Signalling Security in Telecom SS7/Diameter/5G

EU level assessment of the current situation

MARCH 2018

www.enisa.europa.eu

European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please use incidents@enisa.europa.eu.
For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The analysis in this document was produced in collaboration with: European Commission, Art. 13a Expert Group, several electronic communications providers members of GSMA and ETIS.

Several experts were consulted and/or peer reviewed the document: Silke Holtmanns, Albert Nguyen, Cathal Mc Daid.

Many thanks to GSMA for providing us access to important and relevant work in the field.

Legal notice

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

ISBN: 978-92-9204-252-3, DOI: 10.2824/38400

Table of Contents

Executive Summary

Telecommunications are key in nowadays societies. They represent the backbone, the primary infrastructure based on which our society works and constitute the main instrument in allowing our democracy (and other EU core values such as freedom, equality, rule of law, human right) to function properly. As a consequence, here in ENISA (the EU cyber security agency) we consider assuring the security of our infrastructure as a top priority.

The present study has deep dived into a critical area within electronic communications, the security of interconnections in electronic communications (signalling security). Based on the analysis, at this moment there is a medium to high level of risk in this area, and we do consider that proper attention must be granted by all stakeholders involved so as to find a proper solution.

As mobile technologies evolve so does the threat landscape. Early generations of mobile networks 2G/3G rely on SS7 and its IP Version SIGTRAN, a set of protocols designed decades ago, without giving adequate effect to modern day security implications. Nobody at that time envisioned the scale that mobile networks could reach in the future, so trust and security were not issues. Nonetheless at the moment we are still using this legacy set of protocols to assure the interconnection between providers. The industry and security research community has started covering the topic, by providing good practices and necessary tools. But still, a lot more has to be done. Basic security measures seem to be implemented by more mature providers, but these measures assure only a basic protection level. More efforts need to be made so that an optimal protection level is achieved.

Current telecommunication mobile generation (4G) uses a slightly improved signalling protocol called Diameter. Build with the same interconnect principles in mind but on an IP base, the protocol has been proved vulnerable. The industry is still trying to understand exact implications and to identify possible workarounds. Attackers are also in the same phase. It is our impression that the next step will be made soon. As soon as SS7 becomes sufficiently protected their focus will change towards the new attack surface.

5G, the new mobile generation, is still under development. Early releases from some manufacturers are available but the standards are still in their infancy. Nevertheless there is a certain risk of repeating history. Given the improvements that 5G will bring (more users, more bandwidth etc.) having the same security risks could be extremely dangerous.

This document represents an EU wide (and not only) assessment of the current situation. We have analysed areas like types of attacks and their frequencies, security measures in place, available best practices and other constraints so that we can get an overall picture of signalling security in Europe. As you will notice in the document, further efforts are needed at global level to tackle current threats and prevent future similar situations. Special attention must be granted by different stakeholders involved so that an adequate level of protection is achieved across EU.

Please find below a set of high-level recommendations that we urge responsible stakeholders to take into account. For further details, pls. refer to the rest of the document.

For EU Commission:

1. Consider revising the current legal landscape so that signalling security is covered.
2. Consider the adoption of baseline security requirements for electronic communications providers to include signalling security.
3. Consider taking necessary measures to support the improvement of security for current legacy elements sustaining the EU telecommunication infrastructure.

4. Thoughtfully supervise the implementation of the 5GPPP to cover also signalling security among the various tasks of the Security Working Group.
5. Further increase the international cooperation as a global effort is needed to overcome the threats.

For ENISA and Art. 13 EG

1. Periodically analyse the situation to identify further developments.
2. Consider publishing EU guidelines for assuring an advanced protection level at Member State level.

For National Regulatory Authorities

1. Regularly analyse the national situation and be aware of any developments that can cause significant incidents in this area.
2. Consider revising the national legislation (if needed) so that signalling security should be covered in terms of reporting incidents and adopting minimum security requirements.

For Industry

1. Electronic communication providers: adopt the necessary measures to ensure an adequate level of security and integrity of telecommunication networks.
2. Standardisation bodies: ensure security is covered properly within the new 5G standards.

1. Introduction

1.1 Background

In today's digital era, people are depending more and more on mobile communications. According to GSMA, a renowned association that represents the interests of mobile network operators worldwide, there are over 5 billion unique mobile subscribers and over 2000 operators worldwide (800 full members + 992 MVNO and 260 MNO sub-brands[1]). GSMA covers 220 countries. In Europe, according to GSMA Mobile Economy Europe 2017 there are 456 million unique mobile subscribers in Europe, equivalent to 84% of the population. Europe is seeing rapid adoption of 4G services. Also at the "end of 2016, there were 226 million 4G connections in Europe (up 46% year on year), accounting for more than a third of total connections (excluding M2M). 4G connections will overtake 3G connections in the region in 2017 and reach 61% of the total by 2020".Each mobile network has its own specificities, but all the mobile networks are interconnected and count as one global and worldwide network providing services to a large part of the population. In telecommunication, signalling means the use of signals for controlling communications (the sending of a signal from the transmitting end of a telecommunication network to inform a user at the receiving end that a message is to be sent)[2].

The SS7, SIGTRAN, GTP and Diameter signalling protocols are underpinning mobile telephone networks across the globe. It is widely known that these signalling protocols have several severe security weaknesses, which can be exploited by attackers in many different ways. Although these attacks do not happen at a large scale, the impact for individual subscribers can be quite significant. At the same time, weaknesses in signalling protocols are not easy to tackle.

While mobile technologies have evolved in the past twenty years to meet subscribers' expectations, especially in terms of bandwidth and number of connections, the underlying technologies used to interconnect networks did not follow the same course of evolution. While quantity and resilience has been always a key concern, security was hardly a requirement. In recent years, the development of mobile networks has been totally business driven, as mobile generations have increased their capacity for voice and data, but little attention has been granted to the legacy technologies used to interconnect networks.

What was once a safe interconnecting environment, due to the small number of providers with no real need for access control, has now become a "Wild West" running on legacy infrastructure. As nowadays we have more coverage, more clients and more networks that interconnect worldwide the risk level has certainly increased significantly. Not only telecom providers need interconnection access but also location service and content providers.

Second and third generations of mobile networks – 2G/3G - are based on SS7. Signalling System 7 (SS7) is a set of signalling protocols developed in 1975, used to exchange information among different elements of the same network or between networks (call routing, roaming information, features available to subscriber etc.).

The current mobile generation - 4G - uses Diameter as a replacement for SS7. However, all generations – 2G/3G/4G – have kept the same interconnect principles, inherited from wireline networks. Public Switched Telephone

[1] https://www.gsmaintelligence.com/research/2015/02/the-global-mvno-footprint-a-changing-environment/490/
[2] https://en.wikipedia.org/wiki/Signalling_(telecommunications)

Networks (PSTN) have been interconnected based on trust, between a small number of operators, within a closed group. Deregulation and market opening have made access to interconnect networks much easier resulting in a huge number of operators interconnected worldwide.

Security researchers have been drawing media attention to the problem of SS7 weaknesses since 2014[3]. In the following years, new attacks were published in the media and security literature. Most of these attacks only use functions provided by mobile networks to succeed. The only requirement for a successful attack is access to an SS7 network, which is typically reserved to network operators. But, nowdays SS7 access can be easily purchased.[4]

From the description above it is easily understandable why the interconnect environment has become perilous. Protocols designed decades ago, with no security or access control in mind, cannot cope with today's challenges. In order to benefit from all business opportunities today, operators need to open their networks for different types of partners, either operators or other types of service providers. This allowing of uncontrolled access to multiple partners is the main reason for increasing the security risks in signalling, but since it is a business enabler, it is highly improbable that operators will stop doing it. Attacks are based on the exploitation of legitimate SS7/Diameter traffic/messages making it very difficult to detect.

One important factor to mention is that in most of the cases the subscriber cannot do too much in order to protect themselves from these risks. As most of the attacks are developed at the providers' level (as both SS7 and Diameter are protocols functioning within the providers' core network), the possible actions available for subscribers are very limited (e.g. encryption). Most of the security work has to be done at the providers' level.

A notable study that points out how vulnerable mobile networks are can be found here. According to the source[5] no mobile network is secure, subscriber data is in jeopardy and NO operator (either big or small) can guarantee security. The researchers launched several attacks against the probed networks and managed to execute 80% of DoS attacks, 77% of leakage attacks, and 67% of fraudulent actions.

Currently, there are several key documents highlighting the security risks as regards SS7 and Diameter. Below we list some of them:

- April 2014: P1 Security presents at the "Hackito Ergo Sum" conference two papers related to SS7 attacks.[6]
- August 2014: Washington Post publishes an article on commercial surveillance equipment and services that are taking advantage of SS7 vulnerabilities.[7]
- December 2014: Security researchers present at the 31st Chaos Communication Congress (CCC) two papers describing attacks on SS7 networks.[8]

[3] https://www.theregister.co.uk/2014/12/26/ss7_attacks/
[4] https://www.thedailybeast.com/you-can-spy-like-the-nsa-for-a-few-thousand-bucks
[5] https://www.ptsecurity.com/upload/ptcom/SS7-VULNERABILITY-2016-eng.pdf
[6] http://2014.hackitoergosum.org/slides/day3_Worldwide_attacks_on_SS7_network_P1security_Hackito_2014.pdf and http://2014.hackitoergosum.org/slides/day1_Hacking-telco-equipment-The-HLR-HSS-Laurent-Ghigonis-p1sec.pdf
[7] https://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f_story.html?utm_term=.33db0bf4c1ce
[8] http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf

- December 2015: Publication of the "Common Nordic Recommendations on SS7 Security Issues". Jointly developed by regulators in Norway, Sweden, Denmark, Finland and Iceland.[9]
- April 2016: Live demonstration during the TV show "60 minutes" of an attack to a congressman.[10]
- June 2016: ITU Workshop on "SS7 Security"[11]
- March 2017: FCC publishes a report on "Legacy Systems Risk Reductions"[12]

The range of attacks that can be developed through weaknesses in signalling varies a lot. The industry's focus has been around the following types of attacks: SMS spam, call intercept, subscriber DoS, subscriber account fraud, call intercept, location tracking. A list of successful attacks or demos is included below:

- A **data session hijacking** which was achieved by performing GTP attacks.[13]
- **Eavesdropping** attack demonstrated for the CBS 60 minutes TV show. [14]
- O2 in Germany confirmed that some customers in Germany have had their accounts drained by attackers that used SS7 to intercept and redirect mTANs to their own phones.[15]
- Positive Technologies presented one time password theft and account takeover.[16]
- SMS and one time password interception was presented at the 2017's IEEE International Conference on Communications.[17]
- (Attempted) Data interception attacks using SS7[18]
- DoS performed on a an operator[19]
- Subscriber Profile Extraction and Modification via Diameter Interconnection was presented at the 11th International Conference on Network and System Security 2017.[20]

1.2 Scope

In order to determine the risk level of the situation EU wide, ENISA has conducted an analysis within EU Member States. In this paper, the current 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. Providing

http://events.ccc.de/congress/2014/Fahrplan/system/attachments/2553/original/31c3-ss7-locate-track-manipulate.pdf

[9] https://eng.nkom.no/topical-issues/news/nordic-authorities-collaborating-on-measures-against-vulnerabilities-in-networks

[10] https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

[11] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx

[12] https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf

[13] https://www.corelan.be/index.php/2014/05/30/hitb2014ams-day-2-on-her-majestys-secret-service-grx-a-spy-agency/

[14] https://www.cbsnews.com/news/60-minutes-hacking-your-phone/

[15] http://www.sueddeutsche.de/digital/it-sicherheit-schwachstelle-im-mobilfunknetz-kriminelle-hacker-raeumen-konten-leer-1.3486504

[16] https://www.theregister.co.uk/2017/09/18/ss7_vuln_bitcoin_wallet_hack_risk/

[17] http://icc2017.ieee-icc.org/

[18] https://www.adaptivemobile.com/blog/malicious-data-interception-via-ss7

[19] https://www.digi.no/artikler/roper-hvem-som-forarsaket-telenors-mobil-havari/348087
https://www.adaptivemobile.com/blog/ss7-security-putting-pieces-together

[20] https://link.springer.com/chapter/10.1007/978-3-319-64701-2_45

technical solutions that can solve the problems is rather not the objective of this document. Nevertheless, taking into account the technical aspects of the topic, in some cases technical details have been provided in order to validate the findings.

1.3 Target audience

The target audience of this work is as follows:

- EU Commission, as a technical input for defining further policies in the field, as this document will provide a good understanding of the risk associated with the topic.
- Relevant EU national authorities, as a technical input for defining/adapting their national policies in the area.
- Electronic communication providers in Europe and outside, as an awareness raising initiative.
- Industry associations and other bodies with roles in standardisation and mobile security.

1.4 Methodology

The underlying study presented in this report involved a three-tiered methodology consisting of a primary desktop research reviewing the relevant literature, a subsequent online questionnaire-based information gathering, and a final set of in-depth interviews to address more nuanced and detailed issues that could not have been captured in the survey. The approach aimed to collect all the available information regarding the practices employed by industry and EU regulators. The survey was opened for 9 months and has been sent to all National Regulatory Authorities across the EU with the requirement to be sent to their national electronic communications providers. The Nordic countries have developed their own survey before the ENISA study started and this has been taken into account in this document.

The survey was also promoted through different industry associations such as GSMA, ETIS etc. On top of this the desktop research included information collected from several renown experts working in the field through interviews, discussions etc.

39 electronic communication providers across the EU have provided an answer in this study. The responses come from a mix of operator, from the biggest ones in EU (covering many Member States) to local ones.

NOTE: ENISA generally employs in-depth ***QUALITATIVE ANALYSIS*** (deep dive) to describe, in detail, specific situations using policy analysis tools such as interviews, surveys and desktop research and provide insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. ENISA is not a research agency and does not engage in extensive statistical analyses. ENISA is a technical advisory agency to the European Commission and to the EU Member States and, in this capacity, uses the simplest appropriate methods to measure variables that are conclusive for the decision making process and for policy implementation. Therefore, the agency’s focus is that the policy process involves all relevant stakeholders and that the consultation process is comprehensive and thorough.

1.5 About ENISA and the Art. 13a Expert Group

Art. 13a, of the Directive 2009/140 EC, is part of the Telecom Package and aims at ensuring the security and integrity of electronic communication networks and services, dealing mostly with prevention of outages or service disruption (availability of the service). This is partially achieved through requiring telecommunication service providers to take the appropriate technical and organizational measures to manage the risks posed to security of networks and services, guarantee the integrity of their networks (ensure the continuity of supply of services provided over those networks) and notify the competent national regulatory authority (NRA) of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services.

As a response to the directive's requirements, in 2010, ENISA, Ministries and NRAs from Member States, initiated a series of meetings (workshops, conference calls) in order to achieve a harmonized implementation of Art. 13a of the Framework directive. As a result of these meetings, a group of experts from NRAs, now entitled the Art. 13a Expert Group, reached agreement on several non-binding technical documents[21] providing guidance to the NRAs in the EU member states.

Since the group's focus is mostly related to availability of services, signalling security was not within the main topics of the agenda. Since the latest developments, where availability related incidents started being reported to the NRAs, the group together with ENISA decided to further analyse the EU level situation.

[21] https://www.enisa.europa.eu/topics/incident-reporting/for-telcos

2. Assessment of the current status at EU level

The findings within the following section are based on the survey developed by ENISA during 2017. More details on the survey can be found in the Methodology section.

2.1 Overall considerations

One of the main questions of the survey was about the perceived level of threat level associated with signalling. As you can see in the figure below the vast majority of providers indicated a medium to high level. The perceived level refers to the subjective individual measure of the danger.

The image below is reinforced by the different documentation publicly available, mentioned in the previous chapter.

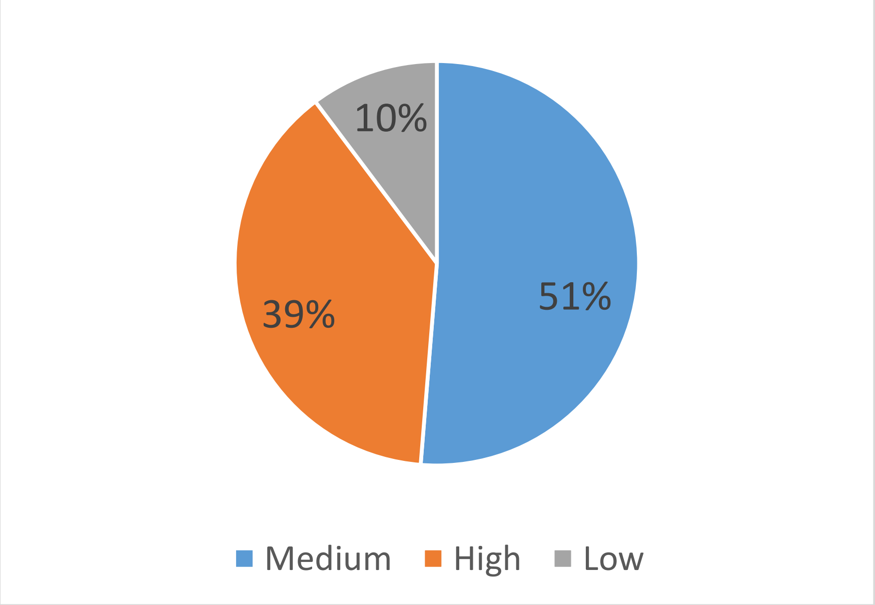


Figure 1 – Perceived signalling threat level

2.1.1 Types of attacks

The survey had several questions regarding the **common types of attacks** encountered “in the wild”. Based on the findings the most common attacks are described below. For a brief description of the attacks, pls. check Table 1.

SMS traffic is still a big source of revenue for mobile operators. Even if SMS peer-to-peer traffic decreases every year, SMS traffic from applications to users still increases significantly. Attackers have started to find new ways to bypass charging associated with SMS termination. That is why SMS Spam attack is a type of incident that almost every operator had faced.

Tracking attacks are generally easy to perform. Furthermore, detection of these attacks is more subject to false positives than any other type of attacks. The main cause for such false positives is misconfiguration. In many cases, the operator cannot distinguish between traffic coming due to misconfiguration errors or because of a real incident. Therefore, the occurrence of such an attack is most probably overrated.

Intercept attacks are more complex and require the attacker to keep a connection open in the network, waiting for victims to communicate. While operators have observed such kind of incidents, they still count as the least part of the perceived attacks. However, publicly available tools will make the deployment of intercept attacks easier and an increase is expected for the coming years.

Denial of service attacks involve procedures associated with the reset of a piece of equipment. Thus, their impact is limited to a part of the network, usually much less than the whole infrastructure. Denial of service attacks may also affect a specific component, in which case the impact is again limited to a part of the network. Small-scale denial of service attacks are harder to detect.

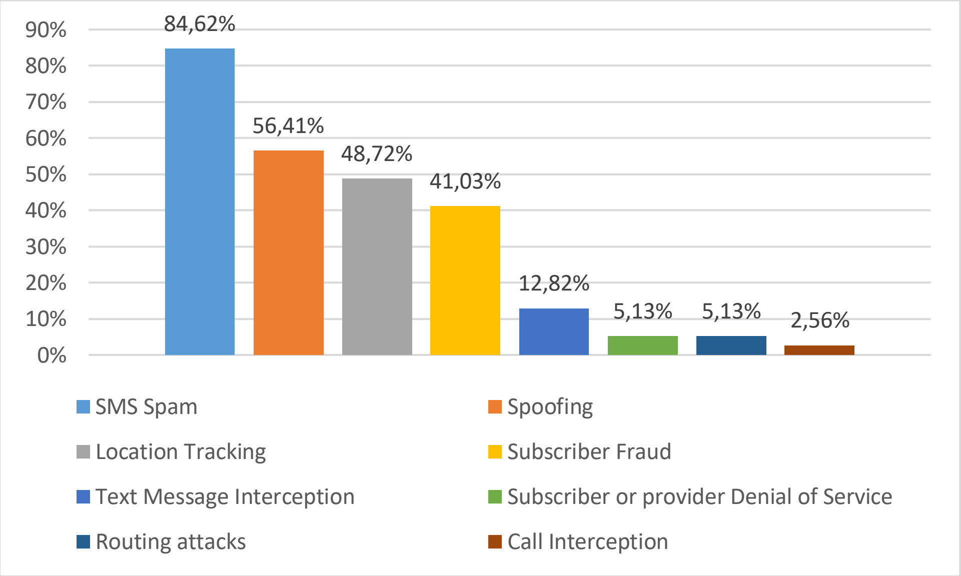


Figure 4 – Common types of attacks

The following table provides brief description of the main types of attacks.

TYPE OF ATTACK	DESCRIPTION	POTENTIAL IMPACT
SPAM	Routing a short message to the Mobile Terminating device has a cost, which shall be correctly charged to the sender. An attacker can send bulk SMS messages, bypassing the correct route, and hence evading billing. Another option is to spoof various SMS parameters, such as sender ID, or bypass a control system to send directly SMS to victims. In this context SPAM does not refer to unsolicited communications sent through email.	Massive sending of SMS and calls, with the goal of stealing personal data, or gain financial benefits using toll numbers.
SPOOFING	Identifiers (addresses, names and subsystem numbers) used are various levels of SS7 and Diameter are not authenticated and may be spoofed by malicious actors.	Evade billing. Interwork with networks which are not roaming partners
LOCATION TRACKING	An attacker can locate a target subscriber based on its MSISDN. As mobile networks need to efficiently route messages to subscribers, home network knows where to send messages to contact any given subscriber. In some cases, the attacker does not even need to send	Obtain the coarse location of a given victim. This has been used on high-profile victims in the US to demonstrate what attackers may gain (CBS).

	messages, since passive eavesdropping may reveal the target location. Obtaining subscriber's visited location is also a prerequisite for further attacks such as intercept.	
SUBSCRIBER FRAUD	An attacker can tamper with subscriber's profile, or send signalling messages to trigger malicious charging, with the objective to benefit from a service while evading billing.	Objectives can be: • To get or steal prepaid voice, SMS or data credits • To modify profiles, e.g. to transform prepaid into post-paid subscribers • To alter charging, e.g. overbill another subscriber or simply evade it • To abuse mobile money services based on MAP USSD
INTERCEPT	An attacker can alter current subscriber's location and profile in order to receive mobile terminating and/or mobile originating calls, SMS, or data traffic. This attack allows eavesdropping victim's communications, or may involve a full man-in-the-middle with alteration of communication. Access to signalling interface, allows an attacker to organize efficient local interception attacks based on fake antennas.	As SMS is commonly used for a second authentication factor (2FA), attackers may also eavesdrop SMS in part of a larger attack, to circumvent 2FA. Communication interception
DENIAL OF SERVICE	An attacker can cause a denial of service to the whole network, or to a set of subscribers, or even to a single targeted subscriber. Mobility offers functions to remove a subscriber from a specific geographical zone, and an attacker has only to use it to deny a service to a specific user.	Typical high-level impact is a regional network equipment reboot, which would discard all subscriber's contexts who are currently attached to it. As it is repeatable at will, it can cause persistent troubles.
ROUTING ATTACKS	Interconnect based on packet networks make use of routing (a process of selecting a path for traffic in a network), and hence may be sensitive to routing hijack attacks.	Due to the lack of integrity checks and encryption, an attacker may eavesdrop or alter interconnect traffic.
INFILTRATION ATTACKS	An attacker can abuse interconnect to obtain access to otherwise inaccessible systems. User data are tunnelled when traversing the mobile core network. Misconfigurations may allow attackers to get illegal access to part of the mobile core network. Attackers may also get access to mobile core network systems via mobile data or operational interfaces, which may lead to other attacks.	Unauthorized access to mobile core network elements. Typical impacts include personal data theft, or access to other sensitive assets such as other Packet Data Networks.

Table 1 – Common types of attacks

As regards the frequency of attacks, most of the providers have declared having less than 10 incidents per year. The picture below portrays also other frequencies declared in the survey. No other publicly available information was identified to confirm these findings, but there are studies pointing out how vulnerable networks are against such threats.

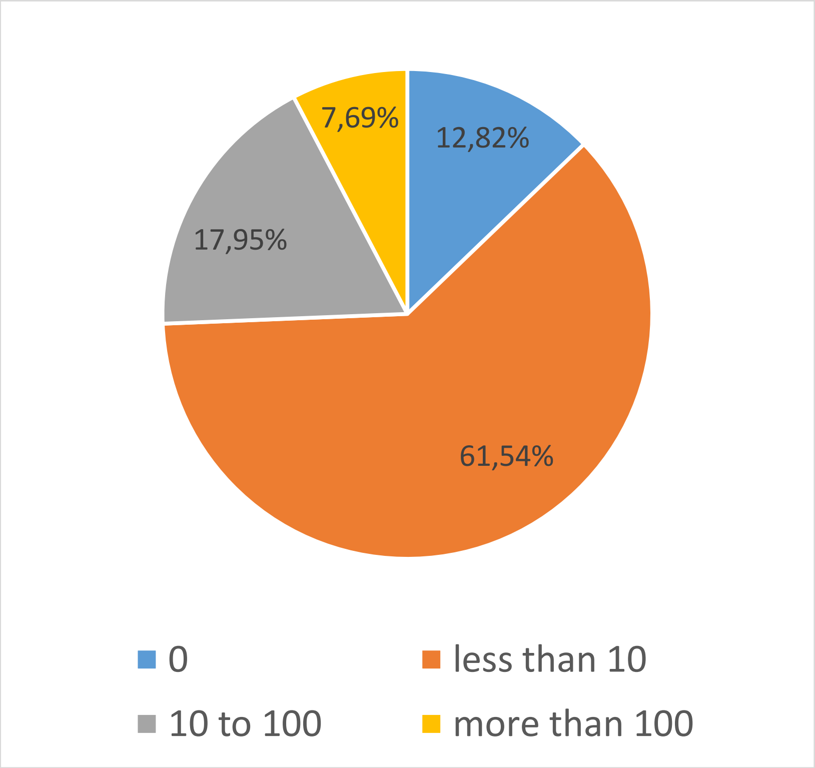


Figure 5 – Attack frequency per year

Nevertheless 61% of the respondents declared having in place processes and adequate resources for handling such incidents.

2.1.2 Security measures in place

Several questions were asked about the available measures in place. Pls. find below the answers provided.

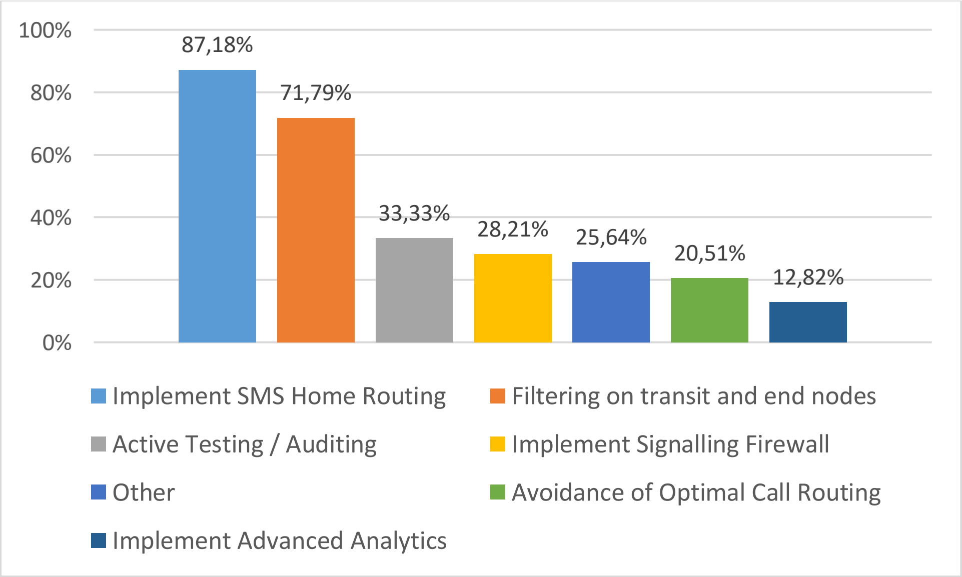


Figure 6 – Security measures in place

As indicated in the above chart, **in general, most of the operators have implemented basic security measures especially for SS7**. But basic measures only cover basic attacks.

SMS has been a target for attackers since a long time. Most operators (87%) implement SMS home routing, to protect their networks against from leaking sensitive information associated with a subscriber[22], which would help to mount further attacks . SMS home routing offers additional security by implementing message management mechanisms in the home network to provide protection against external messages.

Filtering on nodes refers to applying different rules on signalling messages that pass through the nodes to remove the ones that might be malicious. 71% ensure filtering on transit and end nodes.

Monitoring the signalling network is regularly done by 69% of the respondents. Monitoring is of the utmost importance because it is the first step towards identifying and mitigating threats. Without monitoring, you cannot detect malicious traffic, and consequently you cannot react to it. In terms of methods used for traffic analysis, operators are using more than one method to achieve better results: 38% indicated statistical analysis of message logs, 35% real time detection of occurrences of predetermined signatures and 35% mentioned a regular analysis of massage logs.

We described before that one of the common practices that operators are using to implement interconnection is via a carrier. It is important to highlight, that only 38% of the operators impose security requirements on their carriers.

Signalling firewalls have been implemented by roughly 28% of the respondents, a rather low percentage. But firewalls have their drawbacks also, as a firewall with only filtering could well protect the home subscribers in the home network, but the home subscribers in roaming or inbound-roamers could not be easily protected mainly because the SS7/Diameter are vulnerable to spoofing and the "Location Update" is not authenticated.[23] In this respect signalling protection should not only be based on filtering but also on assuring confidentiality and integrity.

In line with a good security posture, some operators have established bi-directional links with a small number of their partners. Though such a solution would never be applicable to all roaming partners, it has the advantage of offering security properties such as source authentication, integrity and confidentiality.

GPRS Tunnelling Protocol (GTP) allows mobile subscribers to maintain a data connection for internet access while on the move. GTP manages tunnels for transporting IP packets throughout the core network to the internet. GTP comprises three parts—control plane (GTP-C), user plane (GTP-U) and charging (GTP-C). By GTP monitoring, we refer to performing security checks on protocol messages. 53% of the respondents do monitor GTP-C traffic.

One important aspect to be considered in terms of security measures is that due to the architecture of the signalling protocols & infrastructure the electronic communication providers are the only ones capable of adopting any kind of security measures for customer protection. Subscribers are capable of adopting limited measures (e.g. data encryption).

[22] Namely, the IMSI (International Mobile Subscriber Identity), which identifies a subscriber for network related operations.

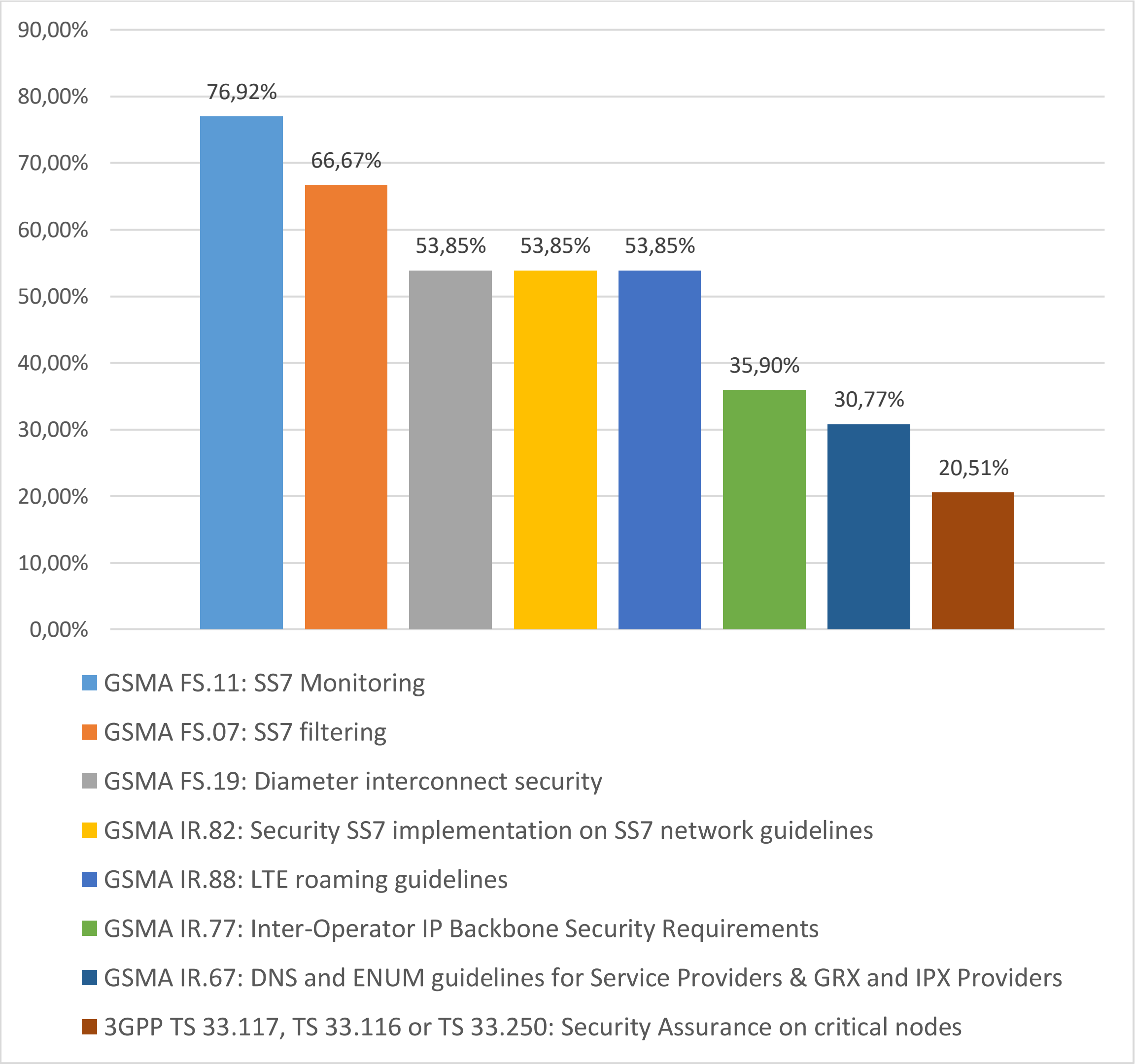
[23] https://www.blackhat.com/docs/us-17/wednesday/us-17-Kacer-SS7-Attacker-Heaven-Turns-Into-Riot-How-To-Make-Nation-State-And-Intelligence-Attackers-Lives-Much-Harder-On-Mobile-Networks.pdf

2.1.3 Available best practices

Operators are generally aware and they do follow GSMA documents addressing signalling security, even though they are generally used more as a template than a checklist. GSMA guidelines are very well appreciated by the industry, representing the reference point in this area. One of the drawbacks, until recently, was that access to them was restricted only to GSMA members, preventing other types of stakeholders (e.g. regulatory authorities) to consult them. Fortunately, during the development of this study, GSMA has understood the importance of sharing these guidelines with the regulators also. In this respect, an easy-to-follow procedure has been put in place by GSMA so that regulators from EU Member States could have access to the documents.

Figure 7 offers a good picture of the most used guidelines.

Some national regulatory authorities in the EU have taken the initiative to address this issue from a regulatory perspective. The Nordic countries (Sweden, Norway, Denmark, Iceland) have published joint recommendations on measures against vulnerabilities in electronic communications networks[24]. The guidelines have also a confidential regime, being accessible only to regulators.



[24] https://eng.nkom.no/topical-issues/news/nordic-authorities-collaborating-on-measures-against-vulnerabilities-in-networks

Figure 7 – Guidelines on signalling security

2.1.4 Constraints in adopting more security

The study also contained questions about the eventual constraints as regards the adoptions of more security measures.

Most of the operators (75%) responded that complexity and cost are blocking the implementation of advanced signalling protection. This is certainly not something unexpected. For example, monitoring should be done as close as possible to the interconnect links. Protection against attack patterns requires to monitor the traffic in its entirety. The resilient nature of interconnect protocols, using load-sharing[25] and active/active mode[26] raises technical issues and might threaten availability.

In addition, the use of an SS7 / Diameter firewall poses a few problems: detection and reaction to malicious traffic imposes an analysis on all the interconnect traffic. Detection of malicious traffic will never be perfect and misconfigurations may sometimes be interpreted as malicious actions. Responses to such a false positive may involve operator’s liability and potential financial and legal aspects may apply.

On the other side, firewalling may provide a way to screen operators’ outgoing traffic. Some operators are leasing to third parties SCCP Global Titles[27], which are the addresses for routing signalling messages. In such a case, as they don’t have direct control over third-parties system, they should pay particular attention to their egress traffic. Thus, domestic roaming is a specific topic that needs to be properly addressed by SS7 / Diameter firewalling.

Assuredly implementing a proper signalling protection in place will raise many complexity related issues. On top of this, for an operator to address sufficiently signalling security, a considerable investment is required. There are solutions available but their prices are not cheap.

33% of the respondents have also indicated legal constraints in implementing better signalling protection. As tracking down malicious/malformed signalling messages, one might also consider the potential impact on data retention, data protection and user privacy in general. Applying to much protection with the use of advanced analytics, implies storing parts of the signalling messages and might be considered a privacy violation by some regulators. On the other hand not applying proper security measures to protect subscribers against signalling attacks might be considered a violation of the Telecom Framework in other cases. As some providers have indicated real drawbacks in this area determined by national legislation, a closer look has to be given to certain aspects from the EU and national legislation that might prevent the adoption of advanced security measures.

Nonetheless, other constraints are noticeable at EU level due to the fragmented regulatory landscape that applies to electronic telecommunication providers. In terms of security, the current Telecom Framework Directive[28] covers only the availability of the service, excluding by default signalling incidents that might fall under the integrity or confidentiality protection goals. As most of the Member States have implemented the directive only with availability in scope, signalling related issues (incidents and/or minimum security measures) might not be covered by the national implementation. The current ePrivacy Directive[29] does cover confidentiality in electronic communication

[25] Messages in an SS7 network are load shared for directing message traffic to multiple destinations.
[26] Active/Active mode two or more elements aggregate the network traffic and work as a team to distributes it to the network.
[27] Wikipedia: SCCP Global Titles is the equivalent for IP addresses. The Signalling Connection Control Part (SCCP) is a network layer protocol used in Signalling System 7 telecommunications networks. A global title (GT) is an address used in the SCCP protocol for routing signalling messages
[28] https://ec.europa.eu/digital-single-market/en/telecoms-rules
[29] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN

sector, but might be in the responsibility of another authority at the national level. In this respect, the general view upon the situation might be fragmented at national level. Therefore, the number of incidents reported to ENISA that concerned signalling issues is rather low or even zero for the previous years. This might indicate a certain lack of visibility at national and EU level on the topic.

2.2 Considerations on Signalling System 7 (SS7)

SS7 related vulnerabilities have been analysed extensively by the industry. In recent years, many pages were written and many talks have taken place regarding the issue. As a result, at this point, we have a good coverage of the topic, public and industry awareness levels are high, as strong industry associations (e.g. GSMA) have tackled the problem. Solutions are available along with the necessary guidelines and documentations. The only issue remaining is the adoption/implementation of the proper measures at a larger scale.

More than 84% of our respondents are applying different analysis techniques for SS7 interconnect traffic in order to detect abnormal activities. In particular, over 50% of the respondents mentioned that traffic inspection is done at STP[30] or HLR[31] level, which is the right approach. Inspecting at STP, owing to its central nature, provides a global view of SS7 traffic, and inspecting at HLR ensures home subscribers attacks are detected. Nevertheless, there is still room for improvement, as we do consider these measures belonging to a basic protection level (they only prove checks were made without mentioning how sophisticated the checks were).

More than 80% of the respondents monitor for abnormal SMS activities. Cat 1 messages (according to GSMA FS.11 classification) are monitored by 76% of the respondents while Cat 2 & 3 by roughly 43%.

Over 90% of the respondents mentioned having the ability to react to malicious traffic by applying different techniques. Some operators are able to redirect traffic and some others already blacklist SCCP Global Titles[32], which emit malicious traffic. In addition, SS7 messages that should not be expected at interconnect level, are properly mitigated. Moreover, messages not expected for home subscribers or inbound roamers are also mitigated.

Another important aspect is that providers usually have few signalling experts, and in most of the cases are not part of the SOC teams, IT security teams or security/fraud departments. Further efforts need to be done in this area to increase the awareness/knowledge of such issues within the security & fraud teams.

SS7 attacks can be complex as attackers are gaining more and more knowledge and as they had the time to develop effective attack scenarios. A basic protection will cover probably the majority of the attacks but will leave room for the complex or targeted attacks that can really cause damage at social, economic or political level (e.g. espionage etc.).

As a conclusion, we can mention that in terms of SS7 minimum security measures are adopted by the majority of the providers. This conclusion is also reinforced by industry, through different industry papers, findings or other materials. Nonetheless, one problem arises from the fact that basic security measures are providing only a basic level of security. Also, SS7 infrastructure is quite old in some cases and not all equipment supports the adoption of

[30] Wikipedia: A Signal Transfer Point (STP) is a router that relays SS7 messages between *signalling end-points* (SEPs) and other signalling transfer points (STPs).
[31] Wikipedia: The home location register (HLR) is a central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network.
[32] Wikipedia: SCCP Global Titles is the equivalent for IP addresses. The Signalling Connection Control Part (SCCP) is a network layer protocol used in Signalling System 7 telecommunications networks. A global title (GT) is an address used in the SCCP protocol for routing signalling messages

security measures, not even the basic ones. This is also confirmed by the technical and cost related constraints explained in section 2.1.4.

2.3 Considerations on Diameter

Industry's focus on Diameter security has come later[33] than in the SS7 case, and has certainly not reached maturity yet. Diameter is derived from RADIUS (Remote Authentication Dial-In User Service) and provides an authentication, authorization, and accounting protocol for computer networks[34]. In terms of design, it has borrowed many concepts from SS7, along with its vulnerabilities. Being a purely IP based protocol, there is an increased risk in the possibility of an intruder gaining access through hacking. [35] The more knowledge the attacker has on Internet related protocols the more chances they have to succeed.[36] This makes it in theory, simpler to exploit than SS7.

Nevertheless, existing research[37] indicated that, Diameter is currently less exploited than SS7. Actually, no respondent has mentioned seeing real attacks; nevertheless, there are recent developments indicating their appearance[38]. The exact reason for this must be further investigated but could be related to the narrow adoption of Diameter worldwide, to the fact that attackers did not have the necessary time to prepare the attacks or to the fact that SS7 provides already satisfying results. Nevertheless, its vulnerabilities have been documented and theoretically exploited by the security community[39].

According to our research, 60% of the respondents inspect interconnect traffic, either fully or partially. A large part of operators does not monitor Diameter interconnect at all, possibly resulting in trivial Diameter attacks not being detected: attacks spoofing application ID are likely to work in most cases. It goes without saying that apart from basic attacks, also the advanced ones might not be detected and operators may not be able to identify malicious traffic.

In terms of reacting to malicious traffic 78% are able to respond by applying different techniques such as: dropping or redirecting potential malicious messages, negatively answering / closing transactions of malicious messages.

2.4 Considerations on 5G security

Note: The European Commission signed a landmark agreement with the '5G Infrastructure Association' on 17 December 2013, representing major industry players, to establish a Public Private Partnership on 5G (5G PPP). This is the EU flagship initiative to accelerate research developments in 5G technology. The European Commission has earmarked a public funding of €700 million through the Horizon 2020 Programme to support this activity. EU industry is set to match this investment by up to 5 times, to more than €3 billion euros. [40] In June 2017, as part of the phase 1 of 5G PPP project, a white paper from the Security Working Group has been published, containing an in-depth analysis of 5G security risks and challenges[41].

[33] https://www.theregister.co.uk/2017/12/08/diameter_protocol_security_shortcomings/
[34] https://en.wikipedia.org/wiki/Diameter_(protocol)
[35] https://www.ptsecurity.com/upload/corporate/ww-en/analytics/diameter_research.pdf
[36] http://labs.p1sec.com/2013/07/28/346/
[37] Cathal McDaid, Adaptive Mobile Security, Diameter Security research, presentation GSMA FASG #10, Jan. 2018. https://www.adaptivemobile.com/blog/measuring-the-diameter-protecting-4g-networks
[38] https://speakerdeck.com/yodresh/tids-a-framework-for-detecting-threats-in-telecom-networks
[39] https://www.blackhat.com/docs/eu-16/materials/eu-16-Holtmanns-Detach-Me-Not.pdf
[40] https://ec.europa.eu/digital-single-market/en/towards-5g
[41] https://5g-ppp.eu/new-security-group-5g-ppp-white-paper-phase-1-security-landscape/

Fifth generation mobile networks or 5th generation wireless systems, abbreviated 5G, are the proposed next telecommunications standards beyond the current 4G. 5G planning aims at higher capacity than current 4G, allowing a higher density of mobile broadband users, and supporting device-to-device, more reliable, and massive machine communications. [42]

"5G PPP Phase1 Security Landscape", the white paper published by the Security Working Group within the 5G PPP project mentions:

> *" The challenging traits of 5G networks to support novel and diverse business requirements of vertical sectors have rendered current network security approaches inadequate. For example, multi-tenancy in 5G networks, i.e. infrastructure sharing by multiple virtual network operators will require strict isolation at multiple levels in order to ensure absolute security. In 5G networks, reliability does not only refer to availability or up-time of the network infrastructure but also to ensuring high connectivity, infinite capacity and coverage (and other promised 5G features) anytime and anywhere. This implies a security makeover of how confidentiality, integrity, and availability will be maintained and managed in 5G networks. Furthermore, the already high complexity of securing a network and its services has scaled up another notch with the introduction of SDN and NFV in 5G networks, i.e., due to 'softwarization' and virtualization of networks and network functions. These are just a few examples of security challenges out of many that are anticipated in 5G networks. In addition, service specific security requirements also have to be considered as 5G ecosystem is anticipated to be service-oriented. For example, remote healthcare requires resilient and robust security while IoT demands lightweight security.*
>
> *5G must provide a security and privacy level higher or at least equal to the security and privacy level in 4G. That is, 5G must be able to deliver and maintain SLA to verticals in terms of: availability, security, resilience, latency, bandwidth, access control from an end to end perspective. Furthermore, 5G systems and components must provide strong mutual authentication and authorization and should not be negatively affected by the security of legacy systems with which it interworks.*
>
> *5G will be even more reliant on standards that previous mobile telecommunications networks, due to the expected broad impact on society and the number of ways in which 5G networks will interact with each other and with external systems. In order to minimize exposure to risks, security must be built in from the designing phases and not added on later as an add-on feature.*
>
> *WG Security standardization work should focus and work in order to provide a common agreement and joint contributions:*
>
> - *security requirements which can impact the entire 5G aspects (e.g. radio, core, services)*
> - *a minimal security baseline based on consistent technology and procedures by identifying the security functionality and mechanism required for 5G*
> - *security architecture design based on a the security baseline*
> - *added security functionalities which can be instantiated based on the specific service/contest*
>
> *3GPP is the key SDOs for 5G standardization and it is the main target for 5G-PPP projects, but also other Groups can be considered relevant, such as ETSI, IETF and ITU. Moreover, although not official SDOs, GSMA and NGMN will also play an important role as drivers for the 5G specifications across the industry.*
>
> *With regards to 5G signalling, 3GPP SA3/SA2 has introduced the Security Edge Protection Proxy (SEPP) in the 5G Architecture as the entity sitting at the perimeter of the PLMN network and terminating the signalling messages received from other PLMN (through IPX). The interconnection model will be then somehow*

[42] https://en.wikipedia.org/wiki/5G

equivalent to the existing one, with the Diameter Edge Agent acting as a proxy at the edge of the PLMN. And the security requirements for SBI (Service-based interfaces) will take into account the presence of this new functional entity. 3GPP standards are still under definition in the following groups:

- *3GPP CT3/CT4 are discussing the API/protocol issues.*
- *3GPP SA3 is defining the security requirements. "*

5G Security for core network is still under formation in 3GPP. Deeper aspects of IPX security, like IPX service provider usage and hop-by-hop routing and security might become part of later 3GPP releases.

Our survey included also one question about concerns regarding 5G security. According to the responses we received, one of the main concerns is that 5G signalling will incorporate the same vulnerabilities as Diameter. Pls. see figure below for more details.

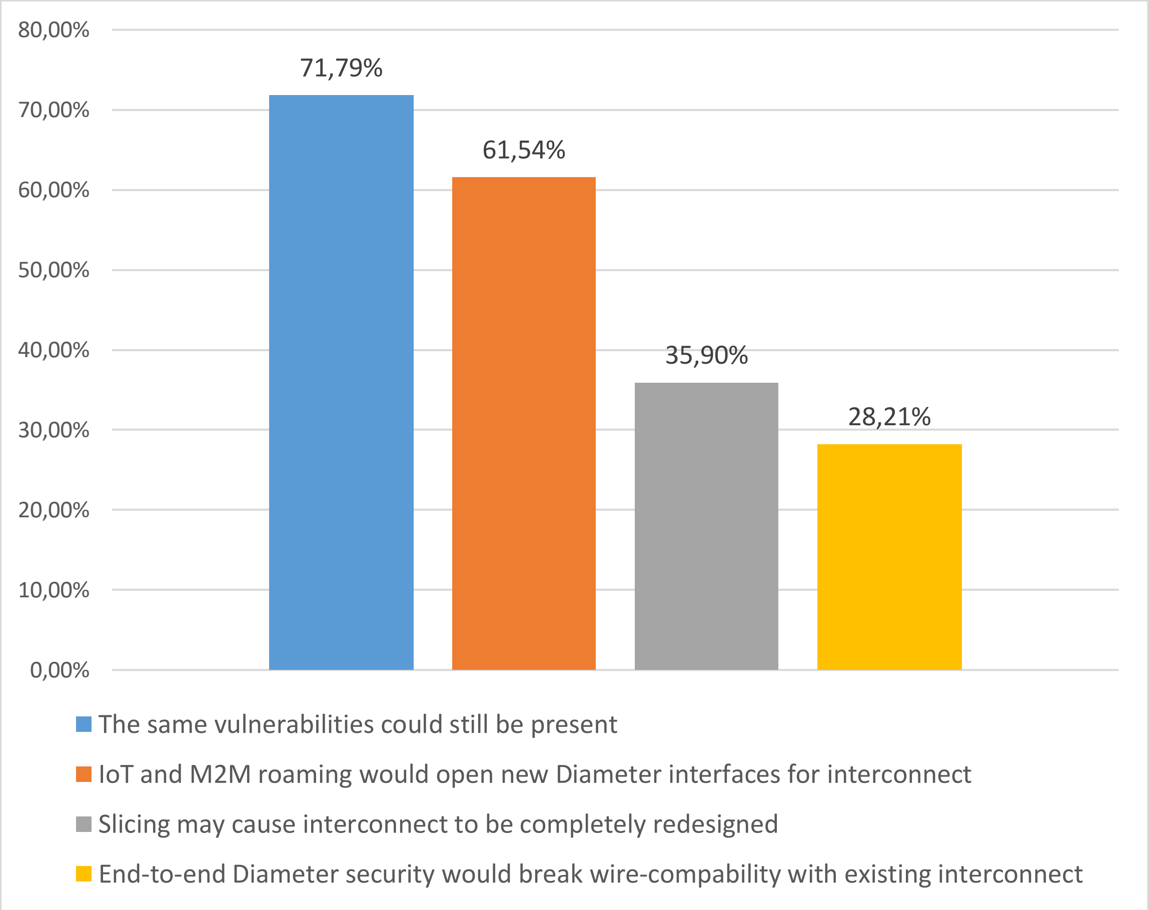


Figure 8 – 5G security concerns

This concern is shared also by industry. Although 5G standards are still in their infancy, with a planned complete 5G definition in 2019[43] [44], some companies have already rolled out and tested pre-versions of 5G[45] [46].

[43] http://www.3gpp.org/release-15
[44] https://www.fiercewireless.com/wireless/3gpp-declares-first-5g-nr-spec-complete
[45] http://www.telecomtv.com/articles/5g/25-mobile-operators-already-testing-5g-technology-14394/
[46] http://www.zdnet.com/article/intel-and-ericsson-work-on-5g-interoperability-across-3-5ghz/

Big telecommunication equipment manufacturers have published their concerns regarding 5G security [47] [48]. According to them 5G has to support new service delivery methods in order to sustain new business requirements coming from IoT and more bandwidth needed by customers. Its IT driven infrastructure will increase the attack surface resulting in an evolved threat landscape. New technologies that will be part of 5G, like Network Function Virtualisation (NFV), are also expected to bring new security concerns. Privacy assurance is an important aspect to be covered nowadays, especially in Telecom, as more and more industries are using mobile technologies as a business enabler.

Considering the above, the conclusion might be that special attention must be granted to 5G security. As mobile plays a huge role in our digital society, assuring our everyday digital infrastructure in support of the economy itself, the stakes are high. Older mobile generations have proven their drawbacks in terms security and the same approaches cannot be repeated anymore. As Diameter related vulnerabilities are beginning to be publicly uncovered the future use of this protocol or similar approached should be avoided. Carriers will need a new signalling architecture that can address the impact of introducing billions of roaming and static devices, the subscriber behaviour and bandwidth requirements, and new applications. [49]

Though not covered in the scope of this paper, additional security troubles may arise:

- Voice over LTE – the use of IMS to transport voice calls in 4G – requires the use of SIP and RTP. Research is available on how to track users based on SIP signalling[50]. While attacks based on SS7 and Diameter require an access to IPX / GRX, tracking using SIP has the benefit to achieve the same objective while using mobile data access.
- 5G current intention[51] is to break out from Diameter to use HTTP/2 as a base applicative layer. While it may add more functionalities, it will make the number of interconnects multiply accordingly. Attackers may draw benefits from multiple generations of interconnect to gain stealth abilities: attacks may span multiple interconnects, and remain undetected, until it is too late. Each interconnection must be properly monitored, and all interconnects may get to be monitored as a whole.
- 5G uses common "Internet" protocols like HTTP, TLS, and REST API. Vulnerabilities for those type of protocols are quickly discovered and exploits are integrated into all kind of penetration testing tools readily available. This implies that the grace period between vulnerability discovery and real exploitation will become much shorter compared to SS7 and Diameter.

[47] https://www.ericsson.com/assets/local/publications/white-papers/wp-5g-security.pdf
[48] http://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf
[49] http://www.netnumber.com/5g-world-improving-signalling-efficiency-security-iot-network/
[50] https://www.sstic.org/media/SSTIC2017/SSTIC-actes/remote_geolocation_and_tracing_of_subscribers_usin/SSTIC2017-Article-remote_geolocation_and_tracing_of_subscribers_using_4g_volte_android_phone-le-moal_ventuzelo_coudray.pdf
[51] http://www.3gpp.org/ftp/Specs/archive/29_series/29.891/29891-110.zip

3. Conclusions and recommendations

Telecommunications are key in nowadays societies. They represent the backbone, the primary infrastructure based on which our society works and it's the main instrument in allowing our democracy (and other EU core values such as freedom, equality, rule of law, human right) to function properly. As a consequence, here in ENISA (the EU cyber security agency) we consider assuring the security of our infrastructure as a top priority.

The present study has deep dived into a critical area within electronic communications, the security of interconnections (signalling). Based on the analysis, at this moment there is a medium to high level of risk in this area, and we do consider that proper attention must be granted by all stakeholders involved so as to find a proper solution.

As mobile technologies evolve so does the threat landscape. Early generations of mobile networks 2G/3G rely on SS7 and SIGTRAN, protocols designed decades ago, without giving adequate effect to modern day security implications. Nobody at that time envisioned the scale that mobile networks could reach in the future, so trust and security were not issues. Nonetheless at the moment we are still using this legacy protocol to assure the interconnection between providers. The industry and security research community has started covering the topic, by providing good practices and necessary tools. But still, a lot more has to be done. Basic security measures seem to be implemented by more mature providers, but these measures assure only a basic protection level. More efforts need to be made so that an optimal protection level is achieved.

Current telecommunication mobile generation (4G) uses a slightly improved signalling protocol called Diameter. Build with the same interconnect principles in mind but on an IP base, the protocol has been proved vulnerable. The industry is still trying to understand exact implications and to identify possible workarounds. Attackers are also in the same phase apparently. It is our impression that the next step will be made soon by all parties involved. As soon as SS7 becomes sufficiently protected their focus will change towards the new attack surface.

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. In addition, tools to scan and potentially attack mobile networks are now freely available[52].

5G, the new mobile generation, is still under development. Early releases from some manufacturers are available but the standards are still in their infancy. Nevertheless there is a certain risk of repeating history. Given the improvements that 5G will bring (more users, more bandwidth etc.) having the same security risks can be extremely dangerous.

Further actions are needed! Pls. see in the sections below some recommendations on possible further actions.

3.1 High level recommendations

Given the situation described above, we consider the following high level recommendations should be considered by the specified stakeholders:

For EU Commission:

[52] https://github.com/SigPloiter/SigPloit

1. ***Consider revising the current legal landscape so that signalling security is covered.***
   As explained in chapter 2.1.4 the current regulatory landscape influencing electronic communications providers might not fully cover signalling security and/or might prevent operators in adopting a proper protection level. Special attention should be granted in harmonising electronic communications related regulation. Currently different regulatory initiatives are affecting the Telecom industry (Electronic Communication Framework, ePrivacy Directive, GDPR etc.).
2. ***Consider the adoption of baseline security requirements for electronic communications providers to include signalling security.***
   Several applicable technical/organisational measures were described within this document. The only way in which adopting security measures in this area can benefit the whole EU telecommunication infrastructure is if the measures are adopted on a large scale. In this respect, it might make sense to have EU wide baseline security requirements for telecom providers that must include aspects regarding signalling security.
3. **Consider taking necessary measures to support the improvement of security for current legacy elements sustaining the EU telecommunication infrastructure.**
   As explained in sections 2.2 and 2.3 the current set of protocols used for signalling has certain weaknesses. Nevertheless, as the transition process towards new technologies takes place (mainly 5G) and taking into account that it might take many years until a wide adoption of 5G is achieved, actions should be taken to improve as much as possible the current vulnerable infrastructure elements. Allocating funds through H2020 or another relevant EU financing scheme towards improving signalling protection and/or develop proper protection tools for the private sector, might be one of the solutions.
4. **Thoughtfully supervise the implementation of the 5GPPP to cover also signalling security among the various tasks of the Security Working Group.**
   As mentioned in section 2.4, future signalling technologies and protocols should not be based on the same approached or repeat the same mistakes. In this respect, the EC should carefully supervise the 5GPPP Security Working Group objectives, so that the 5G signalling security part is cautiously considered.
5. **Further increase the international cooperation as a global effort is needed to overcome the threats.**
   Signalling security is a global issue and global attention should be granted. Having a secure infrastructure in EU might be undermined by other networks outside EU that have not adopted the same level of protection. More international cooperation is needed to reduce risk at an acceptable level.

For Art. 13 Expert Group and ENISA

1. ***Periodically analyse the situation to identify further developments.***
   As signalling security has been proven a sensitive area with a quite high risk level, ENISA and the national authorities should periodically supervise the situation. New attack scenarios or new vulnerabilities might be discovered and a close attention from responsible authorities is needed.

2. ***Consider publishing EU guidelines for assuring an advanced protection level at Member State level***.
   Signalling security is a topic falling under multiple regulatory initiatives (as explained in section 2.1.4) and this creates confusion when applying security measures. Also applying technical measures rises many difficulties for the carrier as additional elements or processes added to the network might affect functionality.
   Nevertheless, a level playing field should be achieved in EU so as a proper level of protection to be assured for subscribers at home and in roaming across EU.

For National Regulatory Authorities

1. ***Regularly analyse the national situation and be aware of any developments that can cause significant incidents in this area***.
   As signalling security has been proven a sensitive area with a quite high risk level, national authorities should periodically supervise the situation. New attack scenarios or new vulnerabilities might be discovered and a close attention from authorities is needed.

2. ***Consider revising the national legislation (if needed) so that signalling security should be covered in terms of reporting incidents and adopting minimum security requirements.***

For Industry

1. ***Electronic communication providers: adopt the necessary measures to ensure an adequate level of security and integrity of telecommunication networks.***
   Operators provide the main infrastructure for electronic communications. They are the first line of defence. Operators should adopt measures to assure an adequate protection level across EU. Section 2.1.3 provides a comprehensive view upon available good practices produced by GSMA. The adoption level of these guidelines should be increased.

2. ***Standardisation bodies: ensure security is covered properly within the new 5G standards.***
   5G will definitely bring improvements in terms of bandwidth and number of connected subscribers/devices. The attack surface will increase accordingly bringing more opportunities for attackers. In this respect, the future solutions should address security properly to remove as much as possible from the threat landscape.

3.2 Technical recommendations

The initial design of interconnect protocols has made security hard to implement in today's landscape. Several proposals to secure SS7 and Diameter have never been adopted by the industry (MAPsec, TCAPsec, Diameter over IPsec, Diameter over SCTP/DTLS). A good approach is to implement end-to-end security solutions, providing both confidentiality and integrity to sensitive exchanges, but at this point, there aren't any. GSMA has thus initiated a Roaming and Interconnect Fraud and Security (RIFS) subgroup studying possible ways to implement end-to-end interconnect security for LTE and 5G networks. 3GPP currently works at defining 5G, and operators have expressed their doubts about properly addressing current weaknesses at interconnect. IoT use cases requires to support 1 million devices per square km, which may dramatically rise the traffic at interconnect, and draw M2M (machine-to-machine) in the scope of security expectations. Operators are in general expecting than even in 5G, the same vulnerabilities could be still present, thus upgrading the infrastructure is not necessary a solution to the problem.

Ensure global and exhaustive monitoring of SS7 / Diameter / GTP. This encompasses capturing and detection capabilities. As threats evolve, this requires the function to be flexible enough to adapt.

Operators should be capable to protect against basic attacks. Addressing this point does not require the use of SS7 / Diameter firewall.

Operators should adopt SS7 / Diameter firewalling, which may be in the form of an add-on of their Internetwork Packet Exchange (IPX). Carriers may see here an opportunity to address security as a new business.

Development of specifications and standards for new mobile signalling elements such as SS7 firewalls or routers is an action where EU might be able to contribute. Further cooperation with main actors that are developing guidelines and recommendations, like GSMA, ITU, etc. is essential. Particularly, we can consider the establishment of baseline security measures for each category (3G/4G/5G) which NRAs will impose to their operators can help towards a more secure interconnection environment.

Promote communication between operators' CERTs/SOCs at EU level. Given the complexity of these incidents, more information sharing should happen at EU level between operators.

3.3 Good practices

The following table presents a categorization of common good practises.

CLASSIFICATION	MEASURES
Core measures: they are the minimum set of measures to detect attacks and compromises	Monitor all interconnect traffic Monitor core network elements Monitor outgoing traffic Hardening network nodes
Intermediate: they add security assurance to the core measures	Regularly perform external network security assessments and penetration tests Ensure liability and legality of responses to malicious traffic Analyse Interconnect messaging Advice carriers to adopt security options in their interconnect offers
Advanced: they enable to identify and mitigate yet unknown attacks	Redirect to captive environment Detect prequels to attacks Detect advanced attacks Deeply screen signalling messages

Annex A: Short technical description of interconnections in telecom

For a better understanding of the issues raised by this document it is important to briefly describe the fundamentals of interconnections. Understanding how mobile networks interoperate is important before exploring the issue further.

Mobile networks offer services to end users, which are typically:

- Messaging: short and multimedia messages;
- Voice calls, with supplementary services such as call forwarding;
- Data: access to the Internet or other private packet networks.

All these services are available in **mobility**. Users are usually able to make use of their services when travelling abroad. Roaming is the ability for subscribers to use their home services while attached to a visited network, different from theirs home networks. Note, that domestic roaming cases exist for various reasons, e.g. to benefit from a partner-operator radio coverage. Thus, it is important to make clear that roaming is not necessarily associated with traveling abroad.

When speaking about a roamer – a subscriber in roaming – we can distinguish between two scenarios:

- A subscriber is attached to a radio network different from his/her home network: he/she is an **outbound roamer.**
- A subscriber is attached to radio network, but it is not a local subscriber: he/she is an **inbound roamer**.

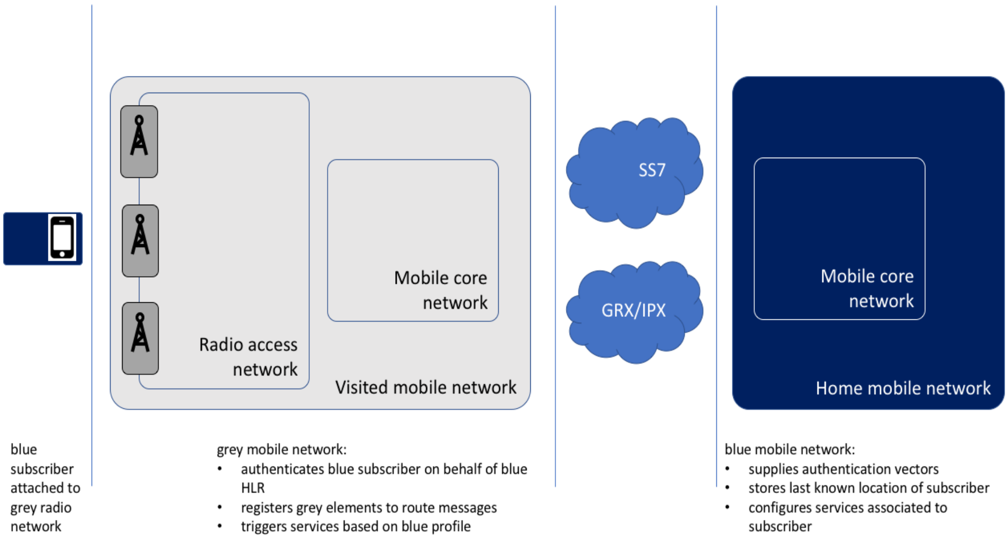

SS7
GRX/IPX
Mobile core network
Radio access network
Visited mobile network
Mobile core network
Home mobile network
blue subscriber attached to grey radio network
grey mobile network:
• authenticates blue subscriber on behalf of blue HLR
• registers grey elements to route messages
• triggers services based on blue profile
blue mobile network:
• supplies authentication vectors
• stores last known location of subscriber
• configures services associated to subscriber

Figure 2 – How visited and home networks interoperate when roaming

Figure 1, depicts how visited and home networks interoperate when a user is in roaming. All the subscriber profiles are located into the home operator's HLR (in blue). So, for the blue subscriber, the visited network (in grey), has to reach the blue operator, firstly to retrieve authentication vectors, and afterwards to correctly setup the requested services.

Main elements of mobile core network involved at interconnect are outline in Figure 2. The diagram is overly simplified, but it outlines the following entities:

- Home Location Register / Home Subscriber Server: it is a database that contains subscribers' profile, shared secret that is also located in subscribers' SIM card, and transient information such as current location of home subscribers.
- Visitor Location Register / Mobility Management Entity: a local database that contains parts of subscribers' profile who are currently attached to radio network. It consists in home profiles, and remotely setup profiles, retrieved from subscriber home HLR/HSS.

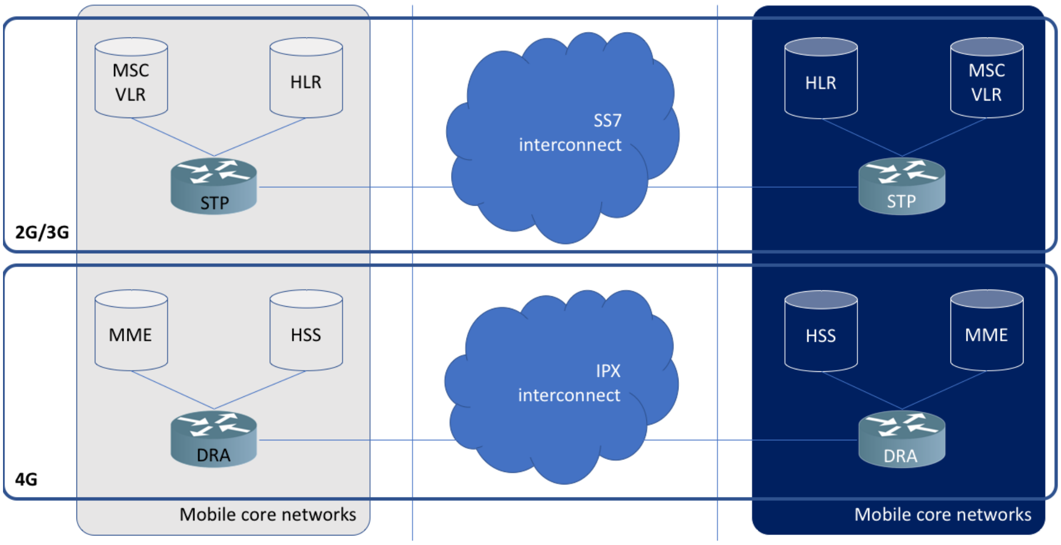


Figure 3 - Mobile networks interconnect main entities

Mobile operators have two ways to interconnect between them:

- **Direct bilateral agreement between two operators.** In this case, operators have the control to protect their link with the appropriate security measures.
- **Subscribe to an SS7 / GRX / IPX Carrier, which will interconnect to other mobile operators and to other carriers**. In this case, carriers may offer secured links, but traffic between them is only protected up to their boundaries. End-to-end security, between mobile operators, cannot be guaranteed.

Figure 3 illustrates the above-explained types of interconnections.

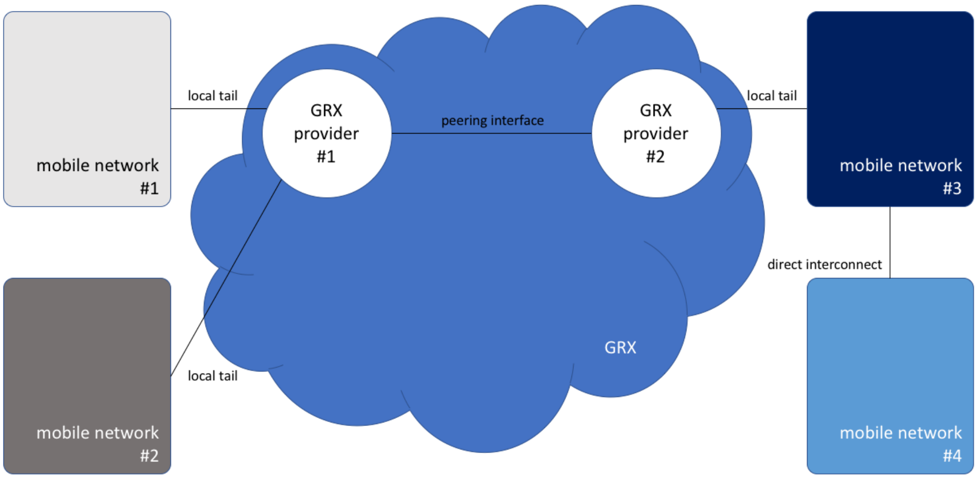


Figure 4 - Carriers connect mobile networks and carriers

ENISA
European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Catalogue Number: TP-01-18-302-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-252-3
DOI: 10.2824/38400