Mobile Telecommunications Security Landscape

March 2021

Contents

Executive Summary

Welcome to the GSMA 3rd 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.

2020 saw a range of changes in the security landscape whilst traditional threat areas and actors continue to be present and pressure on networks remains.

Many businesses, including network operators have re-shaped operations and practices to enable remote working as Covid-19 has significantly reduced travel to traditional places of work, coupled with this some businesses have rapidly adopted and rolled out digital components to their services which has broadened the threat surface area that attackers seek to exploit. Alongside this, fraudsters and attackers have targeted this broadened surface area of home-working due to Covid-19. In addition, conspiracy theories spread around 5G and Covid-19 have resulted in base station attacks and on the engineers working on installations[1].

Mobile networks have proved highly resilient as the amount of traffic they carry and services that rely on their operation has increased. Mobile networks continue to support a changing economic and societal health challenged by the Covid-19 pandemic, and the industry is strongly motivated to identify and mitigate the threats.

Many security threats are able to be anticipated and with good hygiene, continued action and vigilance, mitigated. Trends towards more open and virtualised networks have continued with the consequent emergence of new approaches to security. Security must be managed across people, processes and technology and through the full lifecycle from service definition, deployment, operation and ultimately decommissioning.

The supply chain continues to be a critical consideration in the security landscape.

5G services are being rolled out typically in non-standalone mode and we are seeing the first 'beyond trial' deployments of open network based solutions. The complexity of deployment options may increase the surface area over which attackers seek to exploit vulnerabilities. Particularly for 5G network implementations, there are more controls, options, tactics and features that will aid in the reduction of exploitable vulnerabilities.

This guide gives insights into the security landscape of the mobile telecommunications ecosystem, details key dimensions of consideration, and offers guidance to mitigate and tackle such threats.

1 https://www.thisismoney.co.uk/money/comment/article-8211113/BT-BOSS-stop-mindless-idiots-truly-believe-5G-Covid-19-linked.html

Introduction

Mobile telecommunications networks remain under daily attack. The industry understands that no security threat can be tackled in isolation, and that threat actors will continue to exploit vulnerabilities in deployed technologies and processes to achieve their goal. In the face of this persistent threat it is crucial to develop a broad understanding of evolving threats facing the industry. The European Union Agency for Cyber Security (ENISA) has published comprehensive threat reports on cyber attacks[2] and specifically for 5G[3].

Our aim is to advise on the current security landscape and highlight potential future threats affecting the mobile telecommunications industry and identify likely mitigations and where the industry is taking action.

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

2 https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

3 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks

Security must continue to evolve and adapt to changing threats and enable technology adoption and process improvement to remain effective in combatting and out maneuver those working against or exploiting the mobile ecosystem.

The headline security topics identified for this year's report are illustrated by Figure 1.

FIGURE 1

GSMA'S 2021 SECURITY LANDSCAPE TOPICS

Document Structure

This third edition of the GSMA Security Landscape report aims to provide an understanding of mobile telecommunications security hot topics at a high level, what action is being taken and what likely mitigations are recommended to combat a number of highlighted threats. Each chapter in this report represents a single security topic although as the topics can overlap in some areas, it is recommended that the whole document is considered in order to gain maximum benefit. All chapters that appeared in the 2020 report have been updated to reflect how these security topics, and the industry, have evolved during 2020. As the landscape has evolved, GSMA has assessed some security topics relegated to a lower status and been replaced with others of higher status.

This does not mean that legacy threats have disappeared. They still need to be addressed. As a result this report builds on the 2019 and 2020 Mobile Telecommunications Security Threat Landscapes[4] to present an updated view of the evolving security landscape.

For each domain the GSMA aims to outline the nature of the security topic, offer insight and propose recommendations and actions the industry could implement. Each chapter is structured as follows:

THE GSMA'S OVERARCHING VIEW OF THE THREAT

FURTHER INSIGHTS INTO THE THREAT

RECOMMENDATIONS PROPOSED BY THE GSMA

4 https://www.gsma.com/security/resources/mobile-telecommunications-security-threat-landscape/

Software & Virtualisation

There are many industry initiatives driving more open architectures and virtualised telecoms infrastructure such as TIP, O-RAN Alliance, Linux Networking Foundation and the Open Networking Forum. The telecommunications industry uses software from the open source community in a range of architectural deployments. This includes providing virtualised middleware, as a software component running on virtualised infrastructure or within proprietary code implementation.

There are numerous advantages to open source software as by definition the source code is accessible and subject to inspection, a wide community of developers can contribute with the potential to accelerate telco cloud implementation. However, it is worth noting that there are numerous tests for 'what makes secure software' but it is the developer's choice whether to adopt and enforce these in the open source community whose main focus can be limited to functionality[5].

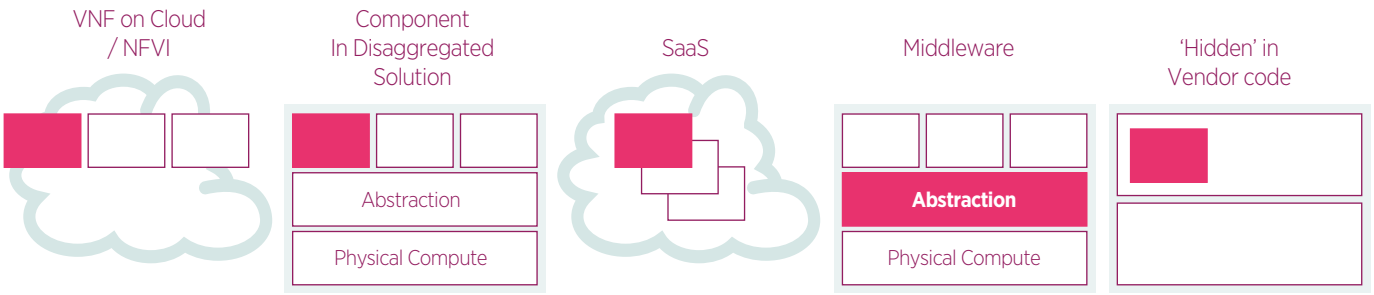
Poorly written code of the insertion of malicious code could be used to compromise network operation or uses of a compromised network.

5 https://www.linuxfoundation.org/wp-content/uploads/2020FOSSContributorSurveyReport_121020.pdf

There are differing deployment arrangements for open source software as illustrated below.

FIGURE 2

OPEN SOURCE SOFTWARE DEPLOYMENT ARRANGEMENTS



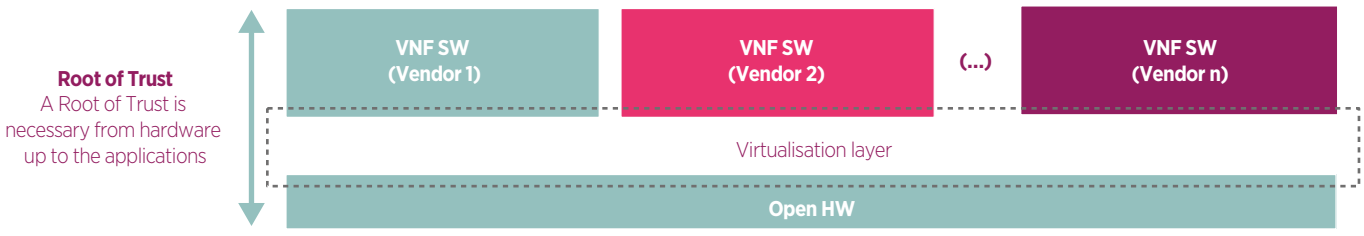
Open source software may be applied in a wide range of ways including:

- **as discrete code** (such as a Virtual Network Function (VNF) running on top of Cloud / Network Function Virtualisation Infrastructure (NFVI), or as virtualised Central / Distributed RAN Units on Cloud / NFVI;
- **as a component** within a disaggregated solution;
- **as part of the provision** of a wider Software as a Service (SaaS) provision. This may be found in a variety of deployments, e.g. as part of an open RAN or virtualised core deployment;
- **as middleware abstraction or virtualisation layer** between Commercial Off The Shelf (COTS) physical compute and the applications sitting on top. The applications may themselves be open source or proprietary in origin. This definition might be extended to include other software such as variants of Linux and Apache;
- **re-used** within vendor executable code. The fact that open source code is deployed may be obscured or 'hidden' as the executable code is difficult to inspect and source code may be difficult to obtain and inspect.

Consider a generic implementation with an underlying open hardware platform supporting a virtualisation layer (e.g. Openstack) in turn supporting multiple VNFs each from differing vendors / supply routes.

FIGURE 3

A MULTI-VENDOR VIRTUALISED SOLUTION



Software implements the functionality of the unit. The code can be proprietary and contain open source components and may contain commercially supported open source virtualisation software to allow interfacing between the code and the supporting open hardware or Cloud infrastructure. Differing architectural decisions result in variances in the levels of abstraction and separation between workloads within virtualisation fabrics. Each respective layer may have security controls, yet it is important that the implementation works together to implement a coherent security solution.

Security consideration is needed for the selection of both the virtualisation and networking software layers of code that can, in many cases contain elements of, or are completely open source code in origin with the potential to include malware or compromised code. Therefore, strong code support is necessary to ensure malware and compromised code are fixed before attackers can exploit them.

Proprietary code developers may aim to speed delivery of their products by re-using open source code. Although open source code may be a small proportion compared to proprietary code, the proprietary code developer must recognize the continuing responsibility for the entire code base, proprietary and open source. These responsibilities include keeping track of open source code dependencies and making updates as they become available from the open source community providing the open source code. For proprietary executable code, the vendor will typically provide all the development resources (coders), follow their own company-specific software development coding practices (ideally benchmarked to the best in industry) and controlled according to their own configuration management processes. Support for the code is usually provided in a Maintenance contract with service level agreements.

Community open source code is produced from an open source community and entirely supported from within that community. Packages are free to download within the terms of open source licensing. There is often significant churn in open source community developments. This can result in a significant number of 'dead' or inactive code branches which are unlikely to attract further code development and support. In contrast, active branches will benefit from enhancements and bugs fixes. Whilst certain code branch functionality may seem attractive, it is important to understand the support, development and coder quality associated with it to ensure there is longevity to the code deployment and that security weaknesses and bug fixes can be implemented.

Commercial open source code is open source code often produced from code developed by the commercial entity and contributed to a code base under one of the open source license types e.g. GNU alongside other contributors. Commercial open source code is not the same as proprietary – it is often free to download in both source and executable forms but typically support etc is a chargeable element. Both commercial and community approaches have advantages; one key differentiator is in the area of support / bug fixes. With a Community support arrangement, the software user is dependent on the community to generate the code fix / update to a non-deterministic timescale. Commercial open source can often be backed by a service level agreement to integrate newly developed open source software, update the software with the latest security patches and ensure that modifications to the software do not disrupt user operations. The service agreement is based around a service offer, i.e. it does not imply any ownership of the underlying code itself.

For open source developed code, the main focus is typically to deliver required functionality and can be highly distributed by workforce and geographies. There is often little requirement for best practice development processes and for coding standards in general save for any that the community may agree to adhere to. Support for the code is varied leading to the threat that historic code bugs can remain unresolved. There are some well supported code bases that are contributed to by significant corporate groups. Elsewhere, support can depend entirely on the goodwill of the open source code developers and there is no guarantee of code fixes etc. As above, a major advantage of open source is that the source code is available for detailed inspection unlike vendor-specific executable code. This is also a disadvantage because attackers can equally inspect open source code to assess vulnerabilities.

6 Huawei Cyber Security Evaluation Centre (Hcsec) Oversight Board Annual Report 2019

An example of proprietary code re-using open source code can be described through the HCSEC Report in 2019[6]; when reviewing the Huawei code for an older LTE eNodeB product asserted "3.33 The report analysed the use of the commonly used and well maintained open source component OpenSSL. OpenSSL is often security critical and processes untrusted data from the network and so it is important that the component is kept up to date. In the first version of the software, there were 70 full copies of 4 different OpenSSL versions, ranging from 0.9.8 to 1.0.2k (including one from a vendor SDK) with partial copies of 14 versions, ranging from 0.9.7d to 1.0.2k, those partial copies numbering 304. Fragments of 10 versions, ranging from 0.9.6 to 1.0.2k, were also found across the codebase, with these normally being small sets of files that had been copied to import some particular functionality. There were also a large number of files, again spread across the codebase, that had started life in the OpenSSL library and had been modified by Huawei".

CASE STUDY

HEARTBLEED

As an example of the downside of the re-use of open source code, consider the cyber security flaw called Heartbleed. Refer to New Zealand National Cyber Security Centre coverage: "OpenSSL versions 1.0.1 through 1.0.1f contain a flaw that allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library. The bug commonly known as Heartbleed, allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This potentially compromises the secret keys used to secure internet communication, the names and passwords of the users and the actual content. Exploit code for this vulnerability is publicly available."

OpenSSL is the same code identified in the Huawei code described above. It is understood this is now remediated. CVE-2014-0160 is the official reference to this bug. CVE is the Standard for Information Security Vulnerability Names maintained by MITRE.

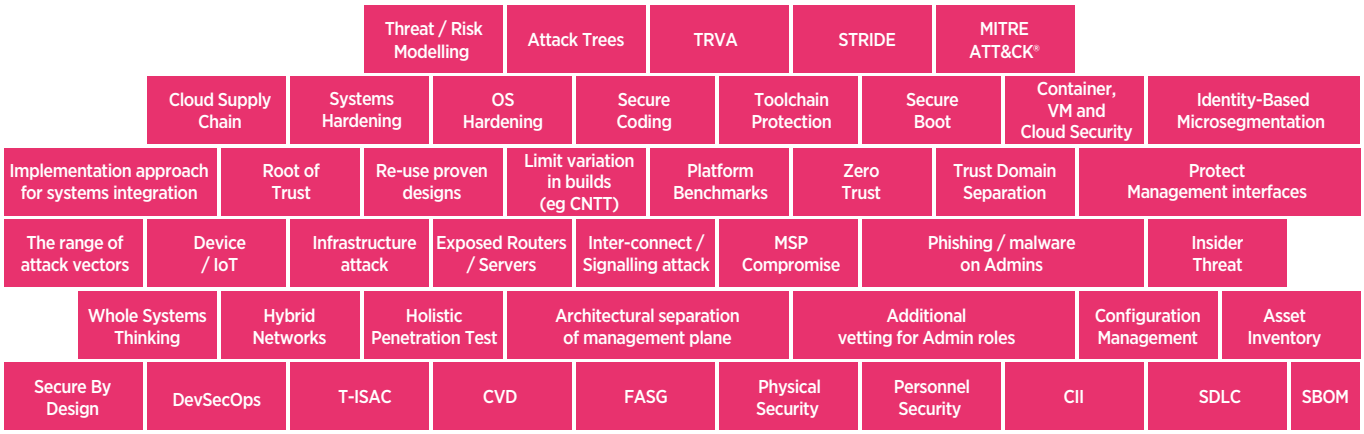
Containers and microservices are the future evolution of NFV cloud native and security is a significant consideration for their rollout. For example, host Operating System (OS) security is a typical container security threat as the lack of isolation from the shared host OS may introduce a potential threat. Container security threats also include container image file security, container orchestration security, container lifecycle management security and container run time security. In order to facilitate the rollout of virtualised networks and services, security technologies to address these threats need to be considered in a timely manner.

A GSMA report[7] has identified a range of developing controls and described them within the contexts of systems, component and infrastructure. Combining the systems and component level considerations can build a framework for considering the design and operation of open networks.

The system security control aspects can be summarised in the system security 'wall' shown below in Figure 4.

FIGURE 4

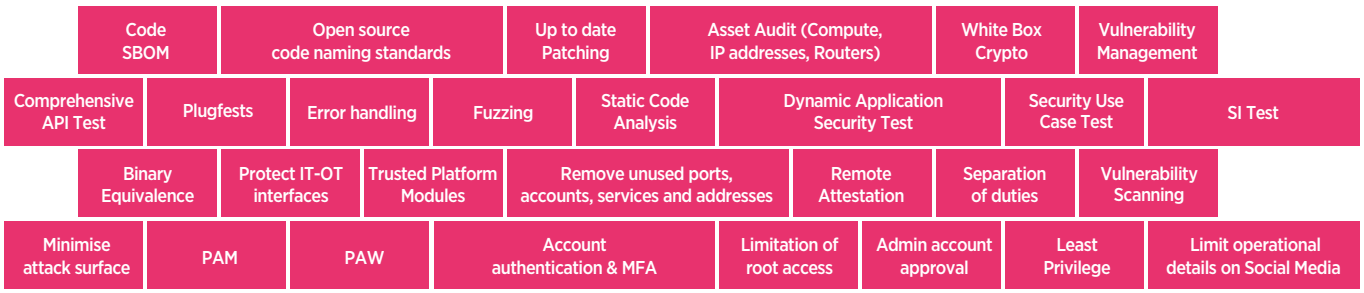
SYSTEM SECURITY WALL CONTROLS



Consideration of component level controls can be summarised in the Component Security 'Wall' shown below in Figure 5.

FIGURE 5

COMPONENT SECURITY WALL CONTROLS



Combining the systems and component level considerations can build a framework for considering the design and operation of open networks. The system and component lifecycles can be combined to illustrate their co-dependence and cyclic nature. The cycle time for each lifecycle will be notably different (i.e. the system lifecycle is likely to be slower) and the number of cycles undertaken in a system lifetime will be different (i.e. there is likely to be many more cycles of the component lifecycle). The application of the different controls will vary depending on where any specific change activity is taking place and at what level of granularity of change. Thus, a secure-by-design approach can then be applied to the process.

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

Cyber and Operational Security

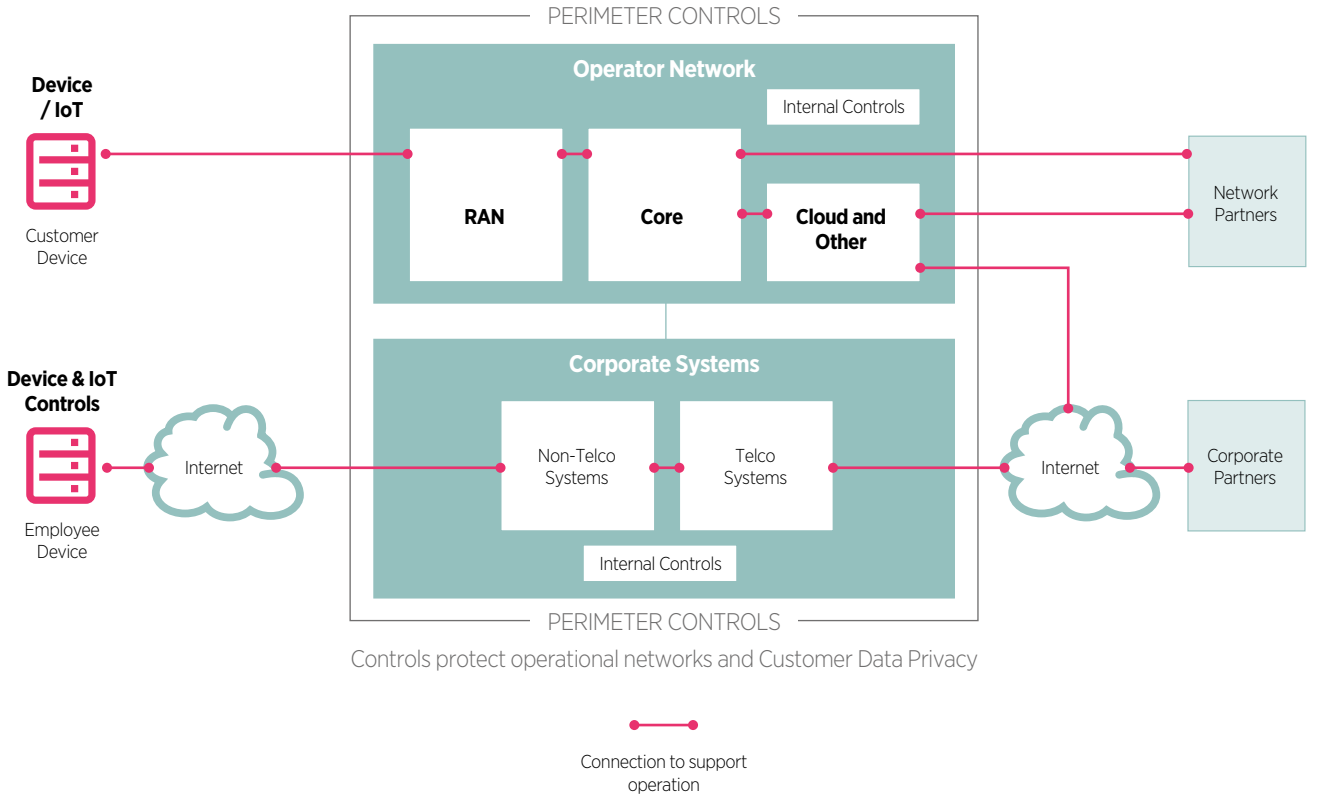
To administer and manage an operational mobile network there are a wide set of telecommunications and information technology (IT) systems (shown below in Figure 6). In addition to telecoms infrastructure, there are often a number of corporate information technology systems that enable the broader business operations. This includes corporate intranet, email, instant messaging and staff systems such as timesheets and sales systems. These systems are accessed by a range of employee devices and used by the full range of staff functions including system administrators for the operational network.

A range of wider corporate partner connections are often in place to provide access to wider IT and cloud services but also can provide access to the operator network to enable managed service providers. Crucially, any connection between the corporate systems and the operator network can provide an operational network attack route through associated IT Networks. Any security solution will involve both perimeter and internal controls. It is essential to protect both the operational mobile network and the associated IT as they are a threat vector for cyber-attack.

This topic explores the holistic need for ongoing security controls for both operational and supporting IT systems.

FIGURE 6

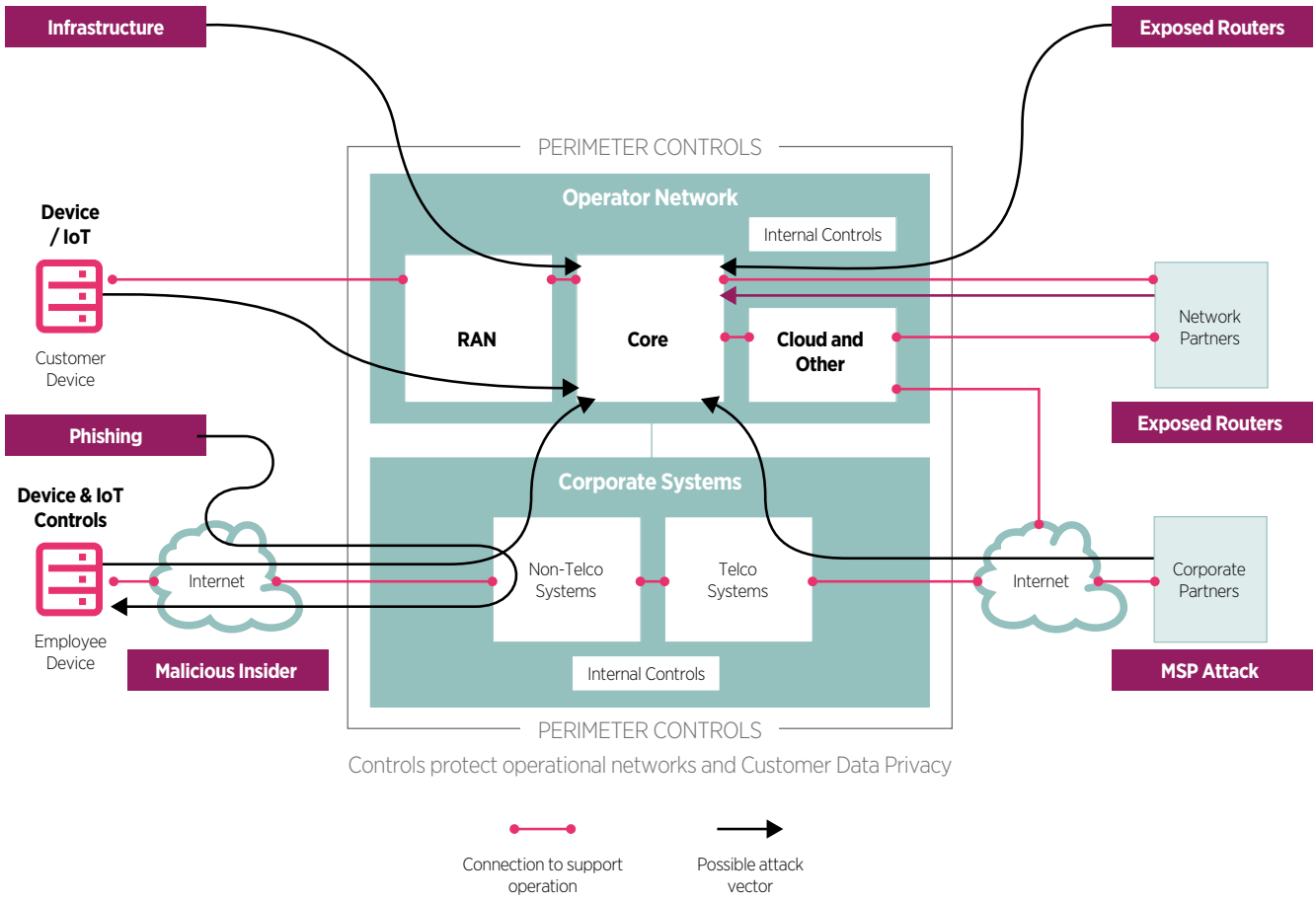
A SIMPLIFIED MOBILE NETWORK



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 7).

FIGURE 7

POTENTIAL SECURITY ATTACK VECTORS



There are a number of attack vectors presented and each requires strong security controls and processes to minimize the threat 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 activities.
- **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 is a well-known attack vector is comprehensively documented and attracts significant coverage in GSMA Member Security documents[8] 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. This threat was evidenced in 2020 with an exposed server at a Thailand-based mobile network operator[9] and a range of attacks targeting outdated servers[10]. It is important to have a strong grasp of the inventory of equipment in order that it can be managed and protected. Once the equipment fleet is identified, it must be protected and configured against attack. 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 Virtual Private Network 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 Site or Data Centres, has been seen this year in the UK[11] where conspiracy theorists attacked 5G Mast sites.
- **Device attack:** with increasing access bandwidth and a range of malware attacks on device, protection must be considered against device-based network attacks (e.g. signalling 'storms', Denial of Service attacks, Internet of Things (IoT) Compromise) back into the network. Additionally, devices themselves may be subject to individual attack and is explored in more detail in a later section of this report.
- **Supply Chain** (not shown on diagram but explored in a later section of this report) where equipment / software experiences interference in the process of supply / deployment, this also includes where third party service providers may also be exploited to compromise the network operator, for example, the recent SolarWinds compromise[12].

The industry[13] has seen cyber hacking attacks against supporting IT infrastructures such as Customer Relationship Management (CRM) systems. USCellular retail store's employees were scammed into downloading malicious software onto a computer. This allowed an attacker to access the computer remotely using the employee's credentials. The threat of attack via corporate IT systems is present and needs to be considered in any security strategy.

8 GSMA Documents FS.11 and FS.19

9 https://rainbowtabl.es/2020/05/25/thai-database-leaks-internet-records/

10 https://www.zdnet.com/article/hezbollahs-cyber-unit-hacked-into-telecoms-and-isps/

11 https://news.sky.com/story/coronavirus-attacks-on-5g-mobile-masts-surge-over-easter-weekend-11973145

12 https://www.solarwinds.com/securityadvisory

13 https://www.securitymagazine.com/articles/94476-uscellular-suffers-data-breach-hackers-accessed-its-crm-software?

Strong security controls in this area can significantly reduce the attack surface and reduce the opportunity for lateral movement and privilege escalation; all techniques exploited by phishing attacks, malware, identity theft, malicious insiders and external attacks via corporate partner arrangements.

One critical security aspect is the link between the corporate and operator networks as it provides an attack vector into the operational network. Good security practices can mitigate this risk through secure networks, strong authentication, least privilege practices alongside strong privileged access management (PAM). Approaches such as Zero trust, Roots of trust and Trust Domain Separation are also important security concepts.

A security strategy may be composed of multiple layers as shown in Figure 8. The combination of security controls taken from each layer build to deliver a bespoke security solution for every operator. Security defences can be built on the controls and mitigations delivered from each previous security layer. Efficient and cost effective security approaches can be delivered by matching security controls to the threat model, understanding the security benefits built-in by lower level security standards and by customising the security decisions in the higher-level security levels. This is especially true where compliance with national regulations may have already mandated some security considerations. The resulting set of security approaches build the overall security design[14].

FIGURE 8

A LAYERED SECURITY DEFENCE

14 This topic is explored more fully in the GSMA Whitepaper, Open Source Software Security, January 2021 at https://www.gsma.com/futurenetworks/resources/open-networking-the-security-of-open-source-software-deployment/

Supply Chain

Supply chain can be broken down into a number of distinct but related areas; the components of a network that go together to deliver an operational resilient service, where those components are sourced (from hardware to software) and the parties that are involved in putting together products and services that aid in the upkeep and maintenance of a network.

The classification of much mobile infrastructure as critical national infrastructure in many jurisdictions, and concerns about national security have increased focus on the security posture of network equipment and the providers of it. In 2020, we saw an increasing trend towards national responses to supply chain threats. These national responses varied from restricting certain vendors, implementing new defensive regulations and security requirements, through to attempts to broaden existing vendor arrangements via open networking and wider initiatives.

The restrictions and in some cases bans[15] on using certain vendors is driving vendor swaps in some markets and a general pressure to diversify the supply chains. Whilst these have potential advantages from a business reliance viewpoint, there is a balance of ensuring any scale changes of vendor are achieved in a resilient manner and utilise robust alternative vendors. The selection and testing of new vendors is therefore a key activity.

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

15 https://www.gov.uk/government/speeches/digital-culture-media-and-sport-secretarys-statement-on-telecoms and https://www.commerce.gov/news/press-releases/2020/05/department-commerce-issues-expected-final-90-day-extension-temporary

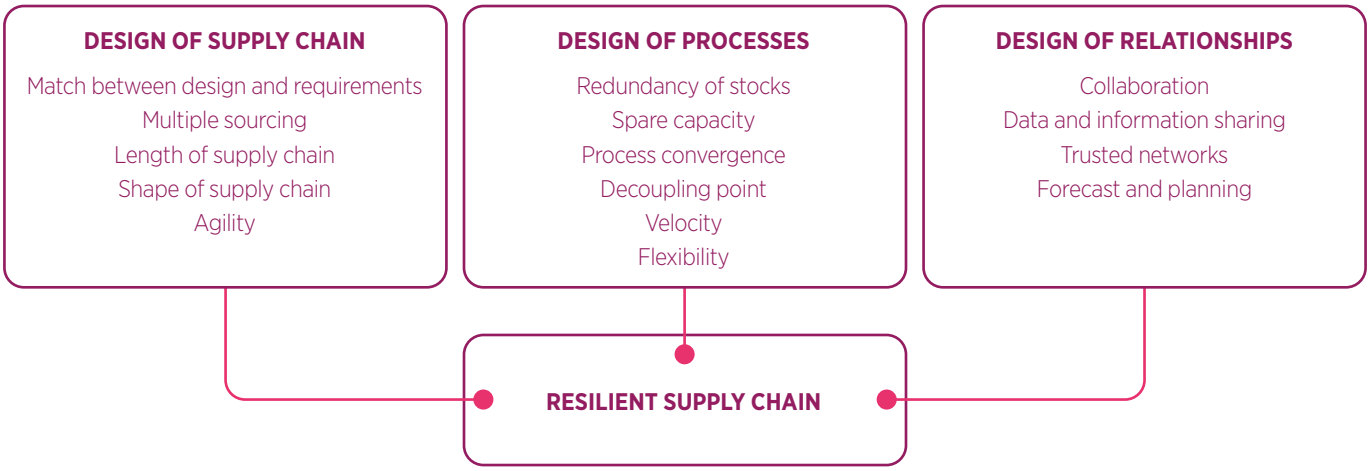
As architectures continue to move towards disaggregated components, leverage cloud and virtualisation architectures as well as increase in third party tools for monitoring, management and security, it is clear that the available 'surface area' for an attacker to exploit is becoming broader. Care must be taken to ensure that configuration and operation of a 'stack' is undertaken with security in mind.

The opportunity for indirect attacks through supplier or third party tooling cannot be underestimated, as was shown when SolarWinds was compromised and delivered infected binaries to many of its customers[16] leading to multiple services that used the platform and tools becoming vulnerable to exploit through a supply chain attack. This emphasizes not only the need for vigilance in which 3rd party tools to use and the security stance of the 2rd party but also good control and separation of assets.

Availability of equipment and diverse suppliers are vital for market economies, market health and to prevent vendor lock in. A resilient supply chain has components available from multiple sources (Figure 9). These sources should be geographically resilient to manage geopolitical or natural disaster type threats. The year 2020 has seen several countries ban or restrict equipment from vendors designated as high risk from being used within 5G networks. In May 2020, the U.S. Department of Commerce (DoC) amended the foreign-produced direct product rule to target Huawei's acquisition of semiconductors that are the direct product of certain U.S. software and technology. In August 2020, the US DoC further restricted access by Huawei Technologies and its non-U.S. affiliates on the Entity List to items produced domestically and abroad from U.S. technology and software. This has highlighted the lack of diversity and resilience within the network equipment supply chain.

FIGURE 9

SUPPLY CHAIN RESILIENCE



There are no quick fixes to resilience threats. The threat has emerged due to the long term and complex nature of the industry sourcing activities, contract lifecycle support needs and technology interoperability requirements. For example, hardware is supplied by one supplier but the service contract for hardware support may be outsourced to another. As a result, removing one vendor may have a knock-on effect on other contracts and services. As new approaches such as open networking are standardised, there is potential for a wider set of suppliers to mature their implementations and offer into the market.

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

The GSMA recommends the following with regard to supply chain security:

- Understand who you do business with; prioritise and risk assess each supplier with specific focus on redundancy, flexibility and the technical and procedural ability to switch supplier if required.
- Map and assess the criticality of any component / service offering within the supply chain. Plan and manage operational security (along with reliability) accordingly.
- Build business continuity plans that consider the removal of critical vendors; understand the impact if one were to be removed.
- Apply the range of security considerations identified in the GSMA Whitepaper covering open source software[17].
- Consider trials of open networking solutions to de-risk selection of new vendors
- Work with local legislators and regulators to understand how potential decisions with regard to supplier bans.
- Engage with and support international standards development. LTE was the first fully interoperable global standard for the mobile networks. Moving away from global standards for 5G would impact the deployment and long term security of the industry.

Encourage suppliers to participate in industry recognised security assurance schemes, such as GSMA's Security Accreditation Scheme (SAS)[18] and Network Equipment Security Assurance Scheme (NESAS)[19] and source equipment from suppliers that participate in these schemes. NESAS, which is focussed on secure network product development, is intended to be used alongside other mechanisms that are focussed on the deployment, configuration and management of mobile network infrastructure to ensure a network is secure, in particular an appropriate set of security policies covering the whole lifecycle of a network. The scheme should 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 and/or propose them to be included in the scheme.

17 GSMA Report Open Source Software Security, January 2021 https://www.gsma.com/futurenetworks/resources/open-networking-the-security-of-open-source-software-deployment/

18 https://www.gsma.com/security/security-accreditation-scheme/

19 https://www.gsma.com/security/network-equipment-security-assurance-scheme/

Cloud Security

This section considers two cloud security topics; one where cloud infrastructure is increasingly part of the underlying technology to virtualise network infrastructure and secondly as a means to store and process customer data as well as enable rich services.

Cloud services usage is on the rise year on year[20] and solutions are becoming more customised to virtualised mobile networks[21]. Any potential economies of scale, offered through virtualisation and cloud services, will only be fully realised if the security controls remain consistent when implemented.

Mobile network operators need to collect, process and store a wide variety of operational data to deliver, improve services for their customers and generate business value.

Customer data requires careful handling to preserve customer data privacy and to comply with local data localisation requirements. Recent data breaches[22] have highlighted the threat from data theft attackers is still a recurring concern whilst the changing regulatory and regional regulation has drawn this topic into a major area of brand and regulatory risk.

As Cloud solutions are becoming a more fundamental component of a network, there is a consequent threat that any systemic security weakness in the service may have a major effect on network operation. Also, there is a threat that if personal data is stored inconsistently with data privacy policies, customer security (privacy) may be compromised and significant fines may apply.

20 E.G. The worldwide public cloud services market is forecast to grow 6.3% in 2020 to total $257.9 billion, up from $242.7 billion in 2019, according to Gartner, Inc; see https://www.gartner.com/en/newsroom/press-releases/2020-07-23-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-6point3-percent-in-2020

21 E.G. The Microsoft Launch of Azure for Operators; see https://azure.microsoft.com/en-us/industries/telecommunications/ & Google Cloud announced a comprehensive new strategy to help telecommunications companies digitally transform including Anthos for Telecom; see https://cloud.google.com/press-releases/2020/0305/google-cloud-telco-strategy

22 E.G. Marriott International; see https://news.marriott.com/news/2020/03/31/marriott-international-notifies-guests-of-property-system-incident

In a 5G era where Mobile Edge Computing (MEC), big data and a plethora of devices on the IoT become synonymous with mobile network operations, the volumes of data created, compiled, stored and processed to meet business demands increases and as such so does the need for free data flow.

Mobile operators' customer personal data remains a prized target for would-be attackers. Customer data can be exploited to directly target individuals through phishing, malware or other attacks or indirectly through sale of data to third parties.

A recent report from Sophos[23] discusses the results of the survey of companies hosting data and workloads in the public cloud: *"Seventy percent of organizations reported they were hit by malware, ransomware, data theft, account compromise attempts, or cryptojacking in the last year"*. Many of the weaknesses appear to relate to security misconfigurations.

Cloud infrastructure is increasingly deployed in mobile networks to exploit a lower infrastructure cost base, gain from economies of scale and increase flexibility. Technical solutions range from private cloud (cloud technology privately owned and operated for exclusive use by the owner), public cloud (cloud technology typically owned and operated by a hyperscale company provided on a shared basis across multiple customers and sectors) through to hybrid cloud (utilising both private and public cloud offerings in combination).

Data can be thought of in three main areas:

- customer data such as sensitive personal data, content, files, emails and photos.
- derived usage data including websites visited, service usage, advertisements invoked, that can be used to derive behavioural considerations.
- system data such as cloud load, processor utilisation, equipment and service management, and bandwidth that is used to manage the overall capability.

There are differing public cloud approaches to resilience, security (such as the use of domestic encryption schemes) and compliance in the geographies of the leading players from US, China, India and in Europe. Cloud data centre deployment is increasing significant not just in national locations but regionally and globally to provide access to the widest market in order to justify hyper-scale deployments. Customer data is not just held abstractly in 'the cloud' rather it is systematically stored in a resilient manner across a range of physical compute devices located in a data centre in a given country(ies). The systematic approach may mean customer data is stored in countries with differing data privacy protection regimes. This globalisation draws into greater focus the differing regional and national requirements to protect and localise personal data.

23 https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

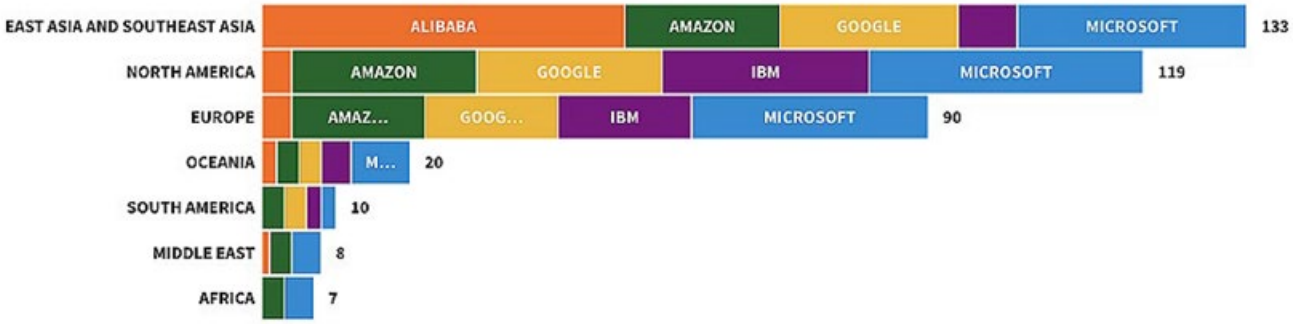
A range of legal, security and privacy concerns in the countries of origin, may require certain standard or specific measures to be implemented either to prevent unauthorised disclosure or to ensure that individuals' rights can be respected without having to take action in the destination country. As regards access to personal data by national security authorities in the destination country, data protection and respect for human rights in the country of origin may necessitate additional measures that go beyond what would otherwise be considered an appropriate level of security.

Individual nation states have differing data protection regimes covering some, all or indeed none of these aspects. Of course, mobile network operators will always seek to protect the all customer data they own in a pragmatic and secure manner irrespective of local regulations. Legislation and regulation continues to change notably where customer personal data is concerned. The recent Schrems II[24] ruling by the European Court of Justice[25] and the US Clarifying Lawful Overseas Use of Data (CLOUD) Act[26] are particularly relevant.

A global distribution of cloud service providers' data centre locations is illustrated below[27]. As the data centre location is where data storage and processing will occur, it is vital to consider how any cloud vendor choice relates to security and data privacy.

FIGURE 10

GLOBAL DISTRIBUTION OF CLOUD SERVICE PROVIDERS' DATA CENTER LOCATIONS



Source: Lily-Zimeng Liu

24 https://www.gsma.com/publicpolicy/certainty-for-eu-cross-border-data-flows-hinted-at-in-schrems-ii-case-may-be-short-lived

25 In a case that was originally brought by privacy activist Max Schrems against Facebook, the European Court of Justice (CJEU) has invalidated one of the legal mechanisms permitting data transfers from the EU to the US ("EU-US Privacy Shield") on the basis that the US national security laws and practices do not provide sufficient protection for EU personal data. The court did validate the Standard Contractual Clauses (SCC), but emphasised that the company exporting the data is responsible for assessing whether the data is adequately protected each time it relies on SCCs taking into account the national security laws and practices in the destination country as well as any additional safeguards implemented.

26 https://www.justice.gov/dag/page/file/1153466/download

27 From: https://www.atlanticcouncil.org/wp-content/uploads/2020/09/CLOUD-MYTHS-REPORT.pdf

Responses to cloud security are addressed in part in the content of previous sections of this report covering Software & Virtualisation, Cyber & Operational Security and Supply Chain.

Additionally, cloud service controls include:

- Cloud supplier selection is a crucial decision subject to keen regulatory focus and from a security perspective makes it really important to consider the security arrangements in place for Cloud service providers.
- There is potential for operators to use cloud procurement contracts to identify cloud provider details for detailed risk management plans, information on hardware vendor choices, incident reporting and performance data. This data can inform vendor selection and maintenance.
- Local policy covering all cloud delivery and deployment models. Specific controls may relate to provisioning, service implementation, vendor choice, data management and destruction, and threat detection services.
- Follow industry guidelines such as the recently updated and comprehensive National Institute of Standards and Technology (NIST) Special Publication Security and Privacy Controls for Information Systems and Organizations.[28]
- Develop consistent services that include security controls at build phase (secure by design).
- Subject cloud systems to the same IT hygiene best practice as physical systems. This includes ensuring contractual controls for security and strong validation of cloud security configurations.
- Cover in-life threat modelling as part of the ongoing risk management process. Develop a threat model for each deployment model and consider cloud-based attacks.
- Check that suppliers hold appropriate compliance to industry-standard certifications to assure that it is following industry best-practices and regulations[29].
- Develop and retain appropriate skillsets amongst staff to manage cloud deployments; specifically cloud based security skills.

28 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

29 E.G. https://cloudsecurityalliance.org/star/

Device & IoT Security

The number of devices connected to mobile networks exceeds the global population and the number of unique subscribers is 65% of the global population. With rapid adoption of IoT devices, connections are expected to exceed 25 billion by 2025 [30]. Devices are becoming more powerful and feature rich and will increasingly rely on network features and functions in the 5G era as well as connecting to a broader array of services and functions within the enterprise and consumer space. The surface area for compromise is growing in width due to connections and in depth due to deepening technical functional reliance.

The rate of change of functionality of a given device and the complexity of the technology 'stack' it typically contains (operating system, applications, functions etc.) is increasing and consequently the need to keep such components up to date with regular firmware / software updates is also likely to increase if vulnerabilities are to be identified and eliminated in a timely fashion.

The significant connected surface area is attractive to attackers both through technological compromise, such as malware, as well as targeting and compromising consumers through phishing, social engineering, etc. As such, both technological controls and measures are needed as well as good education and consumer awareness measures.

30 GSMAi The Mobile Economy - https://www.gsma.com/mobileeconomy/

Failing to update applications (apps) installed on devices results in outdated privacy measures remaining in the ecosystem. This is a threat as Potentially Harmful Apps[31] (PHA) or data leaking[32] apps are not blocked/controlled using the latest updates. This may lead to unauthorised use of consumer data.

In 2020, we observed a 're-branding' of many existing attack methods to a topical use of Covid-19 theme in an attempt to increase successful compromise[33]. These attack methods include Smishing (SMS phishing campaigns), Email Phishing, Vishing (Voice phishing), Robocalls (typically a call utilising a recorded message), Wangiri fraud and Malicious applications (Malware) with Covid-19 themes.

There is also an increased reliance on device security to enable end-to-end traffic protection, for example to support Two Factor Authentication with the second factor commonly residing on a mobile. Additionally, certain market moves such as increased end-to-end encryption and Domain Name Service over HTTPS (DoH) can make operator security interventions more difficult as it may not be possible to gain insight into traffic patterns that could be rogue.

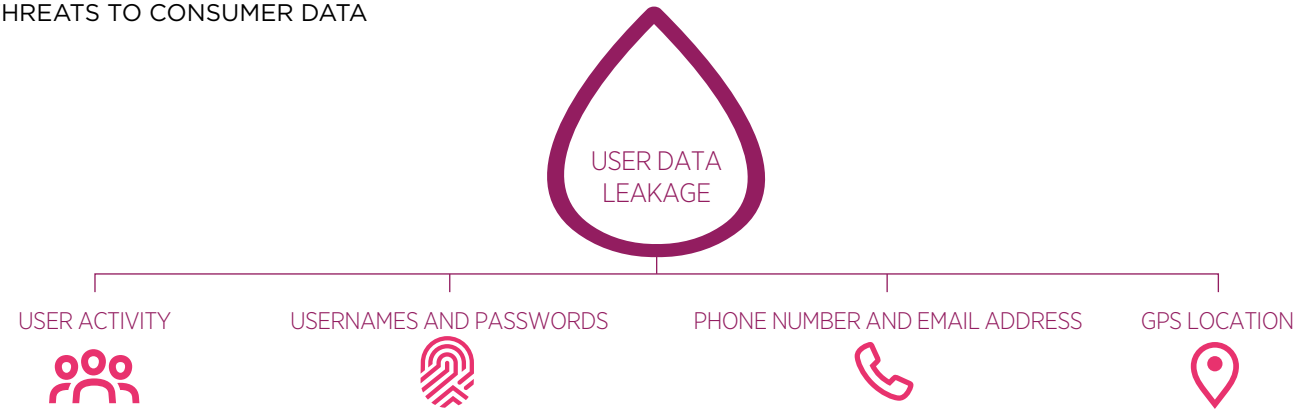
The security design of IoT devices is variable. One approach to enhance security, is to use the security delivered by a mobile device's Universal Integrated Circuit Card to provide a 'Root of Trust'.

There are over 5 billion unique mobile network subscribers[34] and mobile device usage accounts for a large volume of internet traffic. Consumers expect to be able to run their lives from their device, yet increasing awareness of inadequate privacy controls and unauthorised use of data diminishes consumer trust in the entire mobile telecommunications ecosystem.

The combination of vulnerabilities within an out of date app may mean the data may be exploited by an attacker. This was seen in early 2021 as a new campaign targeting Android devices by co-opting them into a botnet with the sole aim to carry out distributed denial of service attacks[35]. Malicious applications with Covid-19 themes have been discovered by mobile security companies[36]. Official App stores appear to be successfully avoiding infiltration.

FIGURE 11

THREATS TO CONSUMER DATA



31 Potentially Harmful Applications (PHAs) are apps that could put users, user data, or devices at risk. These apps are often generically referred to as malware.

32 Unauthorized or unintentional transfer of sensitive information from a mobile device to a 3rd party

33 https://www.gsma.com/newsroom/resources/covid-19-mobile-cyber-security-fraud-threat-observations-and-incidents/

34 https://www.gsmaintelligence.com

35 https://www.hackread.com/matryosh-ddos-botnet-hits-android-devices/

36 https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/

IoT Malware is not a new topic but does represent a relatively new data source, first reported to GSMA T-ISAC via the technical threat intelligence platform MISP (Malware Information Sharing Platform) in July 2020. Since then it has become the second highest reported event. The Indicators of Compromise shared relate to malicious URLs linked to Mirai, Gafgyt and Hajime malware. This threat is further evidenced through a recent report from Nokia[37] that found that "Internet-connected, or IoT, devices now make up roughly 33% of infected devices, up from about 16% in 2019".

There is also an increasing regulatory and industry focus on IoT Security (examples shown below).

FIGURE 12

EXAMPLES OF IoT SECURITY DOCUMENTS

The Universal Integrated Circuit Card (UICC), and its applications and data, play a fundamental role in ensuring the security of mobile subscribers' accounts and related services and transactions. The GSMA's Security Accreditation Scheme (SAS)[38] enables mobile operators to have confidence in the security of their UICC and Embedded UICC (eUICC) suppliers, and of their eUICC subscription management service providers.

37 https://www.darkreading.com/vulnerabilities---threats/nokia-threat-intelligence-report-warns-of-rising-cyberattacks-on-internet-connected-devices/d/d-id/1339243

38 https://www.gsma.com/security/security-accreditation-scheme/

The GSMA Mobile Privacy Principles[39] specifically emphasise:

- Mobile network operators should ensure that privacy risks are considered when designing new apps or services, and develop solutions that provide customers with simple ways to understand their privacy choices and control their data
- Developers of mobile device applications should embed industry-developed privacy principles and related design guidelines such as the GSMA mobile privacy principles
- Protection should be designed into new applications and services (i.e., privacy by design) to provide transparency, choice and control for the individual user, to build trust and confidence

Mobile network operators are encouraged to engage with and contribute to industry initiatives, such as the GSMA's Device Security Group (DSG)[40] to develop secure device best practice for the industry. 5G Security advances such as enhanced user identity privacy i.e., Subscription Concealed Identifier (SUCI) have potential to effect a step-change in protection of the user identity.

GSMA have a range of useful documents offering extensive guidance for IoT Security (see Figure 13).

FIGURE 13

GSMA IoT SECURITY DOCUMENTATION

39 https://www.gsma.com/publicpolicy/wp-content/uploads/2016/02/GSMA2016_Guidelines_Mobile_Privacy_Principles.pdf

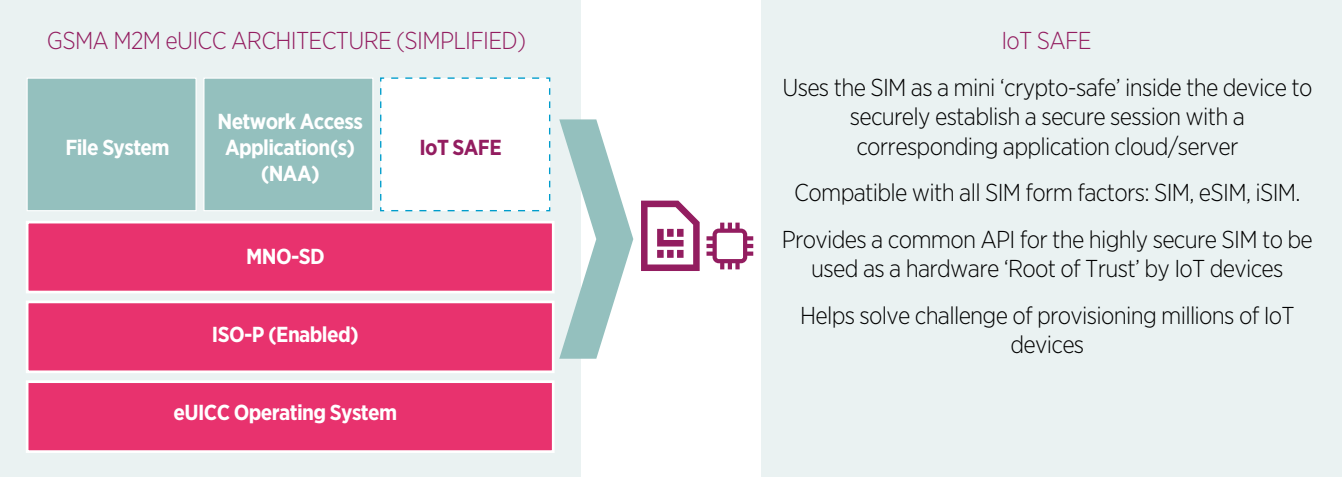
40 Join the DSG here

Mobile network operators use the UICC, commonly referred to as the SIM, to authenticate devices accessing their networks and services. UICCs can also support additional security capabilities that can be harnessed by IoT applications[41]. Leveraging a hardware secure element, or 'Root 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. This requires both the provisioning and use of security credentials that are inside a secure domain within the device.

Developed by the mobile industry, IoT SAFE[42] (IoT SIM Applet For Secure End-2-End Communication) enables IoT device manufacturers and IoT service providers to leverage the SIM as a robust, scalable and standardised hardware Root of Trust to protect IoT data communications.

FIGURE 14

IoT SAFE



IoT SAFE SIM Architecture (Example)

41 https://www.gsma.com/iot/resources/case-study-sim-secure-iot-services/

42 https://www.gsma.com/iot/iot-safe/

Signalling & inter-connect

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 disappear from the ecosystem for many years to come, with the likelihood that 2G networks will outlive 3G due to legacy long life devices and services reliant on such, e.g. sensors and signalling / early IoT.

Traditionally, the inter-connect traffic between operators relies on the underlying signalling protocols for effective and secure operation and there is an inherent trust model that assumes only those entities that need signalling access have it. For legacy networks, this assumption no longer holds true and operators need to recognise that attacks can come through their signalling network and connections to other operators. One report, suggested private intelligence companies were exploiting signalling networks based in the Channel Islands to enable surveillance operations to be carried out against people around the world.[43] The industry has developed a range of enablers to respond to this threat through the use of signalling firewalls, security co-operation and best practice sharing. However, signalling and interconnect remains an important and ongoing threat area that requires monitoring because when signalling is compromised, then the integrity, privacy and availability of services is risked. Consequently, signalling security is still viewed as a priority area on which operators must focus significant attention for enhanced security and fraud avoidance.

Globally, 4G coverage continues to increase[44] as the growing deployment of 5G networks offers an opportunity for a step-change in signalling security. This means that legacy threats will continue to require compensating technologies, controls and continued good cyber hygiene practices to protect consumers whilst they connect through these older trust and technology models.

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.

43 https://www.thebureauinvestigates.com/stories/2020-12-16/spy-companies-using-channel-islands-to-track-phones-around-the-world

44 GSMAi identified growth in LTE (4G) for 2020 was 9.6%

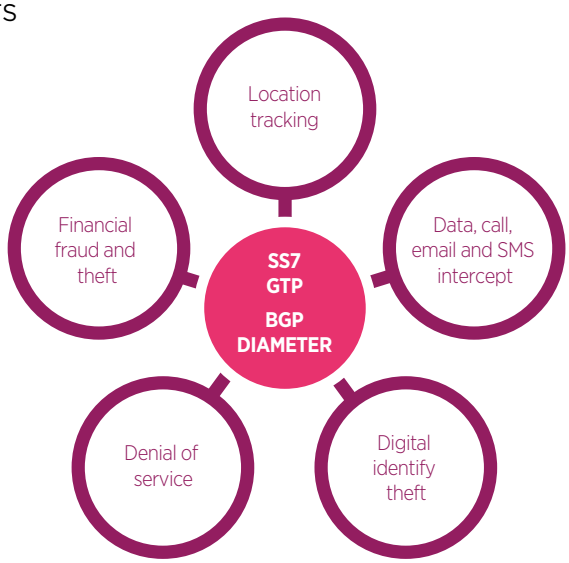
45 https://www.gsma.com/security/t-isac/

The GSMA Telecommunication Information Sharing and Analysis Center[45] is the central hub of 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 telecommunication sector. Drawing on the collective knowledge of mobile operators, vendors and security professionals, the T-ISAC collects, disseminates information and advice on security incidents within the mobile community – in a trusted and anonymised way. Signalling and inter-connect data represents a prime area of data sharing within T-ISAC, reflecting its importance and ongoing focus.

The industry understands the threats posed by signalling protocols, SS7[46], GTP[47], BGP[48] and Diameter[49] (see Figure 16); however fixes would require significant changes to the core protocols and are not straight forward to apply to complex and widely deployed large scale networks. As such, these threats are unlikely to be removed from any threat landscape relating to the mobile telecommunications industry for several years to come and monitoring and mitigation strategies must be employed instead.

FIGURE 15

LEGACY SIGNALLING THREATS



46 Signalling System 7 (SS7) is an international telecommunications standard that defines how network elements in a public switched telephone network (PSTN) exchange information over a digital signalling network.

47 GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols used to carry general packet radio service (GPRS) mobile telecommunication networks

48 Border Gateway Protocol . A 2020 article discusses a suspected BGP attack on Content Delivery Networks; see https://www.zdnet.com/article/russian-telco-hijacks-internet-traffic-for-google-aws-cloudflare-and-others/

49 Diameter protocol is a subscriber authentication, authorisation and accounting protocol particularly deployed in 4G networks.

50 https://www.scmagazineuk.com/criminals-hit-metro-bank-multi-factor-authentication-bypass-ss7-attack/article/1524670

51 https://www.bleepingcomputer.com/news/security/hackers-hijack-telegram-email-accounts-in-ss7-mobile-attack/?utm_medium=email&_hsmi=97801946&_hsenc=p2ANqtz-_mZqbuXolDGZt037MyP2rCktizflJYneG5jUA674yP7czI2HvysZyF3QD781W0CQo4FbRArfMD0rWQWugJhQQJsNvqFQ&utm_content=97801946&utm_source=hs_email

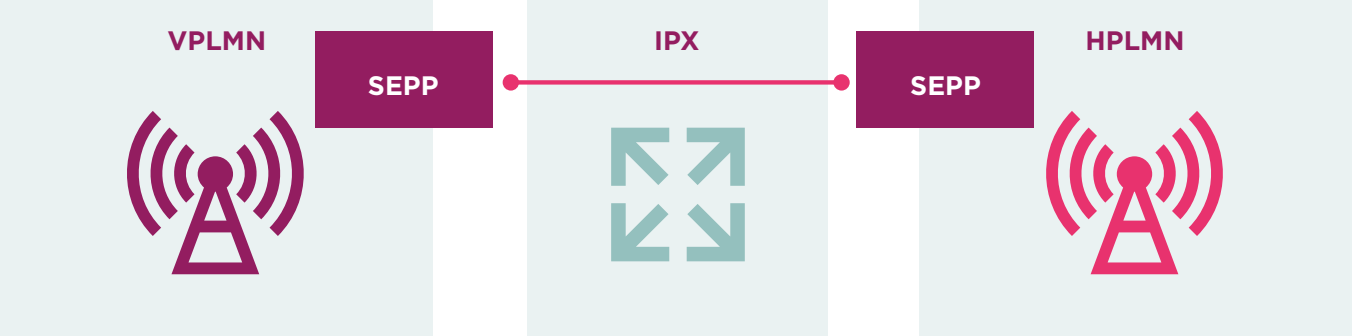
52 https://www.gsma.com/identity/uk-mobile-operators-launch-number-verify

The insecurity of SMS due to reliance on underlying SS7 has affected verticals that rely on SMS as part of their Two Factor Authentication (2FA) processes, notably finance[50]. A recent report[51] highlighted that attackers were able to gain access to Telegram messenger and email data through an SS7 attack targeting subscribers of the Partner Communications Company. This trend highlights the ongoing and legacy nature of this threat as the same threats were reported within industry since 2014. Whilst the transport of SMS is not inherently secure the use of SMS as two-factor authentication is better than only a single factor and other mechanisms such as MSIDN Verify[52] are emerging.

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 16

SECURITY EDGE PROTECTION PROXY



The SEPP is designed to:

- Provide application layer security and protect against eavesdropping and replay attacks.
- Provide end-to-end authentication, integrity and confidentiality protection via signatures and encryption of all HTTP/2 roaming messages.
- Offer key management mechanisms for setting the required cryptographic keys and performing the security capability negotiation procedures.
- Perform message filtering and policing, topology hiding and validation of JavaScript Object Notation (JSON) objects; including cross-layer information checking with address information on the IP layer.
- In addition, enhanced security of the international roaming services are introduced to overcome the existing security risks linked to SS7 and Diameter usage. This introduction of a dedicated security node within the 5G standards is a major improvement over the existing practices in 4G/3G/2G networks using SS7 and Diameter.

Additionally, in support of 5G roaming, operators will need to exchange user plane traffic in a secure tunnel, filter and control their exchange of messages with their roaming partners.

Current signalling protocols will remain in use within the industry for many years to come; as a result, the GSMA recommends that operators implement compensating controls, specifically:

- Provide guidance for consumers and enterprises on the risks of using SMS as a multi factor authentication mechanism
- Implement signalling controls outlined in the GSMA Fraud and Security Group[53] (FASG) guidelines on securing interconnect protocols.
- Have a fraud management system (FMS) to identify, detect and prevent potential fraud transactions within the signalling messages.
- Deploy signalling firewall, or equivalent, technologies to support the monitoring and blocking of signalling traffic.
- Prepare for realistic threat scenarios where the network is compromised. Once these threats are modelled, a set of security parameters, based on the signalling protocols, can be deployed.
- Use 5G deployment programmes to implement new security specifications such as SEPP and user plane protection
- Use 5G deployment programmes to rationalise and close down 2G/3G networks[54]

The GSMA Secure 5G Roaming Solution Task Force[55] aims to secure inter-operator signalling against interception and modification, but balanced with the commercial and operational requirements needed to ensure a globally scalable approach. Additionally, the 5G Interconnect Security[56] group aims to develop and update standardised interconnect security mechanism. Engagement with these working groups can help define best practices and agree secure implementation details.

53 https://infocentre2.gsma.com/gp/wg/FSG/RIF/Pages/Default.aspx

54 Although 4G networks use another signalling protocol (Diameter), they still need to interface with previous-generation mobile networks for converting incoming SS7 messages into equivalent Diameter ones

55 https://infocentre2.gsma.com/gp/wg/IR/5JA/S5G/Pages/TermsOfReference.aspx

56 https://infocentre2.gsma.com/gp/wg/FSG/RIF/N32/Pages/Default.aspx

Securing 5G

5G presents an 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.

This rollout period is a pivotal time, as the approach taken to implement and operationalise the architecture and underlying technologies present 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.

Open networking (discussed earlier) opens new opportunities and threats but may be vital to securing 5G at an acceptable cost.

More and more of a nation's capability and economy is built on telecom networks and the introduction of 5G services is an opportunity to provide a commensurate response.

Worldwide Covid-19 lockdowns have and continue to highlight the reliance on national telecoms networks to deliver resilient and effective connectivity for continued societal and economic good. 5G security needs to be a focus now, as it will be much more difficult to build in security after it is widely rolled out. The introduction of new equipment and the potential for a more diverse supply chain, mean there is potential to introduce configuration related vulnerabilities as 5G is rolled out. To the end of Q4 2020, there have been 135 5G commercial launches in 52 markets, with 25 launches in 17 markets in Q4 2020 alone [57].

The 5G standards[58] outline a service architecture that closes several of the gaps currently being exploited, including fraud and security issues. At present Non Stand Alone deployments are not making full use of the standards based security, as much of this only comes when a 5G core (5GC) is deployed. Therefore, although there is the potential for significant security enhancements, some of the security implementations that 5G can deliver are yet to be realised.

As networks evolve, focus is applied to introducing new capabilities (such as higher bandwidths and low latency) that in turn require virtualised infrastructure and network functions. This focus can sometimes be at the expense of legacy equipment still in service but often builds on top of existing infrastructure (like Non Stand Alone 5G where 5G New Radio is built on top of a 4G core).

Newer and more complex systems will introduce new vulnerabilities but there is a strong focus on deploying these new systems securely[59]. These hybrid networks require consideration as a whole system as security weaknesses in legacy equipment can provide an attack vector into newer systems. For example, older Physical Network Functions (PNFs) may need to trust newer VNFs and both PNFs and VNFs will be susceptible to differing security vulnerabilities, yet both must work coherently and securely[60].

There has been much focus[61] to identify the key threats within 5G networks. There are a range of functions identified as be critically sensitive. These include:

- Virtualisation infrastructure
- Controllers
- Orchestrators
- Internet gateways
- Network slicing
- Mobile Edge Computing
- Routing and switching of IP traffic at the core
- Database functions
- Authentication, access control, and other security functions

These functions therefore warrant the highest levels of protection because a compromise could seriously undermine integrity, availability, or confidentiality.

The GSMA Coordinated Vulnerability Disclosure[62] programme gives security researchers a route to disclose a vulnerability impacting the mobile ecosystem affording industry the opportunity to consider and mitigate threats before they 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.

57 GSMAi Statistic

58 https://www.3gpp.org/release-16

59 See Communications Security, Reliability and Interoperability Council CSRIC VII Report on Risk to 5G from Legacy Vulnerabilities and Best Practices for Mitigation June 2020

60 Explored in s5.17 of 3GPP TR 33.848 V0.5.0 Technical Specification Group Services and System Aspects; Security Aspects; Study on Security Impacts of Virtualisation (Release 16)

61 https://www.ncsc.gov.uk/files/Summary%20of%20the%20NCSCs%20security%20analysis%20for%20the%20UK%20telecoms%20sector.pdf and https://www.enisa.europa.eu/news/enisa-news/enisa-draws-threat-landscape-of-5g-networks

62 https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

5G needs to leverage many technologies and processes already in use, including:

- Apply the range of security considerations identified in the GSMA Whitepaper covering open networking and security of open source software deployments[63].
- The Network Equipment Security Assurance Scheme (NESAS)[64], 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.
- Adopt a zero trust approach[65] for the creation of Trust Relationships between trust domains, between and within the system and can add additional control layers to limit lateral movement and cascaded compromises.
- Supply chain risk assessment and product testing, and ensuring vendors offer appropriate security protection and are accountable for security lapses, especially in disaggregated networks where there may be an increase in the number of vendors.
- Security operations, using Security Orchestration, Automation and Response (SOAR) and embedding 5G data into protective monitoring capabilities.
- Management and network orchestration (MANO), and building of secure templates for server deployments and management. In 5G networks this should be used for network slicing, network function virtualisation and container management.
- Consider cloud security arrangements.
- Consider the whole lifecycle through design, development, procurement, deployment, operations and decommissioning and implement appropriate security for each stage.

These processes should be assessed against the potential 5G threats and be validated to confirm that the security response is sufficient.

Operators should:

- Continue to build 5G networks that comply with 5G standards
- Source network equipment from vendors that have demonstrated a commitment to security and an ability to comply with security requirements defined by schemes such as NESAS,
- Ensure equipment to be deployed at a network level has been independently security evaluated against security requirements, such as those defined by 3GPP in its security assurance specifications.
- Drive industry interoperability to develop economies of scale with regard to security controls
- Use 5G deployment programmes to rationalise and potentially isolate or close down less secure 2G/3G networks
- Join industry initiatives currently developing the implementation models for 5GC and 5G Non Stand Alone (NSA):
  - GSMA Fraud and Security Group (FASG)[66] for the development of the Security Edge Protection Proxy (SEPP)
  - GSMA Networks Group[67] for secure roaming development
  - GSMA CVD[68] for disclosing vulnerabilities impacting the industry

63 GSMA Report Open Source Software Security, January 2021 https://www.gsma.com/futurenetworks/resources/open-networking-the-security-of-open-source-software-deployment/

64 https://www.gsma.com/security/network-equipment-security-assurance-scheme/

65 See also https://www.ncsc.gov.uk/blog-post/zero-trust-principles-beta-release

66 https://www.gsma.com/aboutus/workinggroups/fraud-security-group

67 https://www.gsma.com/aboutus/workinggroups/networks-group

68 https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

Security skill shortage

Mobile network security skills have been in short supply for some time resulting in difficulties for network operators to build and retain in-house expertise, particularly for niche legacy technologies. To address this, operators typically rely on 3rd party expertise by utilising higher-cost contractors and outsourcing to suppliers and systems integrators. The breadth of skills that will be needed in 5G era networks are likely to be much broader (including Artificial Intelligence, big data, IT, Cloud) and will also require the underpinnings of security skillsets in traditional core telco. The threat is that operators will lack the breadth and depth of security skills to comprehensively protect their networks. Developing the right skills to protect future and legacy networks in the current skills shortage is challenging.

> **Two-thirds (64%) of cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants.[69]**
> **Digital, Culture, Media and Sport (DCMS) 2020 Report**

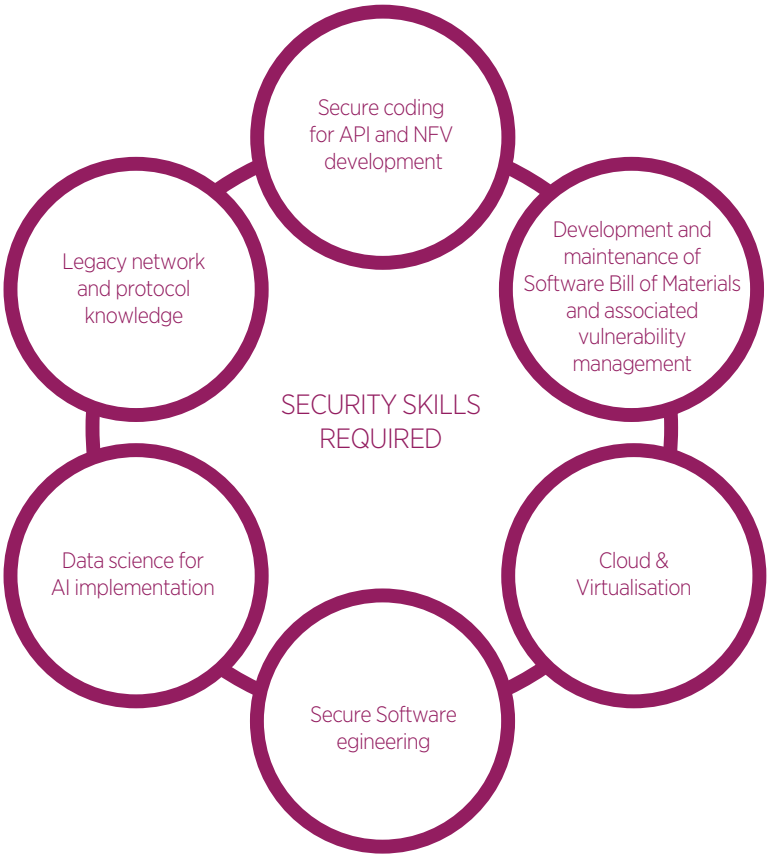
69 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/869506/Cyber_security_skills_report_in_the_UK_labour_market_2020.pdf

Mobile telecommunication networks are some of the most complex, wide reaching and long-standing networks in the world. Increased adoption of cloud security, open source software and virtualised infrastructure brings new skillset requirements more aligned to Information Technology (IT) than telecoms. This also has a potential up-side in enabling operators to draw from a bigger resource pool but that IT skills pool is already a scarce resource. According to a Department for Digital, Culture, Media and Sport (DCMS) 2020 Report: "Two-thirds (64%) of cyber firms have faced problems with technical cyber security skills gaps, either among existing staff or among job applicants"

Each generation of mobile network can often build on top of previous generations[70] and we see 5G Non-Standalone deployments being deployed on top of existing 4G core infrastructure. Mobile networks consist of standardized, open source and proprietary elements with unique configurations and numerous protocols that have developed over five generations. The 5G era revolutionises the way these networks work, introducing new skill requirements yet legacy network generations will remain for years to come; meaning legacy skills need to be retained (see Figure 17). Couple this with persistent advanced threats these networks are subjected to, and the environment becomes a difficult area to resource.

FIGURE 17

SKILLS REQUIRED TO EFFECTIVELY PROTECT A MOBILE NETWORK



70 Although we can see the start of 3G networks being retired to re-farm spectrum more efficiently and build increased network data handling capabilities

To limit the impact of skills shortage, the industry should:

- Model and define the current and future threats, clarify what skills are required to protect against them, and ensure that training plans and skills matrices recognise these required skills.
- Consider the skills development advantage of undertaking new systems integration in-house or with explicit skills transfer built-in.
- Define formal and informal training mechanisms to diversify skills.
- Have a structured skills management capability, focusing on function based skills analysis, highlighting skills gaps. Where gaps are located consider:
  - Build or buy: does the skills gap require immediate externally procured skills or is the threat longer term, allowing the skills to be developed internally.
  - Integrate graduate and apprentice schemes into security skills development.
- Reassess cyber security roles on an annual basis; driving the right knowledge and capabilities within the teams.
- Ensure supplier skill resilience is understood before partnering for strategic initiatives.
- Automate when possible; as a manual security controls matures, consider using automation to remove human touch points. Not only is this more efficient it allows the teams to upskill based on the threats faced.

2021 & Beyond

Network Slicing & 5G Vertical and Private 5G

A network slice is a logical network serving a defined business purpose or customer, consisting of all required network resources configured together. Customer/vertical need defines the characteristics of the slice including data speed, quality, latency, reliability, security, and services. It is created, changed and removed by management functions. Hence network slicing divides an operator's physical network into multiple logical networks. These logical networks would permit the implementation of tailor-made functionality and network operation specific to the needs of each slice customer, rather than a one-size-fits-all approach as witnessed in the current and previous mobile generations which would not be economically viable.

Vertical industries are very diverse, and their requirements are determined by the service features of the related vertical market segment. 5G can provide optimal solutions catering to various requirements and business needs of each vertical in an economical way. It also opens new opportunities for operators to extend their businesses and create new revenue streams beyond connectivity. Mobile operators need to understand how they will secure (and be secured from) 5G verticals/private instances and to package the advanced capabilities of 5G and the configurability of Network Slicing to provide customers with a smart network.[71]

There may be a mix of public and private networks that will allow seamless movement of devices, data and services between the environments and the security should be considered across such boundaries and not be a point of compromise. In many cases private networks may benefit from the inherent security provisions of standards compliant networks.

71 https://www.gsma.com/futurenetworks/wp-content/uploads/2020/01/2.1_Network-Slicing-Use-Case-Requirements-Booklet-1.pdf

Artificial Intelligence

Artificial Intelligence (AI) and Machine Learning (ML) have potential for use in a wide range of telecoms activities including service orchestration, demand management, security response and analytics. Technology advancements such as AI, have the potential to be used in both an exploitative and positive sense. Artificial intelligence and machine learning can be thought of in the same way. Adversarial AI may be developed in a manner to generate new cyber and network attacks. The opposite is also true such that AI is used in a defensive manner to predict and pre-empt attacks. ETSI Securing Artificial Intelligence Industry Specification Group (SAI ISG) has released its inaugural group report[72] that explores the problem statement for AI Security. The GSMA supports the development of applied AI initiatives, especially aimed at sharing insights and developing an expert community in this nascent space.

Quantum Safe Cryptography

The internet trust model has been underpinned by a combination of Public Key Infrastructure, digital certificates and cryptography. It has been responsible for the explosion of conducting a wide range of activities online that would allow businesses, government agencies and institutions to scale up while reducing cost. Quantum computers will be especially good at factorisation of large numbers making them ideally suited to new 'brute force' crypto breaking.

Improvements in computing (Quantum computing) make breaking some cryptographic protocols more practical; meaning communications will become insecure without additional action such as using quantum safe cryptography and exploiting enablers such as Quantum Key Distribution. Whilst the practical implementation of quantum computing may be perhaps 20 years, there is much activity already underway[73] and the latest requirements for cryptographic protocols for mobile telecommunications have been defined with the need to be quantum safe in mind. There is plenty of activity in this area (including in GSMA[74]) and GSMA encourages involvement in the development and considerations of the longer-term strategic view. For example, think about data strategy and how long current data needs to be protected (i.e. is it >20 years) against the speed of technology development.

72 ETSI GR SAI 004 V1.1. https://www.etsi.org/deliver/etsi_gr/SAI/001_099/004/01.01.01_60/gr_SAI004v010101p.pdf

73 https://www.nature.com/articles/d41586-019-02935-4

74 For example, GSMA Document IG.11 Quantum Computing, Networking and Security

Final Thoughts

The 2020 Mobile Security landscape provides a set of recommendations for the Industry to consider 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.

The threats encountered and protection required should not stand in the way of society's desire for technological advancement. Security must stand side by side and support innovation as close to technology conception as possible. This is the only way for secure by design to become common place in the industry.

Threats are not just technical in nature but involve and impact a range of actors across the whole lifecycle that include people, processes and technologies. The response and mitigations must be considered in light of this.

The specific threats discussed in this report relate to technologies that may have been designed with security as a consideration, but still have vulnerabilities that have been exploited and that have resulted in successful attacks. The sophistication of malicious actors continues to grow alongside the growing efficacy of defences and, as always, security has and will be a continuing struggle and 'arms race'. This shows how important it is to ensure security remains in place throughout the lifetime of a product or service and is a continuum rather than a point in time effort.

It is clear that as we enter the 5G era of intelligent connectivity there is great opportunity and capability that must be leveraged to not only continue providing secure, resilient services both in general connectivity as well as feature rich services and collectively as an industry we must execute on such opportunities to ensure that hard earned trust is deserved and maintained.

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

GSMA Industry and Security Standards Activity Areas

GSMA offers its members considerable security[75] expertise and services through a range of activity areas.

Fraud & Security Working Groups

The GSMA's Fraud and Security Group[76] drives the association's management of fraud and security matters related to mobile technology, networks and services, with the objective to maintain or increase the protection of mobile operator technology and infrastructure and customer identity, security and privacy such that the 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.

75 https://www.gsma.com/security/

76 https://www.gsma.com/aboutus/workinggroups/fraud-security-group

Securing the 5G Era[77]

5G has designed in security controls to address many of the threats faced in today's 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 to 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.

Telecommunication Information Sharing and Analysis Center

The GSMA Telecommunication Information Sharing and Analysis Center[78] is the central hub of 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 telecommunication sector. Drawing on the collective knowledge of mobile operators, vendors and security professionals, the T-ISAC collects, disseminates information and advice on security incidents within the mobile community – in a trusted and anonymised way.

Coordinated Vulnerability Disclosure Programme

The GSMA Coordinated Vulnerability Disclosure[79] programme gives security researchers a route to disclose a vulnerability impacting the mobile ecosystem meaning the impact can be mitigated before it enters 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.

77 https://www.gsma.com/security/securing-the-5g-era/

78 https://www.gsma.com/security/t-isac/

79 https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

Security Accreditation Scheme

The Universal Integrated Circuit Card (UICC) in mobile devices, and its applications and data play a fundamental role in ensuring the security of the network, the subscriber's account and related services and transactions.

The GSMA's Security Accreditation Scheme[80] 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[81], 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 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, in particular an appropriate set of security policies covering the whole lifecycle of a network. The scheme should 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.

80 https://www.gsma.com/security/security-accreditation-scheme/

81 https://www.gsma.com/security/network-equipment-security-assurance-scheme/

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators and nearly 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences.

For more information, please visit the GSMA corporate website at **www.gsma.com.**

Follow the GSMA on Twitter: **@GSMA.**

About the GSMA Fraud and Security Team

The team's purpose is to analyse the industry's threat landscape and provide information that enables our member's ability to protect the mobile ecosystem.

The team manage the GSMA's Coordinated Vulnerability Disclosure (CVD) programme, the GSMA's Telecommunication Information Sharing & Analysis Centre (T-ISAC), Security Accreditation Schemes and Fraud and Security Groups (FASG).

For further information, please visit:
www.gsma.com/security

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

March 2021