Rialtas na hÉireann
Government of Ireland

Electronic Communications Security Measures

006 – Signalling Plane Security v1.0

2021

Prepared by Department of the
Environment, Climate & Communications
gov.ie/decc

Table of Contents

1 Foreword

The Electronic Communications Security Measures (ECSMs) have been produced by the Electronic Communications Security Measures working group convened by the Irish National Cyber Security Centre (NCSC), which forms part of the Department of the Environment, Climate and Communications (DECC); and with the support of the Commission for Communications Regulation (ComReg). Industry participation in the WG has involved network operators, including the Mobile Network Operators (MNO) which have been awarded 5G licences, and selected fixed line operators.

This ECSM is part of a series of documents listed below:

Title	Subject
ECSM 001	General
ECSM 002	Risk Management
ECSM 003	Physical and Environmental Security
ECSM 004	Training, Awareness and Personnel Security
ECSM 005	Network Management & Access Control
ECSM 006	Signalling Plane Security
ECSM 007	Virtualisation Security
ECSM 008	Network, Monitoring and Incident Response
ECSM 009	Supply Chain Security
ECSM 010	Diversity, Resilience & Continuity
…	…

2 Introduction

Ireland's modern digitally connected society and economy is highly dependent on reliable and secure electronic communications networks and services (ECN and ECS respectively). They form the backbone of much of Ireland's critical national infrastructure providing connectivity to the essential services upon which citizens rely, such as healthcare providers, energy providers, financial institutions, emergency services and public administration. It is of paramount importance that these vital networks and services are protected from the full range of threats with an appropriate level of technical and organisation security measures.

The ECSM Working Group Convened on the 02nd, 3rd and 04th of June 2020 to discuss matters concerning secure network design, deployment, and operation. The group heard from experts in the field of signalling security and held focussed discussions on the risks, challenges and best practices associated with signalling security as it pertains to telecommunications networks. ECSM 006 – Signalling Plane Security has been developed by the NCSC informed by those meetings.

3 Scope

This ECSM is applicable to all undertakings providing public Electronic Communications Networks and Electronic Communications Services who process, transmit or receive signalling traffic[1], or use Border Gateway Protocol as part of their network deployment.

The legislative basis for the ECSMs is set out in ECSM 001- General

4 References

Document	Title
3GPP 23840-710	Study into routeing of MT-SMs via the HPLMN
3GPP TS 29.573	Public Land Mobile Network (PLMN) Interconnection; Stage 3. 2019
3GPP TS 33.117	Catalogue of general security assurance requirements
ENISA	7 Steps to shore up the Border Gateway Protocol (BGP): 2019

[1] SS7, MAP/CAP, SIGTRAN, Diameter, GTP, SIP, 5GC Signalling etc.

ENISA	Signalling Security in Telecom SS7/Diameter/5G: 2018
GSMA FS.07	SS7 and SIGTRAN Network Security
GSMA FS.11	Signalling Security in Telecoms SS7/Diameter/5G
GSMA FS.19	Diameter Interconnect Security
GSMA FS.20	GTP Security
GSMA FS.21	Interconnect Signalling Security Recommendations
GSMA IR.82	SS7 Security Network Implementation Guidelines
GSMA IR.88	LTE and EPC Roaming Guidelines
MANRS	Actions for Network Operators
UK NCSC	Responsible Use of the Border Gateway Protocol

5 Definitions, Symbols and Abbreviations

5.1 Definitions

Term	Meaning
Border Gateway protocol	A standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet.
Diameter	An authentication, authorization, and accounting protocol for computer networks. It evolved from the earlier RADIUS protocol. It belongs to the application layer protocols in the internet protocol suite
EU 5G Security Toolbox	Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures' document published jointly by member states on 31st of January 2020

EU Risk Assessment	EU coordinated risk assessment of the cybersecurity of 5G networks report published jointly by the EU Member States on 09th October 2019
Fuzz Testing	Negative testing technique for automatically generating and injecting into a target system anomalous invalid message sequences, broken data structures or invalid data, in order to find the inputs that result in failures or degradation of service
National Risk Assessment	Risk assessment carried out by the National Cyber Security Centre and forwarded to the European Commission on 15 July 2019.
Operator	An undertaking providing or authorised to provide a public electronic communications network or an associated facility
Resilience	The ability of a network to continue to operate, possibly at reduces capability, while under attack or in the case of network element failure, and to rapidly recover full operational capabilities for essential functions after the event.
Signalling System No. 7	A set of telephony common channel signalling protocols developed by the ITU-T and standardised in the ITU-T Q .700 Series Recommendations.
SIGTRAN	A signalling protocol that supports the same application and call management paradigms as SS7 using Internet Protocol (IP) .
Undertaking	A person engaged or intending to engage in the provision of electronic communications networks or services or associated facilities.

5.2 Symbols

Nil

36 5.3 Abbreviations

Term	Meaning
2FA	Two Factor Authentication
BGP	Border Gateway Protocol
CAMEL	Customised Applications for Mobile networks Enhanced Logic
ComReg	The Commission for Communications Regulation
DECC	The Department of Environment, Climate and Communications
DMZ	De-Militarised Zone
ECSM	Electronic Communications Security Measure
EECC	European Electronics Communications Code.
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
GSM	Global Systems Mobile
GSMA	GSM Association
GT	Global Title
HLR	Home Location Register
IMSI	International Mobile Subscriber Identity
JSON	Java Script Object Notation
LTE	Long Term Evolution
MAP	Mobile Application Part

MISP	Malware Information Sharing Platform
MNO	Mobile Network Operator
MSC	Message Switching Centre
MSP	Managed Service provider
NAT	Network Address Translation
NCSC	National Cyber Security Centre
PLMN	Public Land Mobile Network
SIM	Subscriber Identification Module
SMS	Short Messaging Service
SMSC	Short Message Service Centre
SS7	Signalling System No. 7
TMSI	Temporary Mobile Subscriber Identity
VLR	Visitor Location Register

37

38

6 Overview of Risk

Earlier generations of networks rely on legacy protocols (such as SS7 and SIGTRAN) designed decades ago, which do not fully consider modern security implications. The protocols were designed with a trust-based model which had not envisaged the scale of modern interconnected electronic communications systems and networks where non-traditional operators have access to the SS7 network. However, these legacy protocols are currently used to assure the interconnection between operators.

The current LTE network uses a slightly improved signalling protocol called Diameter however it also contains a number of vulnerabilities[2]. According to ENISA's March 2018 paper entitled Signalling Security in Telecommunications - *"While work is being done in addressing SS7 and Diameter attacks, only a small portion of the protocols has been studied. It is expected that new vulnerabilities shall be discovered."*

The current approach to signalling often does not reflect that fact that external networks cannot be considered trustworthy. A possible scenario using the SS7 protocol is given below:

- External, untrusted signalling is received by an edge or gateway signalling router (a Signalling Transfer Point (STP), in the case of SS7).
- The signalling router processes part of the message to assess where the signalling message should be sent. In some cases, this device may filter out some basic invalid message types (e.g. GSMA Cat 1,).
- Further signalling routers may then continue to route the message until the signalling message is received by critical core network nodes (e.g. Home Location Register (HLR)/Mobile Switching Centre (MSC))
- The critical core network nodes process the full message and based on the content of the message responds accordingly.

Consequently, the first network equipment to fully parse the message is a critical core node. If there is a vulnerability in the critical core node, an external attacker can directly exploit it. If there is an issue with parsing the message, an external attacker can directly disrupt the critical core. In effect, common approaches to signalling place most of the core at the logical edge of the network, leaving it highly vulnerable. Furthermore, signalling networks have

[2] https://positive-tech.com/research/diameter-2018/

been shown to allow the leaking of subscriber and network data, sometimes in support of criminal activity.

The risks from signalling plane insecurity are well known in the industry and vulnerabilities have resulted in incidents such as network core failures, persons' locations being tracked by criminals or hostile state actors and financial fraud where banks use SMS for 2FA. ENISA conducted a survey in 2018 and found European operators face a number of common attacks due to vulnerabilities in the signalling plane ranging from disruptive attacks to leakage of sensitive user data such as location data.

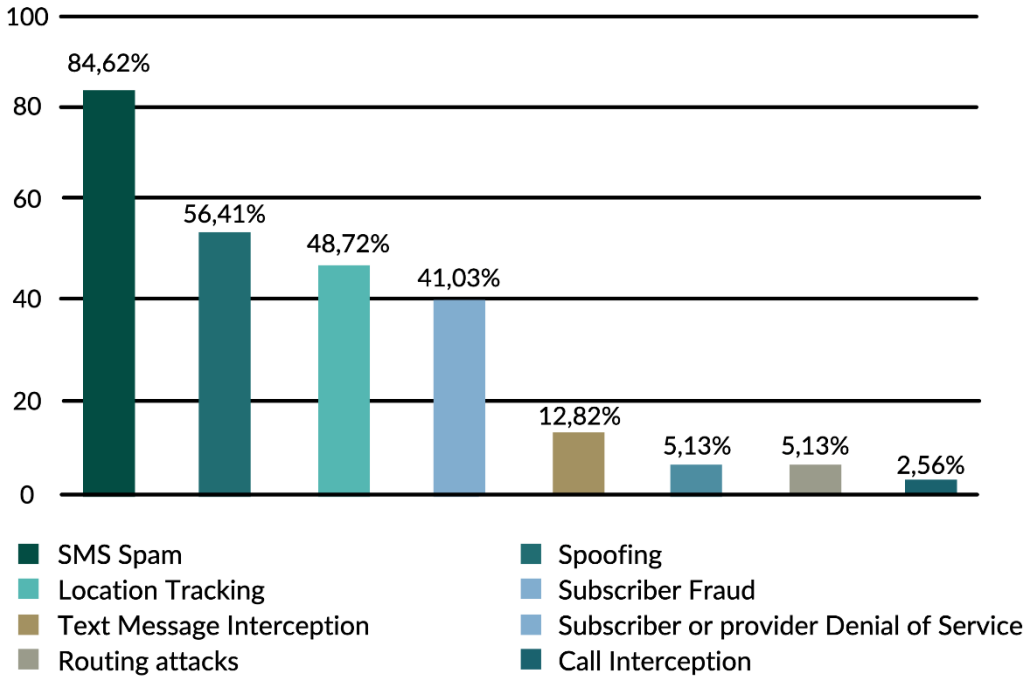

Figure 1 – ENISA survey results outlining common signalling attacks on EU operators

Similarly, the internet protocol of Border Gateway Protocol (BGP) used to route data between service providers, contains a number of legacy vulnerabilities due to a lack of authenticity or integrity checking mechanisms. This allows the protocol to be abused for attacks ranging from small scale financial crime[3] to large scale espionage or disruption[4].

It is acknowledged that the majority of attacks described above originate from outside the State and that the main focus of this ECSM should thus be on international traffic.

[3] https://www.theverge.com/2018/4/24/17275982/myetherwallet-hack-bgp-dns-hijacking-stolen-ethereum

[4] https://www.wired.com/story/google-internet-traffic-china-russia-rerouted/

The intent of the security measures outlined in this ECSM are:

- To increase the network's resilience to disruptive attacks from external signalling networks.
- To inhibit the leaking of subscriber or network data over external signalling networks.
- To monitor and react to BGP attacks to prevent traffic from being maliciously rerouted.

7 Security Measures

The operator should implement the Signalling Plane Security Measures in a manner that is customised to be appropriate and proportionate to the organisation.

Measure	Description
Signalling Plane Security	
SP.01:	The operator shall understand which interfaces and equipment process inbound and outbound signalling, how they could be impacted by malicious signalling and what user or network data could be compromised as a result.
SP.02:	The operator shall not assume trust in external signalling and should only allow legitimate signalling traffic into and out of their networks, wherever technically feasible.
SP.03:	The operator shall monitor and analyse inbound and outbound signalling traffic for malicious or malformed signalling messages.
SP.04	The operator shall filter/block malicious or malformed signalling messages.
SP.05:	The operator shall design their networks to ensure resilience to denial-of-service signalling attacks.
SP.06:	The operator shall design their networks to inhibit the leakage of network or user data, such as through obfuscation techniques / topology hiding.
SP.07:	Signalling nodes shall be hardened. Unused interfaces shall be closed, and only authorised interfaces shall be used to establish communications links with the network elements.
SP.08:	The operator shall conduct security testing of their signalling network to ensure it behaves as expected and is sufficiently robust and secure.
BGP Security	
SP.09:	The operator shall implement measures which detect and mitigate BGP misuse, and should have regard to standards, guidance and best practice.

SP.10:	The operator should collaborate with other network operators and implement technical and organisational measures which minimise incorrect routing information being propagated and mitigates spoofed BGP traffic.

95

96

8 Implementation Guidance

As international traffic represents the most significant risk to signalling security, operators should have a greater focus on international traffic when implementing mitigating measures.

The implementation guidance in the following subsections is applicable to the security measures in section 7 as shown in **Error! Reference source not found.** below.

Table 1 – Security Measures to Guidance Mapping

	NM. 01	NM. 02	NM. 03	NM. 04	NM. 05	NM. 06	NM. 07	NM. 08	NM. 09	NM. 10
8.1	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8.2		✓	✓	✓	✓	✓	✓			
8.3					✓	✓	✓			
8.4			✓	✓		✓				
8.5			✓							
8.6	✓							✓		
8.7	✓				✓	✓	✓	✓		
8.8									✓	✓

8.1 Third Party Providers

Applicable Security Measures: All

Given the sensitivities of the data involved operators may choose to manage the security of the signalling plane from within their own resources. However, as the domain of signalling plane security is a highly complex area, operators may choose to engage in resource pooling by outsourcing this function to a group security function or specialised third party. This approach allows the operator to benefit from the aggregated intelligence and lessons learned afforded by centralising this data with expert service providers.

This approach is acceptable, however, signalling plane security is a critical function and any third party providing this service is a critical supplier and must comply with the security measures outlined in ECSM 009.

8.2 Signalling DMZ

Applicable Security Measures: SP.02, SP.03, SP.04, SP.05, SP.06, SP.07

As the external signalling networks cannot be fully trusted, operators need to build a signalling security architecture that can validate externally derived signalling without impacting critical core network functions. Improved protections for critical core nodes and obfuscating user data will significantly increase the security and resilience of electronic communications networks that receive and process international signalling.

To protect critical core nodes from potentially malicious external signalling, the operator could establish an architectural De-Militarised Zone (DMZ) between external signalling networks and critical core nodes. The architectural approach would be like that used to protect an IP network from any untrusted source (such as the Internet).

It is recommended that the signalling DMZ contains the following functions:

- Filtering messages based on a range of rules, ideally filtering rules will be updatable in near-real time based upon security analysis.
- Authenticating messages where possible (e.g. for 5G signalling).
- A signalling address/identifier translation ('Signalling NAT'), to limit leakage of information about the internal network or users.

Should a node fail in the DMZ, this should have significantly lower impact than the failure of the core nodes themselves. Operators should design the DMZ to ensure that internal services are unaffected should network equipment within the DMZ fail. If implemented correctly, the DMZ should become a focal point for any external signalling attack. Consequently, the DMZ should be proactively monitored to detect signs of compromise.

8.3 Obfuscation and Topology Hiding

Applicable Security Measures: SP.05, SP.06, SP.07

Beyond increasing core resilience, another key principle is to reduce information leakage of network and user identifiers over the external signalling interface. A signalling DMZ would provide an appropriate location to perform address and user-identifier translation. The

principle should be to offer the minimum data externally that is necessary to support the signalling service.

In an ideal scenario, the functionality in the DMZ would only provide a representative, externally facing address for each externally facing service, and these addresses are independent of internal network architecture. For example, for SS7 the signalling DMZ would offer a single HLR address (GT), a single MSC address and a single SMSC address externally, effectively 'hubbing' or "NATing" the internal network services and architecture.

Similarly, signalling flows frequently include personal user data (e.g. identifier or location), but often the flow will work perfectly well if the home network only provides unique temporary identifiers. As a 'hub' for all international signalling, the signalling DMZ would provide an ideal location to translate or obfuscate unnecessary personal user data in signalling flows.

Measures can be taken to prevent a user's location being disclosed using IMSI obfuscation and limiting any unnecessary information about the home network being sent forward to other networks with the signalling data. IMSI obfuscation can be implemented by assigning a Temporary IMSI (TMSI) when the user first connects to a network this is usually done by the authentication centre. This TMSI is retained in the network and in the SIM card even when the handset is switched off so that it is available for use when the handset is switched on again. A new TMSI is created with new update events such as roaming, handoff, etc. and it is used in place of the IMSI to protect the user's identity. Operators should also keep abreast with state-of-the-art encryption techniques for IMSI obfuscation and implement these as soon as is feasible.

Topology hiding is a key issue for operators in terms of preventing attackers from getting visibility of internal network topology (equipment, applications, or software versions). If attackers can get this information, it gives them a significant part of what is needed to allow them to break into a network. This is particularly important for open source applications where source code can be obtained by attackers relatively easily. The Session Border Controller (SBC) is typically the key element that performs this function, it terminates the session and media and establishes a new session inside the operator's network thus hiding IP addresses and other details.

In Diameter based networks the Diameter Edge Agent typically implements topology hiding, GSMA publication" IR.88 - LTE and EPC Roaming Guidelines" is a publicly available document that provides information on this.

8.4 SMS Home Routing

Applicable Security Measures: SP.03, SP.04, SP.06

Home Routing in the recipient network changes the flow of inbound messages from other networks, directing them to an SMS router, rather than straight to target handsets. This feature is described in 3GPP TR 23840-710 and both the VLR global title address and subscriber IMSI can be hidden from originating networks, the latter with the use of a corelation identity inserted by the SMS router. This helps protects against misuse of the SMS delivery mechanism in the unauthorised tracking location of individuals, widespread distribution of unsolicited SMS and other types of malicious activities such as the redirection of SMS messages containing two factor authentication codes which are used to verify identity in banking and electronic commerce.

8.5 Signalling Monitoring & Analysis

Applicable Security Measures: SP.03

When implementing a signalling monitoring function/database, it is recommended that operators consider the following aspects:

- To take a copy of signalling data prior to implementing any security functions, and particularly before messages have been dropped or filtered. This allows the full context of the signalling to be analysed.
- As the signalling database is for the sole purpose of security monitoring, operators should anonymise all user data stored within signalling messages prior to storing the data. Even when anonymised, the signalling database remains a highly sensitive dataset.
- Where possible, ensuring that security analysis can be performed over multiple types of signalling (SS7, DIAMETER, 5G JSON signalling) at the same time.
- Establishing a technical means (such as a MISP) to share signalling security alerts and threat intelligence with other operators.

8.6 Network Testing and Auditing

Applicable Security Measures: SP.01, SP.08

Operators should take a risk-based approach to signalling plane testing and auditing, focussing efforts on the most critical nodes and network elements.

It is essential, particularly when commissioning a new network element, or when making architectural changes to networks, to conduct security pre deployment testing and subsequent security auditing. Auditing the resulting actual security of a network and comparing it to the expected, specified security is the only way to ensure that security is working the way it should.

Operators should conduct vulnerability scanning of their networks to ensure their signalling networks are resilient to evolving attack techniques. Operators should also conduct robustness testing on individual nodes to evaluate nodes resilience to signalling floods or malformed messages. Finally, operators should ensure fuzz testing is conducted on network elements to discover unknown potential vulnerabilities in signalling nodes.

In simplest terms, a PAW is a hardened and locked down workstation designed to provide high security assurances for sensitive accounts and tasks. This is the highest security configuration designed for extremely sensitive roles that would have a significant or material impact on the organization if their account was compromised.

The PAW configuration includes security controls and policies that restrict local administrative access and productivity tools to minimize the attack surface to only what is absolutely required for performing sensitive tasks. This makes the PAW device difficult for attackers to compromise because it blocks the most common vector for phishing attacks: email and web browsing.

To provide productivity to these users, separate accounts and workstations should be provided for productivity applications and web browsing. While inconvenient, this is a necessary control to protect users whose accounts could inflict damage to most or all resources in the organization.

8.7 Signalling Node Hardening

Applicable Security Measures: SP.01, SP.05, SP.06, SP.07, SP.08

Hardening signalling nodes involves reducing the surface of vulnerability by only using necessary services and protocols. Further detail and guidance on hardening of nodes can be found in 3GPP TS 33.117.

8.8 BGP

Applicable Security Measures: SP.09, SP.10

Operators should monitor the BGP protocol, have the ability to detect potential hijacks and have a procedure to respond appropriately when hijacks are detected. This response should extend to blocking traffic from being routed to the hijacked destination in extreme cases. Operators should also ensure that the IP address space they own and relevant contact information is securely maintained up to date in the appropriate registries.

Operators should implement filtering on Autonomous System (AS) prefixes and paths, both received and advertised, to control how traffic is routed and protect against bogus prefixes. This is described in RFC 7454. Operators could also implement security mechanisms where appropriate such as Generalised TTL Security Mechanism (GTSM) as described in RFC 5082 and Resource Public Key Infrastructure (RPKI) which adds authentication to the routing system using digital signatures

8.9 Alternatives

The implementation guidance outlined offers potential methods for an operator to meet the signalling security requirements of the ECSMs. Ultimately it is up to the operator to implement a solution which meets the security requirements set out in Section 7 of this ECSM. Provided the implementation ensures the core network is resilient to disruptive attacks from external signalling networks and prevents the leakage of sensitive user data, it will likely meet the requirements of the ECSMs.

9 Relevant References

The following standards, guidelines and reports offer further detail and will assist operators in designing policies, procedures and processes that meet the *Security Measures* outlined in Section 7 of this document.

9.1 3GPP TS 29.573 version 15.1.0 Release 15; Public Land Mobile Network (PLMN) Interconnection; Stage 3

Specification # 29.573 (3gpp.org)

This document specifies the stage 3 protocol and data model for the PLMN (Public Land Mobile Network) interconnection Interface. It provides stage 3 protocol definitions and message flows and specifies the APIs for the procedures on the PLMN interconnection interface. It covers the functionality of the Security and Edge Protection Proxy (SEPP) on these interfaces.

9.2 ENISA Signalling Security in Telecom SS7/Diameter/5G

Signalling Security in Telecom SS7/Diameter/5G — ENISA (europa.eu)

The SS7, SIGTRAN, GTP and Diameter signalling protocols underpin mobile telephone networks across the globe. It is well known that these signalling protocols have several severe security weaknesses, which can be exploited by attackers in many different ways. In order to determine the risk level of the situation EU wide, ENISA conducted an analysis within EU Member States. In this paper, the EU level state of play is described and some recommendations are made as regards the next possible steps to be taken. The purpose of this document is to provide a good understanding of the status in the EU as regards the security interconnect signalling and the overall risk level, current measures in place and future actions to be taken..

9.3 GSMA FS.07 SS7 and SIGTRAN Network Security

GSMA | FS.07 SS7 and SIGTRAN Network Security - Security

This document provides an overview of SS7 and SIGTRAN and how to handle SS7 messages on the edge of the network. It includes an SS7 and SIGTRAN security analysis and provides a set of countermeasures that can be deployed e.g. filtering rules and other security approaches. It also provides a description of the possible attacks which can be implemented against mobile networks and an evaluation of the real risks raised by them and goes on to propose best practice counter measures.

This document is confidential to GSMA members due to the sensitive nature of the information it contains.

9.4 GSMA FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines

GSMA | FS.11 SS7 Interconnect Security Monitoring and Firewall Guidelines - Security

This document describes how to monitor SS7 traffic, including prevention and detection techniques against suspected attacks. It allows an operator to assess whether received SS7 MAP or CAMEL messages are legitimate or not and apply appropriate firewall rules to protect its network. It guides operators, at a high level and in a non-vendor specific way, on how to monitor SS7 traffic including the establishment of firewall rules and data sharing capabilities. It provides guidelines on how SS7 traffic on the interconnect links can be monitored, what abnormalities to look for, and how to report them. It also contains a risk assessment of all GSM-MAP and CAMEL packet types and provides descriptions of recommended SS7 firewall rules for the handling of MAP and CAMEL vulnerabilities. It should be noted that the information on SS7 attacks listed in this document is not exhaustive.

This document is confidential to GSMA members due to the sensitive nature of the information it contains.

9.5 GSMA IR.82 SS7 Security Network Implementation Guidelines

GSMA | IR.82 SS7 Security Network Implementation Guidelines - Security

This document outlines general SS7 security measures (MAP and CAP signalling), including measures specific to SMS security, and the possible enforcement point for each measure. For maximum benefit. It should be read in conjunction with FS.11 and FS.07. It provides information about the different options for implementing SS7 security features within the PLMN network, the SS7 carriers, roaming and SMS Hubs. It also proposes a concrete technical classification for SS7 GSM MAP messages and message parameters to check

This document is confidential to GSMA members due to the sensitive nature of the information it contains.

9.6 GSMA FS.19 Diameter Interconnect Security

GSMA | FS.19 Diameter Interconnect Security - Security

This document outlines potential operator network specific Diameter based attacks and countermeasures against those attacks. It aims to provide an understanding of potential risks, threats and countermeasures related to LTE and 5G interconnection security. Includes attacks related to interworking between Diameter and SS7 MAP. It should be read in conjunction with FS.07 and FS.11. It should be noted that the information on attacks listed in this document is not exhaustive due to the constantly changing nature of attack techniques and methodology.

This document is confidential to GSMA members due to the sensitive nature of the information it contains.

9.7 GSMA IR.88 LTE and EPC Roaming Guidelines

GSMA | IR.88 LTE and EPC Roaming Guidelines v22.0 - Newsroom

This guideline provides a standardised view on how LTE and EPC networks can interwork to support roaming. It provides access to operators to authoritative roaming guidelines covering how LTE and EPC networks can interwork. It also addresses aspects which are new and incremental to EPC roaming in general and using LTE access specifically.

9.8 GSMA FS.20 GTP Security

GSMA | FS.20 GPRS Tunnelling Protocol (GTP) Security - Security

This document provides a technical background on how the GPRS Tunnelling Protocol (GTP) is used. It outlines potential attacks and exploitation possibilities and assesses the associated risk. It then presents countermeasures for Operators to protect their networks against GTP-related attacks. It needs to be read in conjunction with IR.88. It provides a technical background on how GTP is used, introduces attacks and exploitation possibilities, and derives associated risk. It also presents countermeasures for operators to protect their networks against attacks that involve GTP and provides the GTP Risk Classification and recommendations for GTP firewall.

This document is confidential to GSMA members due to the sensitive nature of the information it contains.

9.9 GSMA FS.21 Interconnect Signalling Security

GSMA | FS.21 Interconnect Signalling Security Recommendations - Security

This document highlights key risks associated with interconnect security vulnerabilities and outlines suggested approaches to mitigate these risks for mobile Operators. It outlines suggested MNO responses to such risks and provides information as what should be included in a business case for investment in interconnect signalling security. It also provides tips on what should be included when issuing RFI/RFP.

This document is confidential to GSMA members due to the sensitive nature of the information it contains.

9.10 ENISA 7 Steps to shore up the Border Gateway Protocol (BGP)

7 Steps to shore up the Border Gateway Protocol (BGP) — ENISA (europa.eu)

BGP is a central part of the internet backbone. It is used by internet service providers to relay internet traffic across the globe. It was designed more than 25 years ago and when it was introduced the main requirement was resilience, simplicity, and ease of deployment. BGP lacks security which make it vulnerable to attacks and misconfiguration errors. In this paper ENISA highlights the security vulnerabilities of BGP and explain why it is so important to address them. Working closely with experts from industry ENISA derived a shortlist of 7 basic BGP security measures which are industry good practices that should be relatively simple to adopt and relatively effective.

9.11 MANRS Actions for Network Operators

https://www.manrs.org/isps/

Mutually Agreed Norms for Routing Security (MANRS) is an initiative to greatly improve the security and resilience of the Internet's global routing system. It does this by encouraging those running BGP to implement well-established industry best practices and technological solutions that can address the most common threats. This publication contains a number of actions that can be implemented by network operators to address three main classes of problem:

1. Incorrect routing information
2. Traffic with spoofed IP addresses
3. Coordination and collaboration between networks.

9.12 Responsible Use Of The Border Gateway Protocol (BGP) For ISP Interworking

Technical report: Responsible use of the Border Gateway... - NCSC.GOV.UK

This guidance was developed by the UK NCSC in collaboration with major UK operators. It is intended to be used by Telecom Operators and ISPs to help them securely specify, design, architect and build their networks. It encourages operators to use the BGP in a predictable and rigorous way, making full use of Internet Registries such as RIPE. By implementing this guidance, operators will be helping to ensure the resilience of the global internet. Whilst initially written with the UK ISP (Internet Service Provider) community in mind, the contents of this document and the principles on which it is built are broadly applicable in all BGP deployments, globally.

9.13 IETF RFC 7454

BGP Operations and Security

This document describes measures to protect the BGP sessions itself such as Time to Live (TTL), the TCP Authentication Option (TCP-AO), and control-plane filtering. It also describes measures to better control the flow of routing information, using prefix filtering and automation of prefix filters, max-prefix filtering, Autonomous System (AS) path filtering, route flap dampening, and BGP community scrubbing.

9.14 IETF RFC 5082

The Generalized TTL Security Mechanism (GTSM)

This document specifies an Internet standard track protocol for the Internet community, and requests discussion and suggestions for improvements. It generalises the technique of the use of a packet's Time to Live (TTL) (IPv4) or Hop Limit (IPv6) to verify whether the packet was originated by an adjacent node on a connected link has been used in many recent protocols. It is designed to protect a router’s IP based control plane from CPU utilisation based attacks.