security Research Labs)

4.2 IPSec

The use of IPSec for the GSM MAP protocol has been considered. Upgrading of SS7 / MAP with IPSec would require a very significant systemic peer-wise effort and most operators are not bound to the FCC or US based practices. Therefore it is considered at this time that IPSec for MAP at interconnection points would have very low impact and very limited benefits, noncommensurate with the complexity implications and requisite investment.

4.3 Diameter & 5G Networks

As described in the Risk Assessment, the evolution towards Diameter being used in the underlying infrastructure creates potential risks that need to be factored into the security approach. Diameter has certain inherent capabilities that make it more difficult to attack. While the Diameter protocol supports the same functions as SS7 (and many more), Diameter could introduce new vulnerabilities that need to be considered. The two protocols work very differently as do their network substrates and systemic effects, and this should be taken into consideration when assessing Diameter. That said, the research community has given demonstrations using the Diameter protocol to execute similar exploits seen on the SS7 network. In addition, researchers have also identified other potential, theoretical exploits on Diameter. Given that service operators currently do not use Diameter for interconnection, there is no empirical evidence that Diameter is being exploited. However, as in SS7, attackers will likely attempt to exploit any potential access susceptibility. The Diameter Edge Agent (DEA) is responsible for protecting the network from unauthorized access and should have the ability to filter all Diameter commands, their Attribute Value Pairs (AVPs), and the origin and destination of the command (host/realm). In addition, the DEA should be capable of examining the application-ID portion of the message to make sure that the Diameter command being sent is allowed to be sent over the received interface (i.e., S6a), in accordance with 3GPP standards. Other potential risk areas beside upcoming Diameter are ANSI MAP (3GPP2 version of MAP), SCCP based Denial-of-Service (DoS) attacks, MAPv1 or Global Title Point code (GTP) data attacks.

The GSMA FASG has developed the Diameter Security Guidelines (FS.19) to address the Diameter vulnerabilities, and European Telecommunications Standards Institute (ETSI) Cybersecurity WG is addressing Diameter as well as 5G security. Diameter is a critical component of 5G networks, and therefore close attention needs to be paid to the Diameter protocol. 5G networks will use diameter as one of their main protocols for communication. For coverage reasons, the device may contain a foreign SIM of the partner-operator to ensure the coverage (i.e. device tries first to connect to the roaming partner and then if not possible attaches to strongest network). All those Internet of Things (IoT) devices with “foreign” SIM will use the roaming interface, i.e. even static devices like meters, fridges etc. may roam. IoT devices are sometimes receiving commands via SMS (even industrial systems).

Network Function Virtualization (NFV) will also play an important role in 5G networks as operators begin moving critical infrastructure and functions into the data center. Further study needs to be considered for both Diameter and 5G security as these systems and networks are deployed.

4.4 Protection against hacking of network nodes (Hardening)

The 3GPP has specified security requirements for the architecture, network elements and interfaces to support mobility management. These requirements reduce the attack surface by addressing key areas including service availability, system integrity, data security and access and core network protections.

4.5 Signaling Aggregators

Aggregators provide wholesale SS7 interconnection capabilities for all types and size of service providers. Acting as a hub, they have a wider view of signaling traffic originating from domestic and international entities and terminating in the U.S. telecommunications network. This view enables more robust monitoring and filtering across the traffic. The major aggregators could then respond, similar to individual service providers in identifying malicious and suspicious traffic using basic message filtering and data analytics applied to multiple message streams. Some attack vectors like the identity of a malicious service provider endpoint may still be a problem. However, extending the security controls at different interconnection points reduces the risk.

4.6 Information Sharing

There has been much discussion around information sharing in the industry. The GSMA has been exploring the possibility of operators sharing telecommunications focused security breaches, and have established a template for the reporting of incidents. The template has actually been put to use, and at least one operator recently submitted a security breach (SMS intercept) to the GSMA FASG.

There already exists a framework for the sharing of incidents within the telecommunications industry. The GSMA Fraud group actively shares fraud alerts with its members, and partners with the Communications Fraud Control Association (CFCA) in information sharing. Additionally, existing threat information sharing resources are outlined in the CSRIC Working Group 5 report as it relates to Department of Homeland Security (DHS) National Coordinating Center for Communications (NCC), the Communications Information Sharing and Analysis Center (ISAC) and collaboration with law enforcement. Also, with the passage of the CISA (Cybersecurity Information Sharing Act) in December 2015, the industry has undertaken to Pilot automated information sharing use-cases specific to the telecommunications sector, inclusive of SS7 scenarios and connection with the DHS Automated Indicator Sharing (AIS) Portal.

Some form of telecommunications focused information sharing may assist operators in developing business cases for the investment in security solutions. Without this ‘evidence’ of intentional signaling abuse, malicious targeting of subscribers and active cyber security breaches, it becomes impossible for security professionals to justify investments in security solutions, and threats are viewed as ‘theoretical and academic.’ The question becomes who will be responsible for the dissemination of these reports without risk of punitive actions against the operator. A third party may be able to assist in managing this reporting and for ensuring the reporting operators are not penalized. CTIA’s ongoing efforts on cybersecurity information sharing within the communications sector could be a model for such third-party efforts.

4.7 Circles of Trust

As discussed in Section 9 of the Risk Assessment report, the 3GPP is studying the concept of trust groups among telecommunications carriers. This could include, extending the authentication framework across user devices, 3GPP and non-3GPP access and core networks and third party services. Forming trust groups across as many upstream and downstream interfaces as possible could be very beneficial, but it is unrealistic to expect global trust and adoption across different types of operators, exchange operators and third party service providers.

While the interconnection model could benefit from a global trust group model, such an approach would need to begin with small steps that can be adapted, as circumstances change, and eventually expanded.

For example, each network will have to deal with messages from partners with which it has the same level of trust and those with different levels of trust. If a network has different levels inside its own network (e.g. global operator acting across different political areas) then the nodes in this network need to be assigned to one or another trust level. This is particularly important if a node or whole countries might become untrustworthy and thus an important task. In determining levels of trust, companies will need to ask a number of questions: How well a network is protected against attacks? Are the nodes hardened? Have regular risk assessments been performed? To whom is the access rented out (wholesale business, MVNO etc.) and is their behavior monitored and are those tenants following the rules? This assessment can rely upon hardening guidelines (e.g. 3GPP TS 33.116 and TS 33.117), monitoring requirements for tenants (e.g. GSMA FS.11, FS.07. FS.19), and legal rules. It may even include trusted hardware for localization purposes and rules for NFV management or employee training against phishing and bribing. The first step is to define what does trust mean and second what area is covered, i.e. U.S. or U.S. + selected partners.

When two trusted nodes communicate with each other, they need to use a secure direct communication, that includes authentication, confidentially and integrity e.g. IPSec. For this a Public Key Infrastructure is needed. A globally trusted PKI may not be feasible. Therefore, as a trusted starting point, a regional trusted PKI may be sensible e.g. potentially run by some third party. The same entity could also provide a revocation blacklist, which is important to identify compromised nodes. All entities in the trust group adhering to the trust level principals could obtain the needed cryptographic material.

A communication is only trustworthy if the whole communication chain is trustworthy. As previously discussed, a message may traverse potentially untrusted nodes and becomes untrustworthy. This could result in there being “two classes” of messages. It is important to note that an interconnection or a backbone connectivity provider may actually be in several trust groups and therefore have several classes of traffic e.g. untrusted, “RegionA-trusted”, “RegionB-trusted”. It needs to be observed that those messages may need to be routed through different security tunnels, as their trust is based on the credentials used for the tunnels.

4.8 Security Assessment of Signaling Infrastructure

It is critical that the signaling infrastructure maintains robust security for the signaling protocol, network architecture, and supporting operations infrastructure. The WG recommends that service providers periodically assess the security of their SS7 signaling infrastructure as appropriate to identify any risks and then remediate the controls framework. This should either be conducted by internal resources or an independent third party that has the necessary skillsets. The security risk assessment may address different aspects, such as:

- Cover the SS7 protocol suite across all of the domestic and international interconnection points
- Assess the people, processes and technology focused on security
- Identify any internal or external weaknesses
- Cover both the control and management planes in terms of security configurations
- Fuzz testing to evaluate the robustness of the protocol filtering and data analytics
- Assess the supporting operations processes monitoring interconnection points and responding to malicious and suspicious traffic
- Examine the lifecycle management of the supplier products in terms of patches, updates and new security functionality

4.9 U.S. Critical Infrastructure Protection

Critical infrastructure (CI) includes different types of systems that provide goods and services that support essential societal and government operations. As described in the Risk Assessment critical infrastructures include the following sectors:

- Industrial Control Systems (ICS) for sensitive manufacturing and processing operations (e.g., chemical plants, refineries, etc.).
- Banking and Finance
- Energy
- Water and Wastewater
- Emergency Services
- Communications
- Transportation
- Federal Government

CI Sectors may face different types of SS7 and possibly Diameter attacks including location tracking, call interception, fraud and denial-of-service. Due to the importance of critical infrastructures for delivery of essential societal functions, it is imperative that SS7 and Diameter vulnerabilities be addressed effectively to ensure that U.S. infrastructures remain resilient and avoid cascading failures. Resilient communications requires on-going monitoring, filtering and threat information sharing.

4.10 Subscriber Encryption Support

The SS7 exploits described in the Risk Assessment conducted for CSRIC V by Working Group 10 and released in December 2016 are primarily effective because of their limited scope. The use of SS7 for mass eavesdropping on calls or mass global tracking is easily detected in even the least sophisticated network. These threats are designed for specific end user targeting and as with any good defense in depth strategy, a layered approach can provide the best protection. A consumer may be able to employ methods to protect the content of messages and voice communications by using end to end encryption.

When making a call using a landline or mobile phone, the call is not encrypted end-to-end. Most mobile phones do use some form of encryption over the air interface between the mobile device and the towers. However, the call is delivered “in the clear” as it traverses the network and is vulnerable to interception using the techniques that have been described earlier in the Risk Assessment Report. End to end encryption means that the data is encrypted at the source device with a user specific key and delivered to the end device where it is decrypted using the same key. In practice, the complexity of key management and encryption/decryption is handled by applications deployed at the end devices. There are a number of such applications available on the market today, but the consumer needs to be wary that they are using an application that truly encrypts end to end.

There are a number of sources that can be used as research references that provide further information on encryption methods and the ability to support voice, messaging and other data types.[6] For voice calls, there are a number of well-known services that offer end-to-end encrypted VoIP capabilities and also traditional voice encryption. A few example applications include:

- WhatsApp (https://www.whatsapp.com/)
- Signal (http://whispersystems.org/)
- Jitsi (https://jitisi.org/)
- Silent Phone (https://www.silentcircle.com/)
- Zphone (http://www.zfone.com/)

However, most popular VoIP provides, such as Skype and Google Hangouts, offer transport encryption. Many of the apps are open source and free to use.

End to end encryption popularity has grown overseas, initially by users in China, Iran and the Middle East, where users may be concerned about government surveillance. These apps have continued to move more into the mainstream as awareness of privacy concerns by end users grows. This may be one way for a consumer to protect the privacy of the content of communications. Other more sophisticated tools exist that can be employed to protect this metadata, such as using Tor over a secure IP connection.

For a VIP or key government official, the use of commercial applications that enable end-to-end encryption provides another layer in the defense against potential information compromise by SS7 enabled eavesdropping. The ease of use in these applications continues to improve and the quality of service has improved as well. These are commercial grade encryption and are not approved for transmission of any government security classified information. They are, however, a convenient tool to protect sensitive but unclassified conversations for potential targets of eavesdropping.

5 Final CSRIC Working Group Recommendations

5.1 Recommendations for the FCC

5.1.1 **Future CSRIC efforts**

The CSRIC recommends that the FCC consider future CSRIC efforts to address continued collaboration with industry relative to signaling network security, reliability and interoperability. Areas for possible future CSRIC consideration include:

- Diameter and 5G networks,
- Circles-of-Trust, and
- Non-GSMA signaling systems, such as: AIN, SIP, ANSI-MAP.

[6] https://pressfreedomfoundation.org/encryption-works provides detailed instructions on using end-to-end encryption to protect instant messages and email

5.2 Recommendations for Industry

5.2.1 Signaling Security Monitoring and Filtering

The CSRIC Recommends that industry continue to implement signaling interconnection monitoring and filtering as outlined in Section 4 and in the Risk Assessment report.

5.2.2 GSMA Security Best Practices and Guidelines

The CSRIC recommends and endorses the GSMA security best practices and guidelines to secure signaling interconnection as described in Section 4 for SS7 and Diameter, and recommends continued advancements in information sharing of threat intelligence to continuously adapt monitoring, filtering and data analytics.

5.2.3 Aggregators

The CSRIC recommends that industry engage signaling aggregators in their efforts to address overall security, monitoring and filtering as outlined in Section 4 and in the Risk Assessment report.

5.2.4 Threat Information Sharing

The CSRIC recommends that the industry continue to leverage and expand the existing threat information sharing resources as outlined in the CSRIC Working Group 5 report as it relates to the DHS National Coordinating Center for Communications (NCC), the Communications ISAC and collaboration with law enforcement.

5.2.5 Automated Information Sharing Pilot

The CSRIC recommends that industry continue the efforts regarding automated threat information sharing through the CTIA sponsored information sharing Pilot to advance telecommunications specific use-cases, and in particular those that relate to SS7, Diameter and in the future 5G.

5.2.6 Emerging Diameter & 5G Networks

The CSRIC recommends that the industry continue to participate in industry and standards forums and adopt the GSMA recommended controls to address emerging Diameter security risks as part of their overall 5G security approach.

5.2.7 Circles of Trust

The CSRIC recommends that industry continue to explore further work as it relates to the possible benefits of Circles-of-Trust, perhaps in future CSRIC efforts.

5.2.8 Ongoing Security Assessment of Signaling Infrastructure

The CSRIC recommends that industry continue its efforts of ongoing security assessment of the network signaling infrastructure to detect and mitigate possible threat vectors, consistent with best practices and standards.

5.2.9 Subscriber Encryption Support

The CSRIC recommends that industry encourage the use of available 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.