Mobile Telecommunications Security Landscape

February 2022

Contents

GSMA CTO Foreword

Now, more than ever, connectivity is key. Deployment of 5G networks must remain at the forefront of change as this next generation technology will stimulate digital growth, innovation and new levels of efficiency across industries. The mobile sector is committed to making a fairer, greener world supported by a thriving and resilient digital economy.

The mobile world is undergoing a number of fundamental transformations, whether it be the move to 5G, new services or cloud-based networks. Security is a key enabler to building in operational resilience that enables confidence, trust and growth.

GSMA has an important role in convening the industry, be that through world-class events like Mobile World Congress, driving innovation in digital technology to reduce inequalities in our world or developing new security mechanisms that enable new generations of mobile technology to be deployed securely. The GSMA, through its work on a wide range of security issues, has long played a significant role in this space.

There is much to do to ensure mobile networks are secure and operate in concert to provide mutual protection. I am delighted to introduce this latest GSMA Mobile Telecommunications Security Landscape Report that highlights some of the ongoing and recent threats in the mobile sector, before offering details on how GSMA members build security resilience into operational mobile networks.

Given the challenge, we will succeed by working together to develop and implement security best practices. Please take the time to read this paper and get involved in this team effort. Existing GSMA members can continue to contribute to our security work and are encouraged to apply GSMA security guidelines and recommendations within their businesses. Other interested stakeholders are welcome to get involved and they can do so by joining the GSMA, which will ensure access to a breadth of security advice and best practices.

Alex Sinclair
Chief Technology Officer
GSMA

Executive Summary

Welcome to the GSMA's 4th annual Mobile Telecommunications Security Landscape report. The report provides an overview of the significant security topics that GSMA see as important for the mobile industry.

This document aims to assist the mobile ecosystem to build stronger security resilience by presenting key security topics through a lens of first, the security threat, and second, the security response. Importantly, the document is positioned to communicate the extensive resources available from GSMA and the wider industry, that will inform any security response against these security threats. The document also demonstrates the ongoing value and difference GSMA is making to security of the mobile ecosystem.

The GSMA approach to building mobile network security resilience is highlighted before exploring a series of important security topics. For each security topic, the security threat is discussed before pointing to relevant GSMA security advice. GSMA offers its members considerable security[1] expertise and services through a range of activity areas that collectively build a knowledge base, guidelines and services that build stronger mobile network security resilience. The member-only[2] content can be accessed by joining GSMA as an Operator, Industry, Rapporteur or Sector member and then using GSMA's resources and extensive document repository. Additionally, complementary content is included on wider (non-GSMA) security best practice recommendations in key areas.

The security topics discussed in this report are categorised into a number of distinct groupings. These topics start at securing 5G and flow through enabling software and cloud topics before covering broader operational security aspects. Following this, two particular functional areas are explored (Internet of Things (IoT) and signalling security) before concluding on the broader supply chain topic. These categories consist of the following:

- Securing 5G
- Software including open source code
- Malware
- Cloud & virtualisation
- Operational Security
- IoT
- Signalling & Interconnect
- Supply Chain

Finally, the report recommends implementing existing advice, maintaining active contributions to building security guidance and seeking out opportunities to get involved.

[1] https://www.gsma.com/security/
[2] https://www.gsma.com/membership/membership-types/

Introduction

Modern mobile cellular networks support a wide variety of services that go well beyond providing basic voice and short messaging services. They now include the provision of high bandwidth communication with complex security requirements. As a result, their security architectures have evolved over successive generations to define an increasingly elaborate end-to-end security coverage.

Meanwhile, rapid evolution of mobile communications over the past decade has led to not only convergence of mobile and fixed network connectivity but also the exposure of mobile networks to new interfaces outside a network operator's control.

This document aims to assist the mobile ecosystem to build stronger security resilience by presenting key security topics through a lens of first, the security threat, and second, the security response.

It is important to consider the wider operating context in which operational mobile networks exist. There is a current (and increasing future) reliance that industry verticals place on mobile networks. This is likely to increase as advanced 5G services enable end-to-end network slicing. Mobile networks are also a potential attack vector into industry verticals (that themselves have industry-specific cyber security requirements). This broader context is explored in a range of interesting publications including:

- The US National Security Agency has published security advisory[3] papers identifying potential threat vectors to 5G infrastructure
- The European Union Agency for Cybersecurity (ENISA) Threat Landscape[4]
- The ENISA Supply Chain Threat Landscape[5]

This fourth edition of the GSMA Mobile Telecommunications Security Landscape report builds on the 2019, 2020 and 2021 reports to present an updated view of the evolving landscape.

THE GSMA'S DESIRE REMAINS TO ENHANCE AWARENESS AND ENCOURAGE APPROPRIATE RESPONSES TO SECURITY THREATS.

[3] https://www.cisa.gov/sites/default/files/publications/potential-threat-vectors-5G-infrastructure_508_v2_0%20%281%29.pdf
[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[5] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Building Mobile Security Resilience

The main purpose of a mobile network operator's security architecture is to provide security assurance characterised by the need to preserve three key attributes: Confidentiality, Integrity and Availability; often known as the 'security triad' or the simply the abbreviation 'CIA'.

In mobile network architectures, as data is processed, stored or transmitted to and from different components of a network or networks, maintaining the security triad throughout is of prime importance to ensure reliable end-to-end security protection.

GSMA offers its members considerable security[6] expertise and services through a range of activity areas that collectively build a knowledge base, guidelines and services that build stronger mobile network security resilience.

Fraud & Security Working Groups

The GSMA's Fraud and Security Group[7] (FASG) drives the association's management of fraud and security matters related to mobile technology, networks and services. The group has two primary objectives, firstly to maintain or increase the protection of mobile operator technology and infrastructure. And secondly, to maintain or increase the protection of customer identity, security and privacy such that the mobile industry's reputation stays strong and mobile operators remain trusted partners in the ecosystem. FASG provides an open, receptive and trusted environment within which fraud and security intelligence and incident details can be shared in a timely and responsible way. Members gain from the significant body of knowledge published on fraud and security matters. FASG has a number of sub-groups including the Fraud and Security Architecture Group, the Device Security Group, the Roaming and Interconnect Fraud and Security Group and the Security Assurance Group.

Securing the 5G Era[8]

5G has designed in security controls to address many of the threats faced in legacy 4G/3G/2G networks. These controls include new mutual authentication capabilities, enhanced subscriber identity protection and additional security mechanisms. 5G offers the mobile industry an unprecedented opportunity to uplift network and service security levels. 5G provides preventative measures to limit the impact of known threats, but the adoption of new network technologies introduces potential new threats for the industry to manage. GSMA explores a range of security considerations including secure by design, 5G deployment models and 5G security activities (see Securing 5G section later in this paper).

Telecommunication Information Sharing and Analysis Center

The GSMA T-ISAC[9] is the central hub of security information sharing for the telecommunication industry. Driven by the ethos "One organisation's detection is another's prevention", we believe information sharing is essential for the protection of the mobile ecosystem, and the advancement of cybersecurity for the telecommunications sector. Drawing on the collective knowledge of mobile operators, vendors and security professionals, the T-ISAC collects and disseminates information and advice on security incidents within the mobile community – in a trusted and anonymised way.

Coordinated Vulnerability Disclosure Programme

The GSMA CVD[10] programme gives security researchers a route to disclose a vulnerability impacting the ecosystem affording the industry an opportunity to assess the impact and mitigation options before details of the discovered vulnerabilities enter the public domain. We work with mobile operators, suppliers and standards bodies to develop fixes and mitigating actions to protect customers' security and trust in the mobile communications industry.

[6] https://www.gsma.com/security/ and member-only resources
[7] https://www.gsma.com/aboutus/workinggroups/fraud-security-group
[8] https://www.gsma.com/security/securing-the-5g-era/
[9] https://www.gsma.com/security/t-isac/
[10] https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

CASE STUDY: Cryptanalysis of the GPRS Encryption Algorithms GEA-1 and GEA-2

Research was submitted to GSMA's CVD Programme which identified weaknesses in two GPRS Encryption Algorithms (GEA1 and GEA2) allowing an eavesdropping attack using a false base station. Despite support being prohibited by 3GPP specification releases over the last decade, a majority of devices (including modern/flagship devices) continued to support GEA1.

The responsible disclosure of the research findings provided time for GSMA, GSMA members and the wider industry to prepare for this research to be released.

The advance notice allowed the industry to issue updates to relevant standards to ensure the removal of GEA1 from devices in the field and new devices, as well as to update test cases for new devices to test for non-support of GEA1. Within a week of the public release of the research, 3GPP standards were updated for devices conforming to older specification releases to not support GEA1 and GEA2.

Changes were also made to the following GSMA Permanent Reference Documents:

- Addition of GEA1 field trials test case to GSMA's Device Field and Lab Test Guidelines (TS.11)
- Change Network Settings Exchange default settings in GSMA's Technical Adaptation of Devices through Late Customisation (TS.32)
- Updated advice in GSMA's Security Algorithm Deployment Guidance (FS.35)

All of these change activities were undertaken by GSMA to ensure the compromised GPRS encryption algorithms are removed from devices to protect mobile users.

Security Accreditation Scheme

The Universal Integrated Circuit Card (UICC) in mobile devices, and its associated applications and data play a fundamental role in ensuring the security of the subscriber's account and related services and transactions. The GSMA's Security Accreditation Scheme[11] enables mobile operators to assess the security of their UICC and Embedded UICC (eUICC) suppliers, and of their eUICC subscription management service providers.

Network Equipment Security Assurance Scheme

The Network Equipment Security Assurance Scheme[12] (NESAS), jointly defined by 3GPP and GSMA, provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines security requirements and an assessment framework for secure product development and product lifecycle processes, as well as using 3GPP defined security test cases for the security evaluation of network equipment.

NESAS provides a security baseline to evidence that network equipment satisfies a list of security requirements and that the equipment has been developed in accordance with vendor development and product lifecycle processes that provide security assurance. NESAS is intended to be used alongside other mechanisms to ensure a network is secure. The scheme has been designed to be used globally as a common baseline, on top of which individual operators or national IT security agencies may want to define additional security requirements.

GSMA Security Publications

The GSMA security website[13] includes a number of informative and instructive publications, whilst GSMA members can exclusively access additional content specifically addressing a wide range of fraud and security topics.

[11] https://www.gsma.com/security/security-accreditation-scheme/
[12] https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[13] https://www.gsma.com/security/

Securing 5G

GSMA's aim for 5G is for it to be secure and resilient in operation. 5G presents an important opportunity for the mobile industry to enhance network and service security both as inherently designed within the network functions as well as through deployment strategies. New authentication capabilities, enhanced subscriber identity protection and additional security mechanisms will result in significant security improvements over legacy generations.

As of Q3 2021:[14]

- 5G was commercially available from 107 operators in 47 markets worldwide
- 5G trials were undertaken at 217 operators in 100 markets
- User adoption was at 135 million connections
- Mobile 5G connections are set to reach 1.8 billion connections by 2025

This rollout period is a pivotal time, as the approach taken to implement and operationalise the architecture and underlying technologies presents a significant opportunity to leverage the security opportunities afforded by the secure by design 5G standards, both within the core ecosystem as well as interoperable non-mobile services. Good operational hygiene, secure configuration and continued focus on security in operation are also key.

The 5G Security Landscape

Analyses of the 5G security landscape have been performed that help inform the likely threat stance. GSMA's 5G Security Guide (FS.40 – available to GSMA members) contains an overview of the security aspects and capabilities of 5G networks. The document serves as an educational resource for GSMA members that describes the security enhancements and capabilities inherent in 5G technology and highlights a range of implementation considerations for network operators.

It is important to recognize that 5G capabilities are likely to co-exist with previous generations of mobile infrastructure for some time. In which case, both existing and new infrastructure will need to be secured. An FCC Communications, Security, Reliability and Interoperability Council (CSRIC) report[15] identifies risks to 5G from legacy vulnerabilities and recommends best practices for mitigation.

There is a high degree of correlation on the key topic areas identified across publications from a number of industry bodies (including the FCC, 3GPP) and these also reflect many of the topic areas addressed in this GSMA Mobile Telecommunications Security Landscape report.

These areas include:

- The cloud-native nature of 5G
- The range of attack vectors
- The threat to the network stack
- The threat to data in-transit, in-use or at rest
- The threat to the integrity of infrastructure
- The security of software defined networks and functions
- Open source software in 5G networks
- IoT in the context of 5G
- Roaming
- Sufficiency of security measures
- The 5G supply chain
- Security of management and signalling planes

[14] GSMAi Statistics: Global 5G Landscape Q3 2021
[15] https://www.fcc.gov/file/18918/download

INDUSTRY INSIGHT:

umlaut[16] reports on some common issues observed in the course of conducting air interface security assessments on 5G networks. Each identified gap offers a security threat that can be mitigated with suitable controls.

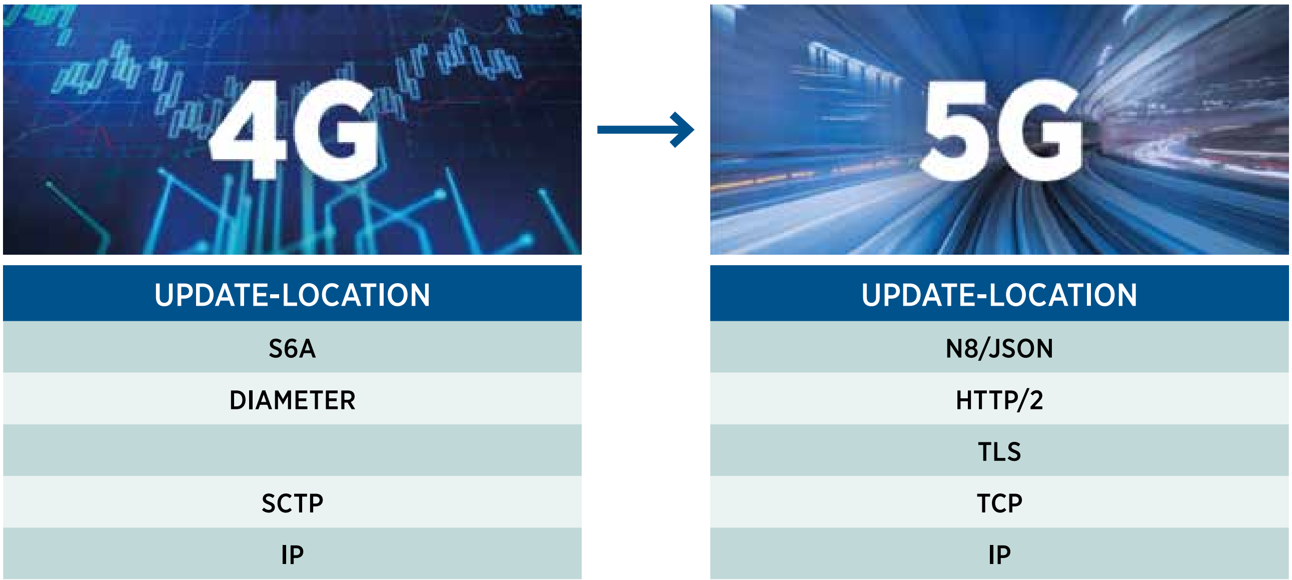
- 5G Stand-Alone and Non-Stand Alone: Confidentiality protection (encryption) is not enabled in all locations on the radio network (user plane). Thus, users on parts of those networks cannot benefit from encryption on the radio communication.
- 5G Stand-Alone: User Plane Integrity Protection (UPIP) is not enabled. It could result in traffic redirection / intercept attacks
- 5G Stand-Alone: Identity protection of the users (SUPI concealment) is not enabled. Location tracking attacks are still possible on those networks
- The temporary identifiers (GUTI / TMSI) are – in some deployments – not randomized (often incremental)
- Lack of security on slices / APNs. Traffic between users is allowed and reachability to core elements is possible from a 5G user perspective

The 5G Security Response

Historically, operator networks have mainly used proprietary protocols for network management. 5G Core (5GC) moves to an IP-based protocol stack, allowing interoperability with a wider number of services and technologies in the future. The following protocols, schemas and processes will be adopted in 5GC (see Figure 1):

- HTTP/2 over N32, replacing Diameter over the S6a reference point
- TLS as an additional layer of protection providing encrypted communication between all network functions (NF) inside a Public Land Mobile Network (PLMN)
- TCP as the transport layer protocol as replacement of the Stream Control Transmission Protocol (SCTP) transport protocol
- RESTful framework with OpenAPI 3.0.0 as the Interface Definition Language (IDL)

Figure 1: 4G to 5G Security Enhancements



UPDATE-LOCATION	UPDATE-LOCATION
S6A	N8/JSON
DIAMETER	HTTP/2
	TLS
SCTP	TCP
IP	IP

[16] http://umlaut.com/en/contact-us

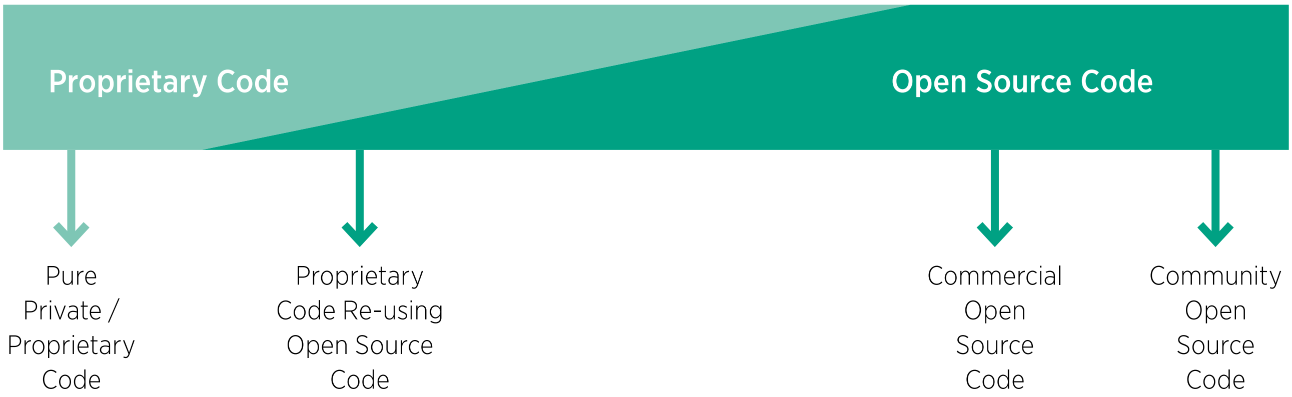
As these protocols are used in the wider IT industry, their use will likely:

- Lead to a short vulnerability to exploitation timeline, and higher impact of vulnerabilities located within these protocols
- Expand the potential pool of attackers. 4G and especially 3G core networks benefit from attackers having little experience or familiarity with the proprietary standards used within them

5G offers the mobile industry an unprecedented opportunity to uplift network and service security levels. These controls are discussed and assessed at GSMA Securing the 5G Era[17]. The GSMA has collated this analysis into a 5G Cybersecurity Knowledge Base[18] to provide useful guidance on a range of 5G security risks and mitigation measures.

The GSMA's 5G Security Task Force (5GSTF) is responsible for monitoring work on 5G security, within GSMA and across the wider industry and the standards development community, with a view to ensuring all necessary enablers are in place to deliver secure and resilient operational networks. In particular, the taskforce focuses on potential gaps between standards and operational implementations and the resolution of those.

Figure 2: A Range of Software Development Arrangements


Proprietary Code
Open Source Code
Pure Private / Proprietary Code
Proprietary Code Re-using Open Source Code
Commercial Open Source Code
Community Open Source Code

[17] https://www.gsma.com/security/securing-the-5g-era/
[18] https://www.gsma.com/security/5g-cybersecurity-knowledge-base/

Software Security

Software is fundamental to the delivery of mobile communications networks both in proprietary form and, increasingly, open source. The telecommunications industry uses software from the open source community in a range of architectural deployments, including to provide virtualised middleware, as a software component running on virtualised infrastructure or within proprietary code implementation. Malicious software (malware) and ransomware (explored in the next section) have the potential to pose a significant risk.

The Software Security Threat

The threat of poorly written code, or the deliberate insertion of malicious code, that could be used to compromise network operation, data or service features is a concern. Software vulnerabilities can be observed in a range of code types as illustrated below in Figure 2.

All varieties of code types can contain vulnerabilities. Open source code can be noted in a wide range of code development including complete modules, libraries, utilities and partial code re-use. For proprietary executable code, the vendor will typically provide all the development resources (coders), and follow their own company-specific software development coding practices but is not typically open for inspection from outside of the vendor. For open source developed code, the main focus is typically to deliver the required functionality. Development processes can vary but open source code is available for detailed inspection.

A list of the most commonly exploited vulnerabilities was published in a Joint Cybersecurity Advisory[19] by the CISA. The document provides details on the top 30 vulnerabilities—primarily Common Vulnerabilities and Exposures (CVEs)—routinely exploited by malicious cyber actors in 2020 and those widely exploited in 2021. The vulnerabilities allowed a range of undesirable actions including arbitrary code execution, arbitrary code reading, path traversal, remote code execution and escalation of privilege.

INDUSTRY INSIGHT:

Regular cloud solutions security testing conducted by umlaut[20] has found a lack of software validation in network systems deployed in production: e.g. software images not being signed, signatures not being verified during installation and acceptance of software images. Additionally, the integrity and protection of software images are not enforced. Certificate based authentication and integrity protection of images is rarely delivered so it cannot be guaranteed that the software being installed is the same version that was created by the vendor. Finally, reverse engineering of some telco software images undertaken means it is possible to uncover hardcoded accounts and passwords from the system which can remain used in production systems. Credentials were able to be extracted which may allow an attacker to access and manipulate the images remotely. Note: All issues found during this testing have been reported in a coordinated way.

[19] https://us-cert.cisa.gov/ncas/alerts/aa21-209a
[20] http://umlaut.com/en/contact-us

The Software Security Response

The GSMA recommends that a secure Software Development Life Cycle (SDLC) is implemented. This lifecycle should include quality control stages, with code review at module and system level, including both static and dynamic testing. Code language choice considers security issues such as type safety and vulnerable functions. An example of the recommended controls includes the objective to prevent Mobile Edge Compute (MEC) applications from attacking the MEC platform / virtualization / hardware layer, recognising that applications may contain malicious code and/or abuse their privileges. Note: MEC should be viewed like a public cloud with similar adversaries and attack vectors. This objective is met through a series of controls including:

1. Block local application deployment except for emergency cases
2. Block installation and execution of unsigned applications
3. Scan workload images/packages continuously for malicious components and/or misconfigurations and/or known vulnerabilities
4. Workloads should execute with least privilege access
5. Isolate workloads, by using multi-layered isolation between workloads and MEC platform to prevent workloads escaping the process sandboxes
6. Isolate workload resources, specifically compute, memory, storage and network
7. Separate MEC control and management networks from workload networks, and utilise confidentiality, integrity and replay protection mechanisms to prevent bypass / isolation break-out and spoofing/ injection into MEC platform internal functional domains
8. Prevent direct pass-through, and malicious workloads that may bypass MEC policies
9. Utilise dedicated resource allocation for local MEC services
10. Deploy workload protection tools at the host to identify and prevent abnormal activities by workloads
11. Prevent workloads and/or services from performing memory/process/kernel dumps
12. When executing workloads with lightweight virtualisation technologies (e.g. containers), ensure that the associated processes enable data execution prevention, address space layout randomisation and stack protection to reduce the ability of malicious workloads from escaping the process sandbox
13. Use true random number generators for cryptographic operations to minimise the ability of applications to predict and or influence cryptographic operations by MEC

The availability of a current Software Bill of Materials (SBOM) is a key measure in building an effective response to software vulnerabilities and CVEs, implementing bug fixes and code enhancements. A strong SBOM provides detailed knowledge of the composition of code including modules that may have been re-used so that it is easier, for example, to understand whether a given CVE applies to the versions of code in-use. There is emerging documentation on this approach, notably from the National Telecommunications and Information Administration (NTIA) who have recently published a report[21] on the minimum elements for an SBOM covering data fields, automation support and practices & processes.

A GSMA report[22] has identified a range of developing controls and described them within the contexts of systems, component and infrastructure. Combining these systems and component level considerations can build a framework for considering the design and operation of open networks.

[21] https://www.ntia.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

[22] https://www.gsma.com/futurenetworks/resources/open-networking-the-security-of-open-source-software-deployment/

Malware

2021 evidenced a range of notable malicious software (malware) attacks including ransomware.

The Malware Security Threat

Malware attacks have been noted covering a range of targets including devices, device applications and infrastructure. The following is a view of some mobile malware attacks seen during 2021:

- CDRThief[23] is a malware threat that targets specific Linux platformed Voice over IP softswitch systems with an aim to access Call Data Records (CDR)
- GriftHorse[24] is a Trojan hidden in malicious apps that targeted Android devices and subscribed unwitting users to premium rated services
- SharkBot[25] is an Android banking trojan that allowed fraudsters to steal sensitive banking credentials and information
- PhoneSpy[26] is an advanced remote access trojan designed to conduct surveillance of Android users and send data to a command and control server
- Android.Cynos.7.origin[27] is one version of the Cynos software modules embedded in Android apps to collect user information and to display advertisements
- AbstractEmu[28] is Android device rooting malware that was hidden in malicious apps to allow attackers assume control over infected devices
- TangleBot[29] is advanced SMS malware that uses COVID-19 lures to expose users to risks of data exfiltration, device control and account theft
- Flixonline[30] is a malicious app that masqueraded as a Netflix viewer spread via WhatsApp using the auto-reply feature by responding to all incoming messages to steal credentials
- Matryosh[31] is a distributed denial of service botnet that re-uses Mirai to target Android device users via a diagnostic and debugging interface
- Qualcomm Mobile Station Modem[32] exploits a software vulnerability in Qualcomm chips to infect Android devices to provide hackers with access to user conversations and messages

In addition to the list above, there has been a significant increase in reported ransomware attacks. A recent report[33] identified the biggest ransomware attacks in 2021. These included reported ransomware attacks on ExaGrid (a backup storage vendor), an attack on Taiwan-based PC manufacturer Acer and the Colonial Pipeline attack[34], leading to gasoline shortages across the Eastern United States. Flubot (see later case study) was particularly prevalent in the mobile industry. It was reported[35] that the operators of the ransomware REvil launched a ransomware attack on the telecommunications company MasMovil. TT Network, the joint mast operation of Telia Denmark and Telenor Denmark, was reportedly[36] hit by a ransomware attack. This range of examples show that no business sector is immune to the malware threat.

[23] https://malware-guide.com/blog/new-cdrthief-malware-targeting-linux-voip-softswitches-to-record-call-metadata
[24] https://www.theregister.com/2021/09/29/grifthorse_trojan_android/
[25] https://thehackernews.com/2021/11/sharkbot-new-android-trojan-stealing.html
[26] https://www.zdnet.com/article/a-stalkers-wishlist-phonespy-malware-destroys-android-privacy/
[27] https://www.theregister.com/2021/11/25/huaweis_appgallery_games_targeting_children/
[28] https://www.theregister.com/2021/11/01/in_brief_security/
[29] https://www.zdnet.com/article/this-new-android-malware-gets-full-control-of-your-phone-to-steal-passwords-and-info/
[30] https://www.technadu.com/new-android-malware-spreading-via-whatsapp-auto-replies/262967/
[31] https://thehackernews.com/2021/02/beware-new-matryosh-ddos-botnet.html
[32] https://gridinsoft.com/blogs/qualcomm-mobile-station-modem-vulnerability/
[33] https://www.techtarget.com/searchsecurity/feature/The-biggest-ransomware-attacks-this-year
[34] https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/
[35] https://cyberthreatintelligence.com/news/spanish-telecom-giant-masmovil-hit-by-revil-ransomware-attack/
[36] https://commsrisk.com/ransomware-attack-on-danish-telco/

The UK telecom regulator, OFCOM reported results of a scams survey[37] that highlighted significant ‘smishing’ ongoing with seven in 10 people (71%) saying they have received a suspicious text. Smishing is a combination of phishing and SMS where the aim is to try to trick users with messages that appear to be legitimate alerts from banks.

‘SIMjacker’[38] is a security vulnerability affecting some SIM/UICCs that contain a legacy software program called the S@T browser. It is intended to allow services to be run, based on SIM Toolkit commands.

The exploit makes use of commands to report a user’s location or device identity to the attacker’s device, without a user’s action or knowledge. The exploit could also be used for fraud (sending SMS/making calls), or other actions such as opening a specific site on the device’s web browser. The attack only succeeds if the SMS message reaches the target device. Network operators can filter SMS messages based on characteristics including message origin and message header information.

CASE STUDY: Flubot

Evidence of the Flubot banking malware was first brought to the attention of the GSMA T-ISAC[39] community by a member operator in March 2021, where Indicators of Compromise (IoCs) consisting of malicious URLs and domains were shared on the threat intelligence platform.

Flubot is a blended attack combining smishing and voicemail lures with banking malware injects. It indiscriminately targets mobile users, with the greatest impact on Android devices that have enabled side-loading of apps, but iPhones are not entirely immune. Although Europe has been the focus of this highly infectious malware, the campaign moved to Australia in August 2021 and a T-ISAC member confirmed the infection had spread to New Zealand in late September 2021. By late November 2021 several European members continued to witness new variants of the campaign, with new activity identified by operators in Finland.

The main objective of the Flubot malware, once downloaded and installed on victim devices following smishing enabled social engineering, is to obtain accessibility privileges/full access to the device. The malware then detects banking and cryptocurrency applications on the device and superimposes fake overlay windows when the applications are opened to capture credentials and credit card details that are sent to a botnet command and control server. Flubot is also able to intercept messages and application notifications.

The infection method follows typical malware infection patterns:

1. The victim receives a malicious SMS with a URL link.
2. The victim opens the URL link that downloads a malicious application.
3. The application is downloaded and installed. (With user unwittingly ‘approving’ application requests for privileges).
4. The malware gains access to the victim’s contact list and sends the same malicious SMS to those contacts.

Predictably, as new Flubot variants were discovered, new tactics were identified and discussed in the T-ISAC chat forum. Voicemail lures, fake Flubot security alerts and WhatsApp ‘credit card phishing’ via age verification emerged as examples of new methods to entice mobile users.

The impact of Flubot on mobile network operators and their customers can vary and be felt in different ways, including the following:

1. Personal disruption and emotional harm to victims – most victims being older and/or vulnerable
2. Deterioration of confidence in SMS as a channel for business and customers
3. Financial harm – initially to customers, and then to the operator as they issue refunds for fraud losses
4. Wider reputational impact for the operator as customers perceive that they have failed to protect them
5. Consumption of resources in Operator customer relationship management and fraud teams.

GSMA’s T-ISAC service allowed members to discuss Flubot related issues in real time which benefitted the network operator response. Valuable information has been shared since its creation including new threat actor tactics, movement of Flubot to other regions, best practice and mitigation, message bodies for feedproxy URLs, signposts to Flubot presentations, webinars and open-source publications and T-ISAC Member reports.

[37] https://www.ofcom.org.uk/news-centre/2021/45-million-people-targeted-by-scams
[38] https://simjacker.com/
[39] https://www.gsma.com/security/t-isac/

The Malware Response

The GSMA has produced extensive coverage of defence mechanisms and the recommendations include:

- Device level: Bundle optional anti-virus software with devices to prevent infection and propagation of mobile malware. Encourage device manufacturers to protect end-users against malicious code by collaborating with security solution vendors to develop and install anti–virus software
- Deploy malware detection and blocking solutions within the network using anti-virus or content filtering solutions
- Deploy technical solutions to detect and block inbound SMS spam to the network
- Operators should ensure that when procuring devices from manufacturers they specify the default state of the device to be one that is correctly configured to provide the best protection from malware
- Exchange information between operators, vendors and software security firms on new malware threats. This helps operators to perform risk assessments and put alerting mechanisms in place to provide users with information on new mobile malware.
- Educate customers on mobile malware threats and remedies directly and through dealers and retailers. Advice to customers includes checking the detail of the text for any details that don't seem right, avoid clicking on suspect links and reporting suspicious texts to their network operator
- Build a "Security Conscious Customer Base" by helping customers take responsibility for protecting themselves
- Implement a fraud management system or signalling monitoring rules to detect unusual behaviour
- Prevent the use of exploits by educating customers about the consequences of jailbreaking or rooting mobile devices

In addition to the aforementioned recommendations, the following resources are helpful:

- The GSMA Operator Guide to Mobile Malware (SG.19 – a member document).
- UK NCSC Guidance: Mitigating malware and ransomware attacks[40]
- CISA Advisory aimed at stopping ransomware[41, 42]
- The Ransomware Guide[43] includes advice such as:
  - Maintaining offline, encrypted backups of data and to regularly test your backups
  - Create, maintain and exercise a basic cyber incident response plan
  - Conduct regular vulnerability scanning to identify and address vulnerabilities
  - Regularly patch and update software and OSs to the latest available versions
  - Ensure devices are properly configured and that security features are enabled
- NIST have released a draft ransomware risk management profile: The Cybersecurity Framework Profile for Ransomware Risk Management, Draft NISTIR 8374[44]

[40] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[41] https://www.cisa.gov/stopransomware
[42] https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware
[43] https://www.cisa.gov/stopransomware/ransomware-guide
[44] https://csrc.nist.gov/publications/detail/nistir/8374/draft

Cloud & Virtualisation Security

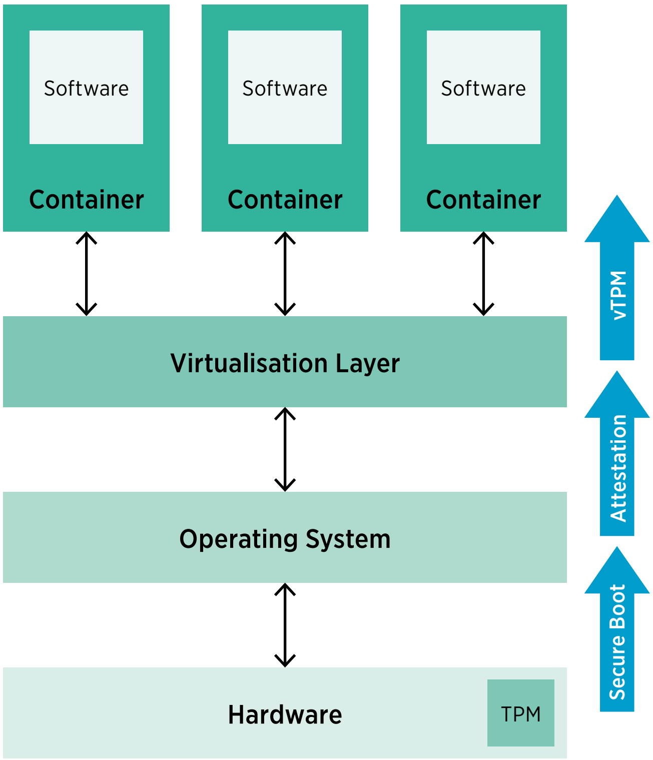
The Cloud & Virtualisation Security Threat

With the implementation of 5G, we are seeing a migration to cloud computing. As a result of this, security considerations that were once the responsibility of the network vendor, may become that of the operator. Since the software is now able to run on a range of non-proprietary platforms, operators need to ensure that whichever combination of hardware and software they use it must be secure. This includes ensuring that the software used is up to date, is running on original and authentic hardware and has been unaltered. To ensure this integrity, a chain of trust, anchored by a secured root is required to ensure that every component is working as intended as illustrated in Figure 3.

Although virtualised networks bring a range of opportunities and benefits, including network slicing, network scalability and greater flexibility of vendor choice, they also introduce a range of potential security threats. For example, unauthorised cross-communication between components such as containers, hardware-based threats, hypervisor threats and attacks on APIs. For virtual machines (VMs), the hypervisor is important software that allows one host computer to support multiple guest VMs by virtually sharing its hardware resources, such as memory and processing.

All cloud workloads have the potential to be compromised by a single compromise of the virtualisation layer. Virtualised workloads which have different trust levels may be consolidated onto a single physical host without sufficient separation.

Figure 3: A Layered Chain of Trust



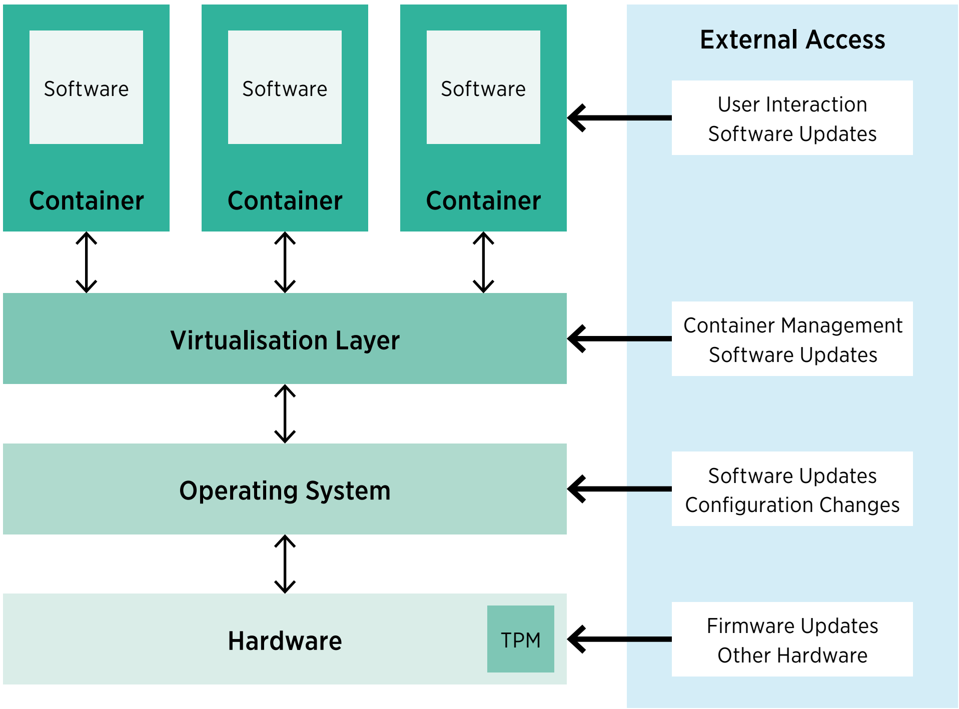
Beyond the network itself, we also need to consider how the management of the network is secured, and how a root of trust is established within the network. The management plane is one of several external systems which can access the network, and is responsible for managing the different layers of the cloud infrastructure and applying any updates to these layers.

Figure 4 shows ways in which external systems may access various aspects of the cloud infrastructure. Any entity which can access the management plane also has the opportunity to disrupt it.

Infrastructure security is important as it underpins Mobile Edge Compute, core networks, OpenRAN and corporate cloud services.

The transition of operator network environments to the cloud creates significant changes to the security operations and management of these networks, as well as to the type and capabilities of security controls. Assets are no longer placed at a fixed location (physical box) with planned capacity and long life cycles. Instead the solution stack relationship changes dynamically, and with it, the network traffic of the physical and virtual switches. This increases the complexity of monitoring the compute, storage and network properties of each component as they are no longer statically bound. Furthermore, the lifespan of such entities gets shorter to serve a workload for a few minutes after which it is decommissioned. In case of compromise there is a need to track not only the alignments of virtual/physical assets, but also the relationship between assets as well as the historic allocations of these assets as they moved within the platform.

Figure 4: Visualisation of External Interaction with the Cloud Network

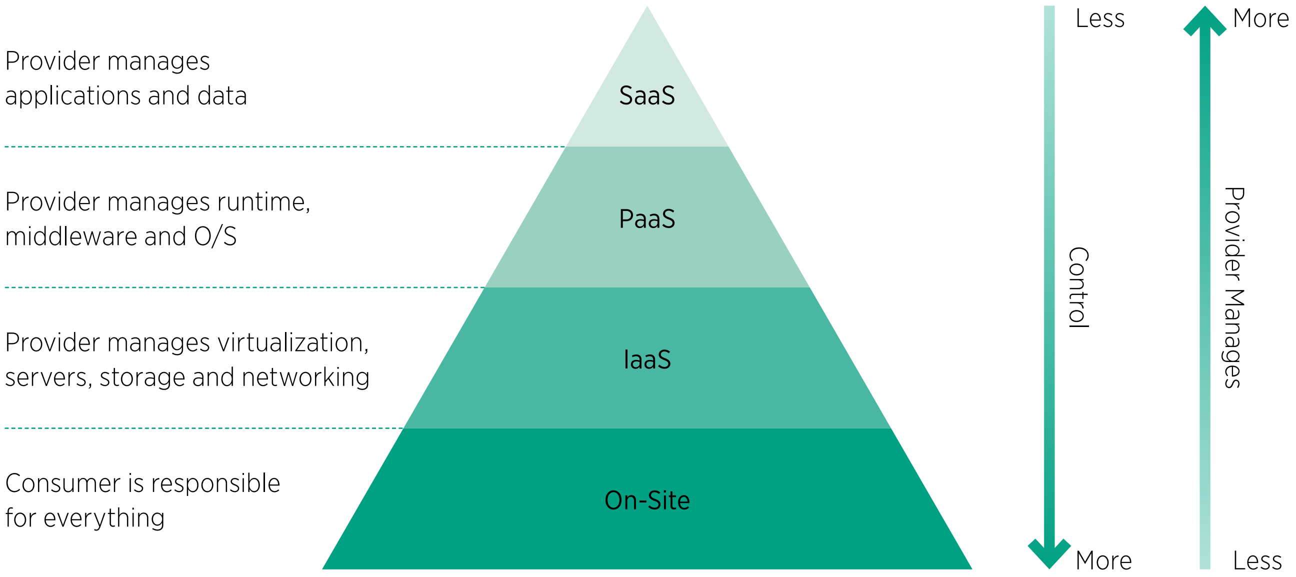


As the industry moves from the traditional approach of dedicated hardware to a cloud-orientated approach, the number of options for infrastructure grows. Typically, modern infrastructure options can be classified into one of four groups: Software as a Service (SaaS); Infrastructure as a Service (IaaS); Platform as a Service (PaaS); and on-site infrastructure. These form a sliding scale of options ranging from the entire product being hosted in the cloud, through to every element being owned and managed by the operator.

Figure 5 illustrates the relationship between each of the models, with lower levels giving the operator more responsibility and control and the higher levels offering the potential to outsource some security controls. As discussed in a later section, these supply chain arrangements provide their own set of attack threats.

Not shown in the diagram, is Network-as-a-Service (NaaS), where the network operator customers consume network services hosted by cloud providers. NaaS can provide a range of network functions including virtual private networks, appliances and load balancers.

Figure 5: Visualisation of the Relationship Between Infrastructure Models. Each Layer Possesses all of the Responsibilities of the Layers Above


Provider manages applications and data
SaaS
Provider manages runtime, middleware and O/S
PaaS
Provider manages virtualization, servers, storage and networking
IaaS
Consumer is responsible for everything
On-Site
Less
Control
More
More
Provider Manages
Less

The Cloud & Virtualisation Security Response

The virtualised network opens up many new possibilities in terms of dynamic scaling and redistribution of resources on demand. Ideally, this should be automated to the highest possible degree and allow the various network functions to grow and shrink capacity dynamically to adapt according to network load and requirements. This means that the deployment of new network elements can be managed with minimal human interaction and that unused, or end of life resources, may be retired automatically. The Network Function Virtualisation (NFV) deployment model will free up human resources for other tasks and also provide an energy efficient network infrastructure that may limit stress on equipment and increase the lifespan of the underlying hardware.

Theoretically, any network element or function may be virtualised. HLRs (Home Location Registers) or MMEs (Mobility Management Entities) are examples of complex network functions that could be delivered as a single, virtual, consolidated appliance. GSMA's Network Function Virtualisation Threats Analysis[45] (FS.33) provides a comprehensive overview of the threats related to NFV and the underlying infrastructure and platforms hosting the NFV. Importantly, it also includes extensive guidance on appropriate risk controls.

These controls act to build a bottom-up security approach including physical, geographic, architectural, hardware, software, data, storage, networking and management & orchestration controls. The bottom-up approach is important, as it acts to preserve the integrity of the solution through the establishment of a root of trust chain. This can ensure the correct workload code is running through the correct virtualisation platform through operating system security functions to any underlying trust arrangements and the underlying hardware.

The GSMA recommends a number of network operation controls, including virtualisation controls, to be applied to the MEC component with the objective to protect the MEC platform from executing code on compromised virtualisation infrastructure (i.e., IaaS) and hardware. Recommended actions include:

- Verify hardware and virtualisation layer integrity during boot
- Verify all underlying layer loaded modules against a good baseline (measured boot), alert and block loading of unauthorised modules
- Alert/block unsigned module installation and/or deployment to prevent secure boot bypass
- Install host-based detection probes at HostOS and virtualisation layers with rootkit detection capabilities with secure remote monitoring to identify and mitigate dynamic attacks (malware/ rootkits)
- Periodically re-initialise the MEC from the hardware layer to minimise the impact of non-persistent attacks (in-memory) and restore the system to a good known state, by a secure measured boot, and evaluate the system only during boot phase

[45] https://www.gsma.com/security/resources/fs-33-network-function-virtualisation-nfv-threats-analysis/

There is close working between the Linux Foundation's project Anuket[46] & the GSMA's Open Infrastructure Task Force (OITF)[47]. The resulting GSMA document NG.126 Cloud Infrastructure Reference Model[48] specifies a virtualisation technology agnostic (Virtual Machine (VM)-based and container-based) cloud infrastructure abstraction and acts as a "catalogue" of the exposed infrastructure capabilities, resources and interfaces required by the workloads. Additionally, a Cloud Infrastructure Reference Architecture focused on OpenStack as the Virtualised Infrastructure Manager (VIM) was chosen based on the criteria laid out in the Reference Model. OpenStack has the advantage of being a mature and widely accepted open-source technology. It has a strong ecosystem of vendors that supports it, and is widely deployed by the global operator community for both internal infrastructure and external facing products and services. This means that operators have existing staff with the right skill sets to support a Network Function Virtualisation Infrastructure (NFVI[49]) deployment into development, test and production. The security requirements include content on:

- Cloud Infrastructure and VIM security
- System Hardening
- Platform Access
- Confidentiality and Integrity
- Workload Security
- Image Security
- Security Life Cycle Management
- Monitoring and Security Audit

The Center for Internet Security (CIS)[50] has useful benchmarks for a range of platform approaches including Google Cloud, Oracle Cloud, Microsoft Azure, Kubernetes, Docker, Amazon Web Services, Red Hat Linux, VM Ware and Ubuntu Linux. These benchmarks can be used to validate that cloud infrastructure is configured as securely as possible. There are open source[51] and commercial[52] tools that can check environments against the recommendations defined in the CIS benchmark to identify insecure configurations.

[46] https://anuket.io/

[47] Accessible via GSMA OIFT Working Group

[48] https://www.gsma.com/newsroom/wp-content/uploads//NG.126-v1.0-2.pdf

[49] https://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-INF001v010101p.pdf.

[50] https://www.cisecurity.org/resources/page/4/?type=benchmark

[51] Eg https://github.com/docker/docker-bench-security

[52] See https://www.cisecurity.org/cis-controls-supporters/

Operational Security

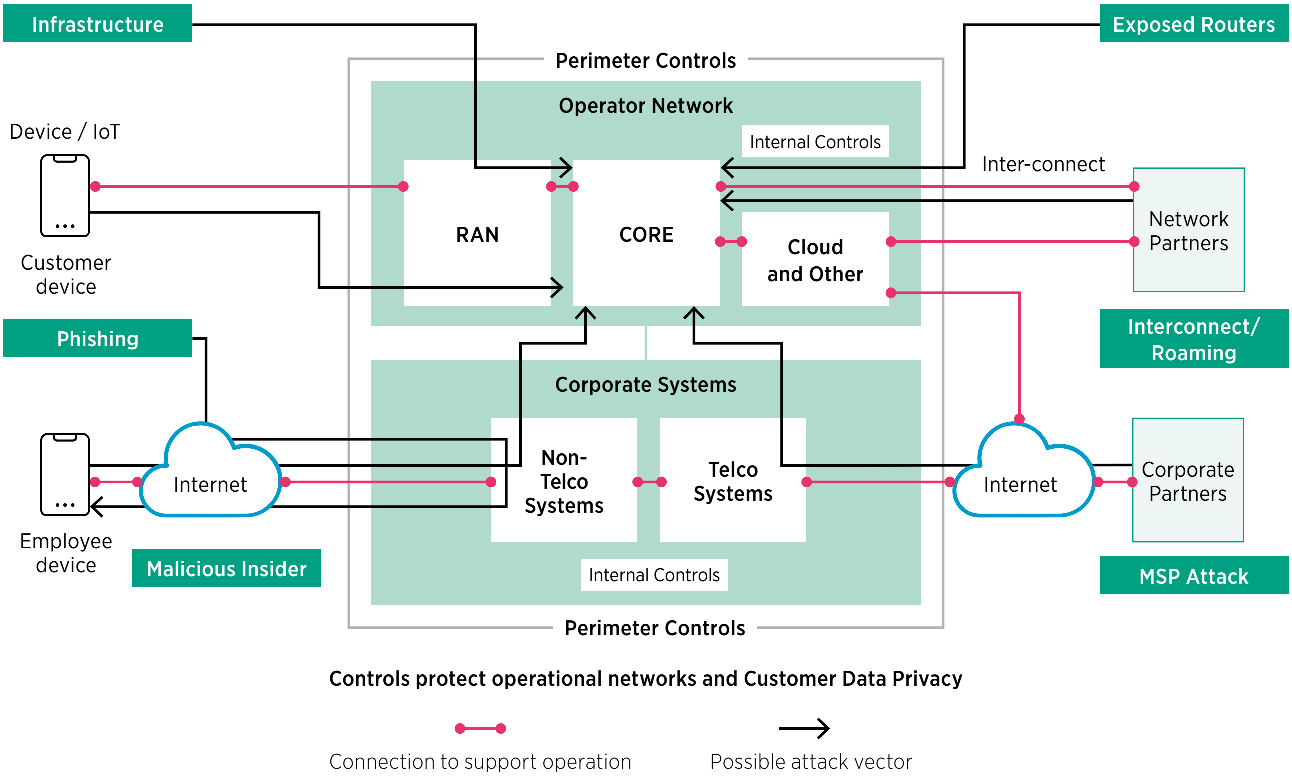
The Operational Security Threat

To administer and manage an operational mobile network there is a wide set of telecommunications and information technology (IT) systems (shown below in Figure 6) to be maintained. In addition to telecoms infrastructure, there are a range of corporate information technology systems that enable broader business operations as well as software for supporting customers which include billing systems and enterprise client dashboard and control systems. The internal corporate systems include intranet, email, instant messaging and staff systems such as accounting and sales systems. These systems are accessed by a range of employee devices and used by the full range of staff functions including the system administrators for the operational network.

A range of wider corporate partner connections are commonly in place to provide access to wider IT and cloud services and can also provide access to the operator network to enable managed service providers. Any connection between the operator's corporate systems and the telecommunications network can provide a pivot attack point into the mobile network from the corporate infrastructure and security solutions will need to include both perimeter and internal controls. It is essential to protect both the operational mobile network and associated IT systems as they are both a threat vector for potential cyber-attack. This topic explores the need for ongoing security controls for both operational and supporting IT systems.

A wide range of attack vectors can be identified when considering the complete system of both operator network(s) and the associated corporate IT systems (see Figure 6).

Figure 6: Potential Security Attack Vectors



There are a number of attack vectors and each requires strong security controls and processes to minimise the threat and impact of any attack:

- **Phishing Attacks:** Well-engineered and styled phishing attacks continue to have a finite success rate in penetrating perimeter defences. Consequently, anti-phishing campaigns and well architected internal network controls making lateral movement more difficult are important requirements.
- **Malicious Insider / Compromised Access:** In a similar manner, internal controls, least privilege and strong authentication make it harder for a malicious insider to gain traction.
- **Managed Service Provider Attack:** Remote compromise of a managed service provider offers a potential attack vector. Strong vetting, least privilege and trust domains form part of any defence.
- **Inter-connect / Roaming / Internet Signalling and DDoS Attack:** The exploitation of control signalling as an attack vector that is comprehensively documented and attracts significant attention in GSMA member security documents[53] and is explored in more detail in a later section of this report.
- **Exposed Routers and Servers:** A network operator will have a significant estate of vendor equipment, router and server infrastructure. It is important to have a strong grasp of the inventory of equipment in order that it can be managed and protected. This is particularly true for any internet-exposed management interfaces. Legacy equipment can use protocols with limited in-built security. These exposed interfaces must be configured to use secure protocols or have additional security controls such as VPN protection to reduce the likelihood of success for an adversary attack. This applies to virtualised deployments in the same sense, in that bare metal compute, storage and network devices must be protected. Additionally, unused management protocols, internet services and accounts can be disabled to limit attack opportunities.
- **Infrastructure Attack:** Physical attack of network infrastructure, such as at cell sites, retail outlets or data centres.
- **Device Attack:** With increasing access bandwidth and a range of malware attacks on devices, protection must be considered against device-based network attacks (e.g. signalling 'storms', Denial of Service attacks, IoT compromises) back into the network. Additionally, devices themselves may be subject to individual attack.
- **Supply Chain (not shown on diagram):** Where equipment/software experiences interference in the process of supply/deployment. This also includes where third party service providers may also be exploited to then compromise the network operator[54] or to access sensitive account systems.
- **Social Engineering (not shown on the diagram):** Where attempts are made to obtain account access by changing account details, accessing security credentials or to influence key individuals (e.g. 'whaling' attacks on senior executives).

[53] GSMA Documents FS.11 and FS.19

[54] https://www.solarwinds.com/securityadvisory

Fraudulent SIM Swap Overview

SIM swap is a legitimate service offered by mobile operators to allow customers to replace their existing SIM with a new one. A SIM swap may be required in the following circumstances:

- A SIM is lost, stolen or damaged;
- A different sized SIM is needed for a new device;
- The customer is porting out their number to a different network.

While SIM swap is a necessary and useful service, it has provided an opportunity for fraudsters to obtain and utilise the replacement SIM card to gain access to users' financial and wider service accounts. Two-factor authentication is commonly used by financial institutions to provide safe and secure services to customers. One of the most common two-factor authentication methods sends one-time passwords to the account holder's mobile number. Social engineering of call centre staff is an ongoing issue for all organisations that are required to service users directly. This form of "account takeover" is seen in many different sectors. With the prevalence of publicly available information available on the internet for most people, building up a legitimate picture of a user can be done with relative ease or with some initial social engineering against the user themselves. If a fraudulent SIM swap is completed successfully, it enables the fraudster[55] to receive authentication messages, calls and one-time passwords from the financial service provider of the victim. This allows those carrying out fraudulent activity to send money from the banking and mobile money accounts of the victim. Network operators and end customers can also lose the use of their devices and incur wider additional costs outside of the direct cost of this fraud.

GSMA's Fraud Manual FF.21 (available to GSMA members only) contains advice on countering fraudulent SIM swapping. Advice includes having an equal level of customer validation for new and existing customers, education and training of sales/dealer staff and to consider implementing GSMA Mobile Connect[56] in order to authenticate users.

An adversary may use the operational communications network as an attack vector to industry verticals. Previously, there has been less evidence of the adversary attacking the actual communications infrastructure, possibly because the communications infrastructure itself is required to be operational to enable an onward attack. This is not always the case though and there are increasing signs[57] of more direct attacks on operator networks. This can be viewed as a further example of a supply chain attack, with the network operator being in the supply chain to the target. These attacks may be aimed at extracting customer or billing data, committing fraud, testing network defences or in extreme circumstances, such as a war, launching direct attacks to disable and disrupt national communications. Any successful attack against an operational communications network that disrupts availability, confidentiality and/or integrity can be seen to have a force multiplier effect that impacts communications and the supported industry vertical(s).

The Verizon 2021 Data Breach Investigations Report[58] investigates data breaches across a range of industries. One, of many, noteworthy changes this year is the increase in rank of desktop sharing as the cause of a data breach, particularly given the link between corporate systems and the operational network can be an attack vector, especially on administrator accounts.

Additionally, the Trend Micro Report[59] summarises the characteristics and threats and contains recommendations to improve the security posture of enterprises' and telecommunications companies' IT infrastructure.

[55] https://www.gsma.com/aboutus/workinggroups/what-is-sim-swap

[56] https://www.gsma.com/identity/mobile-connect

[57] https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/

[58] https://www.verizon.com/business/resources/reports/dbir/

[59] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/islands-of-telecom-risks-in-it

The Operational Security Response

The GSMA recommends core network management controls. Some examples of the security objectives are shown below:

- There should be processes for the secure provisioning and decommissioning of users to ensure only legitimately subscribing customers have access to services
- Protect core network traffic after it is handed over from the radio path to protect against unauthorised interception and alteration of user traffic and sensitive signalling information
- Prevent eavesdropping, the unauthorised deletion and modification of voicemail content, settings and greetings and call break out to generate fraudulent traffic
- Use customer anonymisation techniques to protect identifiers that can be used to identify and track individual customers
- Prevent unsolicited messaging traffic reaching unsuspecting customers and causing potential harm to the network, including denial of service attacks against network elements
- Control which devices can access the network to protect against the connection of counterfeit, stolen and substandard devices and possible network impacts they may have
- The processes and tools used to ensure secure access to critical assets (e.g. core infrastructure)

Further controls covering Network Infrastructure are shown below :

- Security Network Function Virtualisation Infrastructure (NFVI) controls
- Virtualisation controls
- Network controls
- Storage controls
- Management controls
- Container controls

A wide range of controls, such as those for Network Operations control, include:

- Actively manage (inventory, track and correct) all hardware devices on the network
- Establish, implement and actively manage (track, report on, correct) the security configuration of network equipment
- Virtualisation/containerisation controls should be enforced
- Manage the ongoing operational use of ports, protocols, and services on networked devices in order to minimise windows of vulnerability available to attackers
- Continuously acquire, assess and act on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers
- Monitor and analyse core, radio and enterprise network traffic for potential internal or external attacks
- Ensure certificate issuing authorities are managed correctly
- Ensure database services and systems are protected from unauthorised access and misuse
- Implement cloud security principles for all private, public and hybrid cloud (infrastructure, platform or software) computing based provisioning
- Utilise centralised patching software, orchestrate and control patch deployments, and define patch deployment policies
- Implement misconfiguration detection and prevention

Controls for Security Operations include:

- Collect, manage, and analyse audit logs of events
- Control the installation, spread, and execution of malicious code at multiple points in the network
- Utilise open source information (OSINT) and other contextual information to increase awareness of the threat landscape
- Protect the organisation’s information, as well as its reputation, by developing and implementing an incident response infrastructure
- Perform security assessment of live systems to test the overall strength of an organisation’s defence (the technology, the processes and the people) by simulating the objectives and actions of an attacker (‘red teaming’)
- Implement a holistic protective monitoring approach that ensures there is a proactive and consistent approach to detection of abnormal behaviour on networks and systems

IoT Security

IoT offers the vision of a hyper-connected world where billions of connected objects and people seamlessly interconnect, exchanging data and making insightful decisions using artificial intelligence for the benefit of both individuals and society as a whole. IoT services are already widely adopted today across automotive, consumer electronics, enterprise, healthcare, industrial, smart buildings, smart cities, smart homes and utilities.

To support this market, IoT-centric connectivity is becoming mainstream, including low-power-wide-area technologies such as LTE-M (Long Term Evolution for Machines) and NB-IoT (Narrowband IoT), and local area wireless technologies such as Bluetooth LE, Zigbee and Z-wave. 5G networks (which encompass LTE-M and NB-IoT) which support massive machine type communication (mMTC), ultra-reliable low-latency communications (URLLC) and ultra-high device densities which will further accelerate IoT market growth.

IoT services are expected to rapidly grow across all industry sectors. According to the latest GSMA Intelligence IoT market update[60], the number of IoT device connections across all IoT markets is forecast to exceed 37 billion devices by 2030. This figure including all types of IoT devices, from all industry sectors and covering both consumer and enterprise applications.

The IoT Security Challenge

IoT services present security challenges not only due to the scale and breadth of the services, but also due to the critical functionality that many IoT services provide, with many services performing safety critical functions and leveraging private information. These factors, amongst others, make IoT services high value targets for potential attackers who wish to exploit these services, for example, to launch DDoS attacks, extract sensitive private data, or disrupt critical services. Additionally, there exists a relatively large legacy estate of older IoT devices with limited in-built security protections.

[60] https://data.gsmaintelligence.com/research/research/research-2021/iot-market-update-assessing-disruption-and-opportunities-forecasting-connections-to-2030

Recent IoT Attack Examples

Many wide scale attacks on, or leveraging, IoT services have been documented over recent years, with incidents such as the Mirai botnet DDoS attack and various Automotive-centric vulnerabilities making headlines in the mainstream media. Over the past 12 months, new attacks have been reported which serve to demonstrate that the IoT security landscape is evolving and the fundamental security weaknesses present within many IoT devices and services still persist. A few example issues reported in the past 12 months serve to emphasise these points:

- **Security challenges in underlying IoT technology enablers persist. For example:**
  - The 'BrakTooth' vulnerability[61], which was found to affect the Bluetooth software stacks within several major System on Chip providers, is a good example of a vulnerability within a generic IoT technology enabler that could leave billions of IoT devices vulnerable to malicious code injection. Full technical details on the vulnerabilities can be found on the dedicated BrakTooth website[62].

- **Security issues in consumer IoT devices are still widespread, examples of which include:**
  - Unauthenticated remote code execution (RCE) vulnerability in Hikvision IP camera[63]
  - Critical RCE vulnerability related to the web service of the Annke N48PBB network video recorder[64]
  - Unauthenticated RCE on Motorola Halo+ baby monitor[65]
  - A conference call speaker STEM Audio Table vulnerability unauthenticated RCE, which could allow eavesdropping on conversations[66]

- **Security vulnerabilities within Routers remain a major issue, examples of which include:**
  - A Cisco RV34X Router weakness allowing authentication bypass and system command injection, both in the web management interface[67]
  - A NETGEAR DGN-2200v1 series router critical security issue[68] related to accessing the router management pages using authentication bypass and deriving saved router credentials via a cryptographic side-channel.
  - TP-Link 4G routers being used as a botnet to abuse SMS services[69]

The IoT Security Response

Security guidelines, such as the IoT security guidelines[70] issued by the GSMA, have been available for several years and provide a comprehensive guide to IoT service providers. Since their initial publication the guidelines, together with other security resources, are now referenced within international standards including ETSI EN 303 645[71] and NISTIR 8259. In turn, these standards are now being leveraged by regulators, and IoT services providers' will soon be required by law to implement key security requirements in many markets. At the time of writing, IoT security legislation and regulations are being progressed and implemented in multiple countries and regions across the world including Australia, China, Europe, India, Singapore, USA and the UK.

Operating a vulnerability disclosure scheme is a core component of the IoT security lifecycle and is seen as one of the top product security recommendations for IoT companies in the ecosystem (GSMA operates the CVD scheme for industry-wide issues with mobile network connected technologies and services).

[61] https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/09/braktooth-bluetooth-vulnerabilities-crash-all-the-devices/
[62] https://asset-group.github.io/disclosures/braktooth/
[63] https://watchfulip.github.io/2021/09/18/Hikvision-IP-Camera-Unauthenticated-RCE.html
[64] https://www.nozominetworks.com/blog/new-annke-vulnerability-shows-risks-of-iot-security-camera-systems/
[65] https://randywestergren.com/unauthenticated-remote-code-execution-in-motorola-baby-monitors/
[66] https://blog.grimm-co.com/2021/06/the-walls-have-ears.html
[67] https://www.iot-inspector.com/blog/advisory-cisco-rv34x-authentication-bypass-remote-command-execution/
[68] https://www.microsoft.com/security/blog/2021/06/30/microsoft-finds-new-netgear-firmware-vulnerabilities-that-could-lead-to-identity-theft-and-full-system-compromise/
[69] https://therecord.media/botnet-abuses-tp-link-routers-for-years-in-sms-messaging-as-a-service-scheme/
[70] https://www.gsma.com/iot/iot-security/iot-security-guidelines/
[71] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

GSMA IoT Security Guidelines and Assessment

Developed with the support of the mobile industry, the GSMA IoT Security Guidelines[72] and associated IoT Security Assessment[73] scheme provide guidance and expertise to help IoT developers and service providers address the challenge of securing IoT services.

These resources provide recommendations for the secure design, development and deployment of IoT services and provide a mechanism to evaluate security measures. They address all parts of a typical IoT service covering server side components and APIs, communication networks and device endpoints.

The GSMA security guidelines are being leveraged by international standards and over the past 12 month these standards have further evolved:

- ETSI has released a companion test specification to the ETSI EN 303 645 consumer IoT security standard. This test specification, ETSI TS 103 701[74] will allow IoT service providers to assess their compliance to the standard using self-assessment or a test lab.
- The NIST cybersecurity program for IoT[75] now provides a range of guidance including information for IoT device manufacturers[76] through the NISTIR 8259 series of reports covering consumer IoT cybersecurity[77]. This guidance extends their risk management process to include IoT and defines IoT security requirements (NIST SP 800-213) using an accompanying catalogue (NIST SP 800-213A).[78]

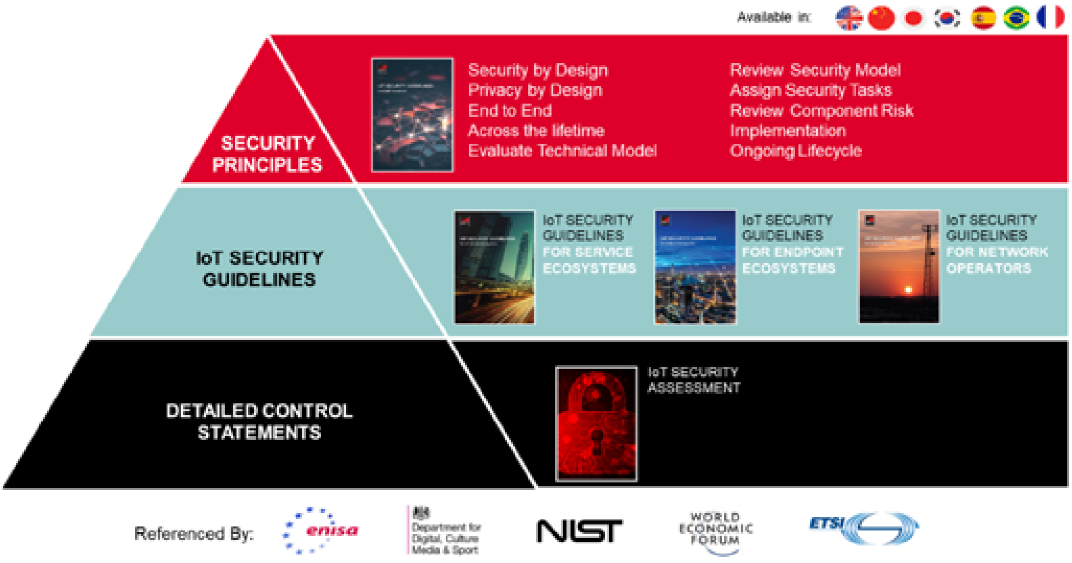
GSMA IoT SAFE

Leveraging hardware secure elements, or 'Roots of Trust', to establish end-to-end, chip-to-cloud security for IoT products and services is a key recommendation of the GSMA IoT Security Guidelines.

Developed by the mobile industry, IoT SAFE[79] (IoT SIM Applet For Secure End-2-End Communication) enables IoT service providers to leverage the SIM (including eSIM and iSIM) as a robust, scalable and standardised hardware Root of Trust to protect end-to-end data communications.

The solution is described in a recent GSMA whitepaper[80], which describes how the SIM can be leveraged as a root-of-trust to secure IoT device-to-cloud communications using TLS/DTLS, the world's most popular application layer security protocols.

Figure 7: GSMA IoT Security Guidelines and Assessment Scheme



[72] https://www.gsma.com/iot/iot-security/iot-security-guidelines/
[73] https://www.gsma.com/iot/iot-security-assessment/
[74] https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
[75] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program
[76] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series
[77] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/consumer-iot-cybersecurity
[78] https://csrc.nist.gov/news/2021/updates-to-iot-cybersecurity-guidance-and-catalog
[79] https://www.gsma.com/iot/iot-safe/
[80] https://www.gsma.com/iot/wp-content/uploads/2021/06/IoT-SAFE-Whitepaper-2021.pdf

Signalling & Interconnect Security

Both 2G and 3G networks are still deployed globally, and whilst we are seeing some closure of 2G and 3G networks, it is unlikely that these will entirely disappear from the ecosystem for years to come. The likelihood is that some 2G networks will outlive 3G due to the reliance of legacy, long-lived devices and services on 2G networks, e.g. the widespread deployment of early IoT devices such as smart meters.

The Signalling & Interconnect Threat

Traditionally, the interconnect traffic between operators relied on the underlying signalling protocols for effective and secure operation and the inherent trust model that assumed only those entities that need signalling access have it. For many years, this assumption has not been correct and operators need to recognise that attacks can come through their signalling network and their connections to other operators and partners. The industry has developed a range of enablers to respond to this threat through the use of signalling firewalls, message filtering and blocking capabilities, security cooperation, intelligence and best practice sharing. However, signalling and interconnect remains an important and ongoing threat area that requires monitoring because when signalling is compromised, the integrity, confidentiality and availability of many services is at risk. Future threats in this space may emerge as current mitigations prove insufficient and new attacks become viable. Also, emerging radio access supply arrangements may present opportunities for signalling attacks over access connections. Consequently, signalling security is still viewed as a priority area in which operators must focus significant attention for enhanced security and fraud avoidance.

The practice of Global Title (GT) leasing has significantly increased the attack surface as granting access to interconnect protocols and systems has extended to third parties, sometimes without the required due diligence, protection or monitoring mechanisms being in place by operators[81].

The interconnect threat is exacerbated by the deployment of insecure and misconfigured network equipment, which can inadvertently result in the generation of suspicious traffic. It is recognised that it is impossible to entirely prevent unauthorised or illicit SS7 network access so detection is essential if such activity is to be identified and isolated. This is in order to reduce the risk of user location tracking, eavesdropping, traffic diversion, spam, privacy breaches, fraud and denial of service. The lack of home routing deployment and inadequate monitoring and filtering capabilities being deployed by mobile networks increases the risk. GSMA has produced comprehensive security recommendations covering all of these aspects.

[81] See Mobileum blog post at https://blog.mobileum.com/the-battle-to-protect-our-subscribers-against-cyber-weapons

INDUSTRY INSIGHT:

An interconnect security survey performed by umlaut[82] at the request of several mobile operators provides some industry insight on the state of signalling and interconnect security. Each gap in completeness offers a security threat that can be mitigated with suitable controls. The list covers over 40 mobile operators mostly based in Europe and with some level of security awareness. Of the operators surveyed:

- 69% of networks have protection measures against International Mobile Subscriber Identity (IMSI) leakage (by Category 1 or bypass SMS Home Routing)
- 88% of the mobile operators have SMS Home Routing deployed
- 81% of the mobile operators have GSMA FS.11 SS7 Category 2 protection in blocking mode
- 5% of the mobile operators have GSMA FS.11 SS7 Category 3 protection in blocking mode
- 79% of the mobile operators have GSMA FS.19 Diameter Category 2 protection in blocking mode
- 3% of the mobile operators have GSMA FS.19 Diameter Category 3 protection in blocking mode
- 18% of the mobile operators have GTP-C inspection protection in blocking mode
- 59% of the mobile operators block, or do not support, GPRS Tunnel Protocol (GTP)-C v0 (deprecated) on the network.

The Signalling & Interconnect Response

Experience has shown that legacy 2G/3G networks make use of insecure, unmanaged signalling protocols and are subject to fraud and security threats on a regular basis. Many of these attacks have been mitigated with security enhancements introduced in 4G and 5G. However, due to the backward compatibility of 4G with 3G/2G they will not disappear until the legacy technology or backward compatibility ceases to exist.

The industry understands the challenges posed by signalling protocols, for example SS7, GTP, Border Gateway Protocol (BGP) and Diameter; however, fundamental resolutions to address these challenges would require significant changes to the core protocols and are not straightforward to apply to complex and globally deployed large scale networks. To address these challenges GSMA has developed a wide range of security controls and mitigations that act, when implemented by network operators, to significantly moderate these security challenges.

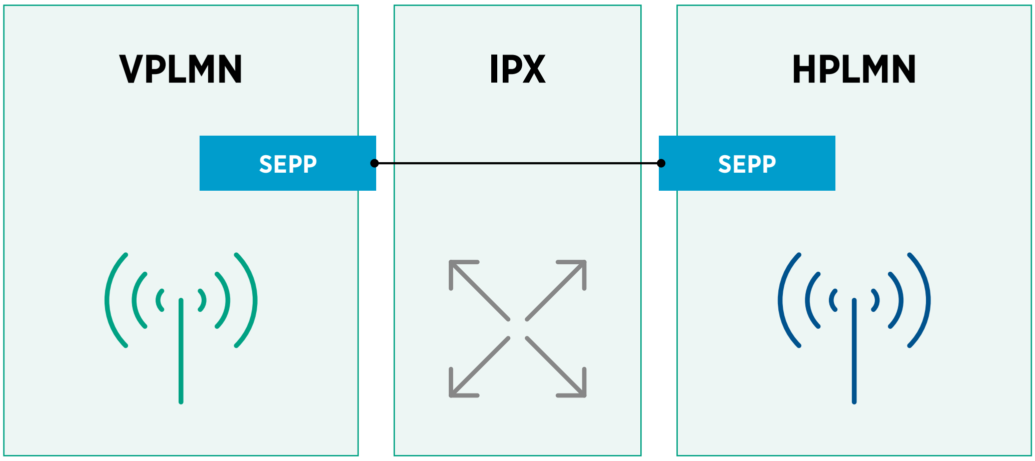
[82] http://umlaut.com/en/contact-us

5G is an opportunity for the mobile industry to enhance network and service security. New authentication capabilities, enhanced subscriber identity protection and additional security mechanisms will result in significant security improvements over legacy generations. In practice, the deployment of 5G is being achieved through two approaches, namely Non-Standalone (NSA) or Standalone (SA) architecture. NSA allows operators to utilise their existing communications and mobile Evolved Packet Core (EPC), instead of deploying a new core for 5G. 5G SA is a completely new core architecture defined by 3GPP that introduces significant changes such as a Service-Based Architecture (SBA) and the functional separation of network functions.

A significant difference between NSA and SA is that NSA provides control signalling of 5G to the 4G base station, whereas in SA the 5G base station is directly connected to the 5G core network and the control signalling does not depend on the 4G network.

Significant progress on interconnect security has been made with the advent of 5G for which new inter-network controls such as the Security Edge Protection Proxy (SEPP) have been defined. The SEPP is a new network function that protects the home network edge, acting as the security gateway on interconnections between the home network and visited networks.

Figure 8: Security Edge Protection Proxy



Supply Chain Security

The Supply Chain Threat

ENISA has published[83] a supply chain threat landscape mapping and studying the supply chain attacks that were discovered from January 2020 to early July 2021. ENISA found 62% of attacks took advantage of customer trust in the supplier; this is analogous to the historic SS7 signalling trust flaws, where operators trusted each other implicitly which subsequently opened an attack route for malicious third parties. One of the new attacks in the ENISA report was the Kaseya compromise[84].

Countries and national regulators are responding to the need for increased resiliency in network infrastructure by placing requirements on all operators to increase the levels of security and controls. This can include new supply chain arrangements to manage national operator use of specific suppliers. A recurring feature is to have an active management of an operator's supply chain. Consideration will be necessary as to the required 'depth' of management and 'deep understanding' of supply chains to ensure they are resilient and diverse.

Vendor selection is also important when considering managed service providers and also providers of non-network product (or underpinning) related services such as cloud providers. The business reliance placed on these aspects is crucial as part of the security and operational models are increasingly delivered by third parties and this introduces new threat vectors.

The opportunity for indirect attacks through supplier or third-party tooling and services cannot be underestimated, as was shown when SolarWinds was compromised and unwittingly delivered infected binaries to many of its customers[85]. This attack led to multiple services, that used SolarWinds platform and tools, becoming vulnerable to exploits through a supply chain attack. This type of attack emphasises not only the need for vigilance in relation to which 3rd party tools to use and awareness of the security posture of the 3rd party, but also good control, management and separation of assets. The force multiplier effect for an attacker across all the target's customers makes using a compromised vendor an attractive proposition.

Virtualised infrastructure and more open interfaces deliver significant benefits but also make the 5G supply chain more complex and multi-party compared to 4G and earlier. For example, virtualised infrastructure for a private cloud solution may comprise commodity compute hardware, virtualisation code to enable virtual machines and containers and potentially a number of code vendors delivering services. This enables significant flexibility, scalability and potential cost savings but also is a more complicated supply chain.

[83] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

[84] In July 2021, attackers exploited a zero day vulnerability in Kaseya's own systems (CVE-2021-3011632) that enabled the attackers to remotely execute commands on the VSA appliances of Kaseya's customers. Kaseya can send out remote updates to all VSA servers and, on Friday July 2, 2021, an update was distributed to Kaseya clients' VSA that executed code from the attackers. This malicious code in turn deployed ransomware

[85] SolarWinds Compromised https://www.ft.com/content/c13dbb51-907b-4db7-8347-30921ef931c2

CASE STUDY: Syniverse

According to an Ars Technica[86] report Syniverse (a company that routes hundreds of billions of text messages every year for hundreds of carriers), revealed to government regulators that a hacker had gained unauthorized access to its databases for five years. A filing with the Securities and Exchange Commission said that “in May 2021, Syniverse became aware of unauthorized access to its operational and information technology systems by an unknown individual or organization. Promptly upon Syniverse’s detection of the unauthorized access, Syniverse launched an internal investigation, notified law enforcement, commenced remedial actions and engaged the services of specialized legal counsel and other incident response professionals.”

Syniverse said that its “investigation revealed that the unauthorized access began in May 2016” and “that the individual or organization gained unauthorized access to databases within its network on several occasions, and that login information allowing access to or from its Electronic Data Transfer (‘EDT’) environment was compromised for approximately 235 of its customers.”

The Supply Chain Response

The GSMA Supply Chain Toolbox[87] outlines a number of services and guidelines to help operators and their suppliers to better understand security and to access best practice. This includes different accreditation and assurance schemes and guidelines pertaining to specific areas of mobile technology. The different resources in the toolbox are organised by relevance to the different stages of procurement by an operator and to different stages of a vendor’s solution lifecycle.

Good security practices can mitigate the risk of third-party unauthorised access through utilising secure networks, strong authentication, least privilege practices alongside strong Privileged Access Management (PAM). Approaches such as zero trust, toots of trust and trust domain separation are also important security concepts in this space.

An example of a recommended control is to implement effective supply-chain and procurement controls to ensure the services they operate and provide comply with legal requirements and manage supply-chain threats. This objective is met through a series of controls:

- Operators should set security hygiene expectations e.g. patching and supply chain risk management key practices
- Ownership and risk governance of the service and infrastructure
- Industry standard assessment programmes to assure vendor products (e.g. NESAS, SAS)
- Mapping planned physical interconnects
- Life-time support arrangements
- Manufacturers of critical components should provide a statement of compliance or local regulation compliance (e.g. using ISO 28000)
- Manufacturers of 5G network equipment should provide a statement of compliance or local regulation compliance. (e.g. using ISO 27001/1)
- Manufacturers of 5G network equipment should provide, for example, an ISO 22301 statement of compliance or local regulation compliance
- 5G service providers should comply with, for example, Service and Organization Controls 2 (Statement on Standards for Attestation Engagements 18[88]) for all services provided under the scope of the service agreement or local regulation compliance

[86] https://arstechnica.com/information-technology/2021/10/company-that-routes-sms-for-all-major-us-carriers-was-hacked-for-five-years/
[87] https://www.gsma.com/security/supply-chain-toolbox/
[88] https://us.aicpa.org/research/standards/auditattest/ssae.html

A second recommendation is that operators should implement 3rd party access and outsourcing controls to ensure the risks of information sharing and outsourcing are effectively managed. This objective is met through a series of controls:

- Processes to identify, prioritise and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process
- Procedures to identify and manage the risks associated with third-party access to the organization's systems and data
- Security controls on internal staff and resources, including privileged access, are mirrored with prioritised suppliers
- Contract and due diligence checks for prioritised suppliers based on a pre-procurement risk assessment
- Breach notification should be provided by suppliers in a timely manner

GSMA encourages suppliers to participate in industry-recognised security assurance schemes, such as GSMA's SAS[89] and NESAS[90] and encourages operators to source equipment from suppliers that participate in these schemes.

The role of a Software Bill of Materials (SBOM) is relevant in the context of managing code vulnerabilities but is also critically important when used to deliver supply chain controls in terms of being explicitly aware of what code is being utilised, the versions in use, where it is sourced from and its lifecycle state[91].

There is national intervention[92, 93] that can result in the limitation or banning of certain vendors.

Finally, in several regions such as Asia, Europe and the US, there is a push not only for a more diverse supply chain, but also for the greater use of national suppliers. This may include government incentives to use certain domestic suppliers. Of course, these vendors must also be able to meet the wider security provisions already mentioned in this report and comply with relevant procurement and industry competition regulations.

[89] https://www.gsma.com/security/security-accreditation-scheme/
[90] https://www.gsma.com/security/network-equipment-security-assurance-scheme/
[91] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf
[92] https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf
[93] https://www.bbc.co.uk/news/technology-53403793

Final Thoughts

This document provides an overview of the security landscape for the mobile industry in the context of current threats facing Mobile Network Operators and the wider ecosystem. In many cases, these threats and recommendations are not new, and effective responses are available to be implemented.

This report recommends:

- implementing the existing advice identified and referenced in this report
- maintaining active contributions to build and augment GSMA security guidance
- seeking out opportunities to get involved in industry security initiatives

Over the coming year the GSMA will continue to support its members on security matters. To get in touch, or get more closely involved, please email security@gsma.com.

GSMA Fraud & Security Services

Building stronger resilience within the mobile ecosystem

GSMA Coordinated Vulnerability Disclosure (CVD)
A way for researchers to disclose vulnerabilities that could impact the mobile ecosystem

GSMA Device Check™
Protect against the risk of handling stolen or fraudulent devices, with this instant look-up service

GSMA Device Registry
Deter device crime, by exchanging device status information across the global ecosystem

GSMA eUICC Security Assurance (eSA)
Instil confidence that eUICC chipsets have reached rigorous industry security standards

GSMA Network Equipment Security Assurance Scheme (NESAS)
Security assessment of vendors' product development/lifecycle processes and infrastructure products

GSMA Security Accreditation Scheme (SAS)
Security audit and certification of SIM/eSIM production and subscription management sites

GSMA member only

GSMA Fraud and Security Working Group (FASG)
Share threat intelligence in a confidential forum and collaborate to maintain the security of operators' and their customers' assets

GSMA Telecommunications-Information Sharing and Analysis Center (T-ISAC)
Share timely and actionable information on cyber security threats in a trusted environment

gsma.com

Find out more at
www.gsma.com

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601