GSMA

Mobile Telecommunications Security Landscape

February 2024

This is an information paper of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is subject to copyright protection and is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Contents

GSMA CTO Foreword

As 5G usage gathers pace in both consumer and enterprise settings, its benefits will spread across the global economy. We reached more than 1.4 billion 5G connections worldwide at the end of Q3 2023. And, today, over 270 mobile operators in more than 100 markets have launched commercial 5G services. 5G mobile connectivity is expected to add nearly $1 trillion to the global economy by 2030, with almost half of this coming from new enterprise services and apps, across sectors including finance, healthcare, and education.

5G networks deliver as part of a multi-generational evolution of mobile infrastructure. 2G, 3G and 4G networks continue to deliver services across the globe and such connectivity becomes ever more fundamental to our daily lives. As such, the cyber security of those networks is a fundamental technology enabler that is increasingly mandated by governments and requires constant scrutiny and investment to keep pace with the changing threat nature described in this, and previous, GSMA mobile telecommunication security landscape reports.

This threat landscape report plays a key role in communicating the ongoing, evolving and escalating nature of the threats facing our industry. Importantly, the report draws on both public sources and reports from within the GSMA security community. Please take the time to read this report and get involved in our team effort to increase the protection of operator deployed technology and infrastructure, customer identity, security and privacy. 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: 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

GSMA Fraud and Security Group Chair

The past year has been another eventful one in the mobile security world. Conflicts around the globe have often focused on telecoms technologies and services, either as a direct target or as a route to another target. In addition, criminal attacks can and have been devastating; ransomware is a constant anxiety and the techniques for compromising businesses have become increasingly effective, often focusing on individual employees and social engineering.

To circumvent defensive measures, attackers often seek to compromise other parts of the supply chain and abuse the trust relationships between organisations. This is something that we'll need to continue to address as an industry, along with other supply chain considerations such as dealing with deployed, common vulnerabilities in software libraries in an effective and swift manner such that the exposure of attack surfaces is minimal.

We continue to see large amounts of fraud globally, using many different techniques. In almost all of these, including where social engineering is involved, there are underlying technical vulnerabilities that have been discovered and then exploited as some part of the attack chain. Our industry needs to ensure that the intelligence about new and emerging frauds is shared and disseminated quickly and most importantly – acted upon, in order to effectively take the fight to the fraudsters, leaving them very little opportunity to exploit systems and subscribers.

Our job in defending against the threats to mobile is what I call the 'Janus problem'. We are required to both look back at all the legacy systems that we need to protect against old and new attacks, but also to look forward and protect new 5G networks that are being deployed, while thinking about what future network security looks like and what attacks we may face. A key area of focus this year for us was addressing commercial spyware vectors, which often use a combination of old and new technologies. We will continue to identify the techniques, tactics and procedures of these threat actors in order to make the mobile network a hostile environment for them to operate within.

There is an increasing recognition of the importance of mobile telecoms security in protecting critical systems and the consequences of failure for individuals through to businesses. The security actions that we've taken as an industry and the recommendations that we have developed are both mirrored in, and inform cyber security policy development by governments around the world. There is a broad commitment by all to meet the challenges faced, but it is also getting more onerous for businesses who may not have the resources to fix all the many issues, particularly with legacy technologies. This can seem an impossible challenge, however these problems will not go away and there is no hiding from attack – they must be addressed. The GSMA Fraud and Security Group (FASG) is a global community of experts in mobile technologies that can help your company, so please join us and get involved.

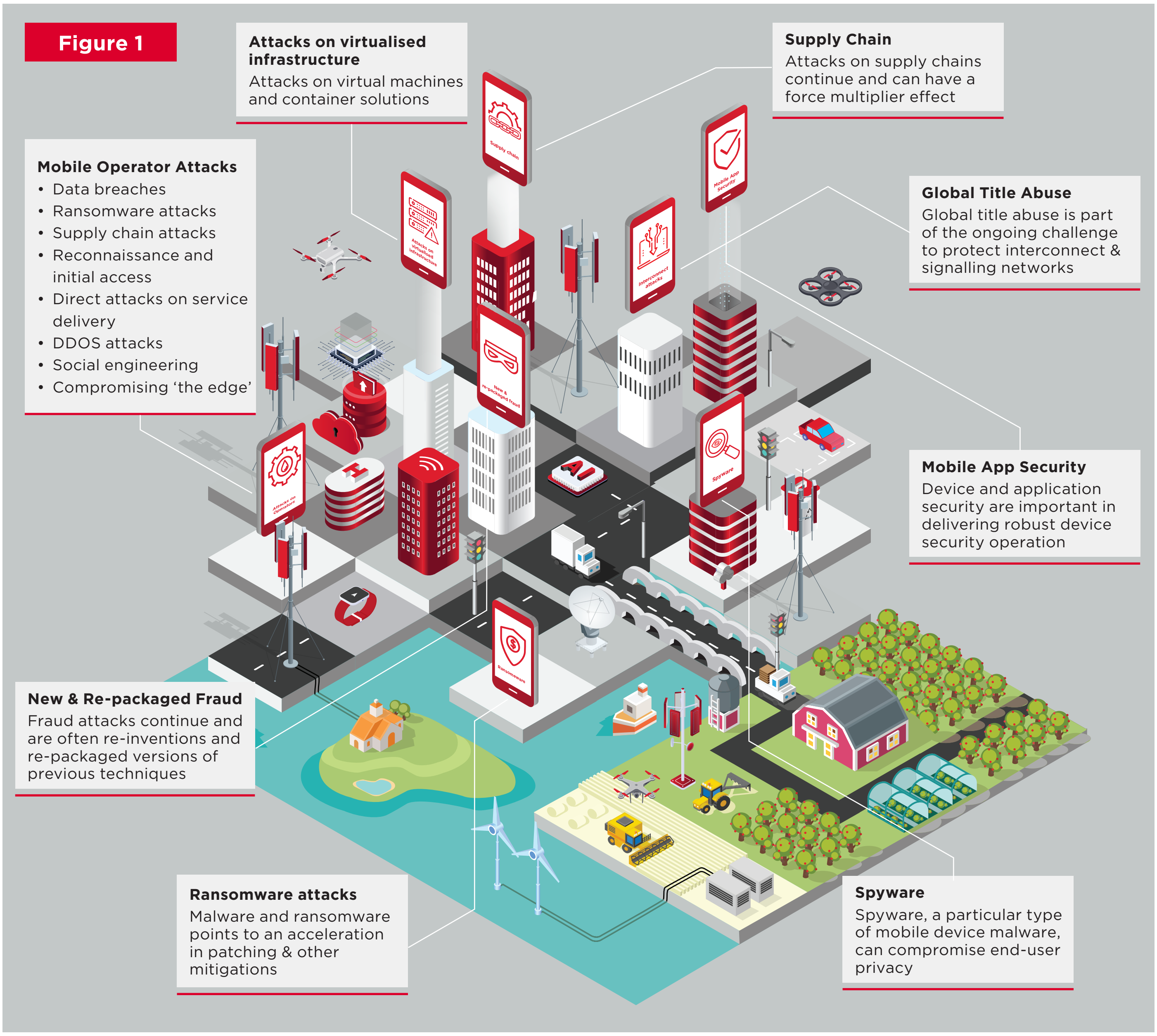
David Rogers MBE - Chair, GSMA Fraud and Security Group & CEO, Copper Horse Ltd

1.0

Key Points

The main topic areas identified in this year's report are shown in this diagram.

Figure 1



Attacks on virtualised infrastructure
Attacks on virtual machines and container solutions

Supply Chain
Attacks on supply chains continue and can have a force multiplier effect

Mobile Operator Attacks
- Data breaches
- Ransomware attacks
- Supply chain attacks
- Reconnaissance and initial access
- Direct attacks on service delivery
- DDOS attacks
- Social engineering
- Compromising 'the edge'

Global Title Abuse
Global title abuse is part of the ongoing challenge to protect interconnect & signalling networks

Mobile App Security
Device and application security are important in delivering robust device security operation

New & Re-packaged Fraud
Fraud attacks continue and are often re-inventions and re-packaged versions of previous techniques

Ransomware attacks
Malware and ransomware points to an acceleration in patching & other mitigations

Spyware
Spyware, a particular type of mobile device malware, can compromise end-user privacy

Malware and ransomware represent a significant, enduring and ongoing threat to the mobile industry, its customers and wider service provider supply chains. The mobile industry (along with all others) has to significantly accelerate its ability to patch and mitigate vulnerabilities.

The security of virtualised and cloud infrastructure is, and will continue to be, vital. A successful attack on such infrastructure can have widespread effects at significant scale.

Securing artificial intelligence/machine learning (AI/ML) platforms, data and algorithms are key protective measures. Beyond that, there is significant potential for generative AI security applications to spot advanced and complex attack types and to counter fraud techniques through advanced analytics. Malicious actors are also highly likely to use AI/ML to generate advanced attack techniques, pointing to a requirement for defensive teams of generative agents capable of engaging in complex real-time defence. Significant and rapid progress is being made in this field, making it a key area of focus.

The report also describes how attack types, such as flubots and phishing, reported in the previous editions of this report are evolving. At the same time, it explores the wider security operating context, which should be allied to the threat topic areas shown in the diagram above.

Near-term actions and investment decisions should be informed by both the current threats and by the emerging wider context. This approach will help ensure investments are efficient and generate longer-term strategic benefits.

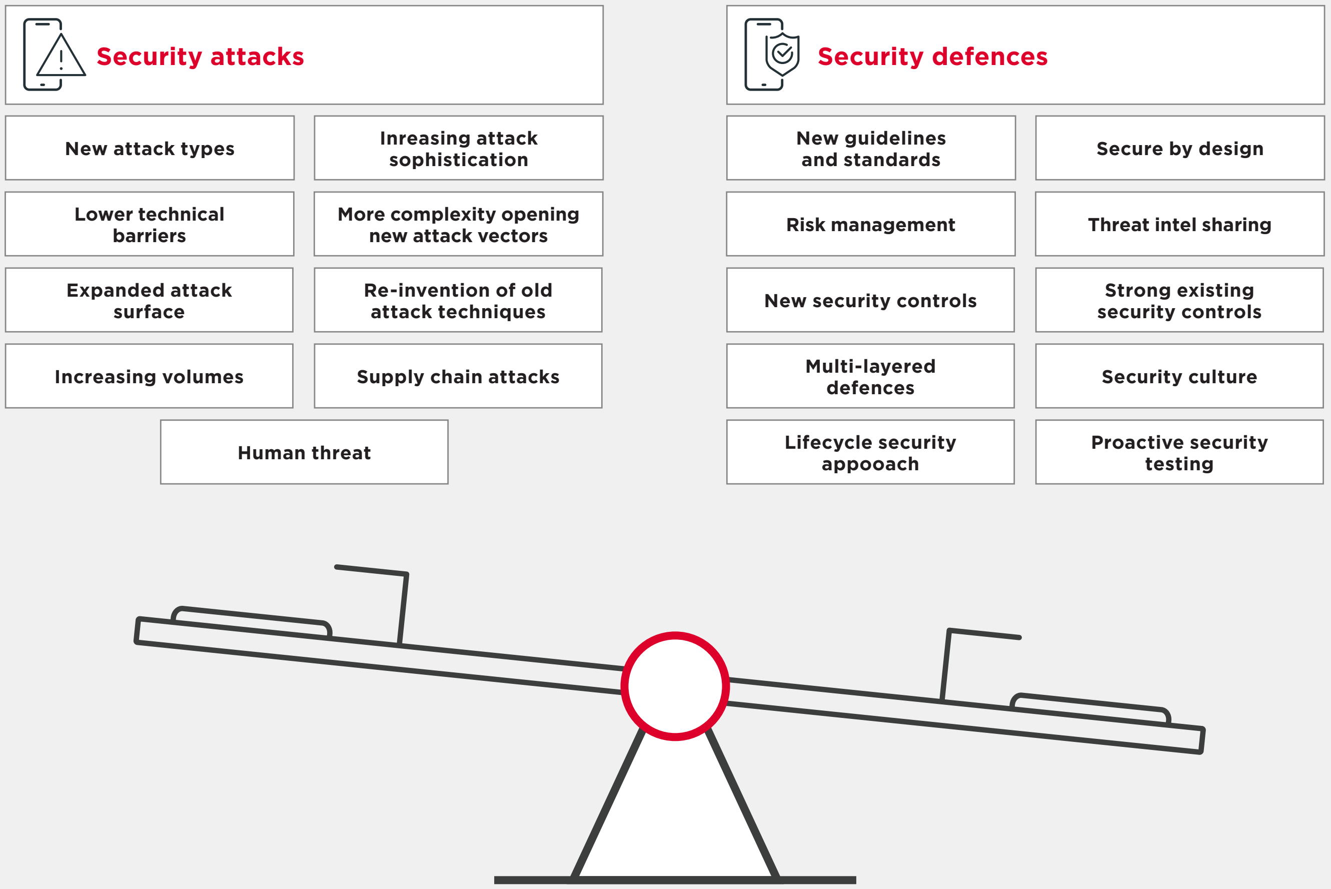
2.0

Introduction

This is the GSMA's sixth annual Mobile Telecommunications Security Landscape report. Building on a number of previous reports[1], it reflects developments during 2023.

As the security landscape changes rapidly, the ongoing challenge is to 'tip the balance' of security in favour of the defenders. Some of the opposing forces - illustrated in the diagram below - are described in this report, although, of course, they do not represent all of the different types of attacks the industry has to deal with, nor all of its defences.

Figure 2



Security attacks

- New attack types
- Inreasing attack sophistication
- Lower technical barriers
- More complexity opening new attack vectors
- Expanded attack surface
- Re-invention of old attack techniques
- Increasing volumes
- Supply chain attacks
- Human threat

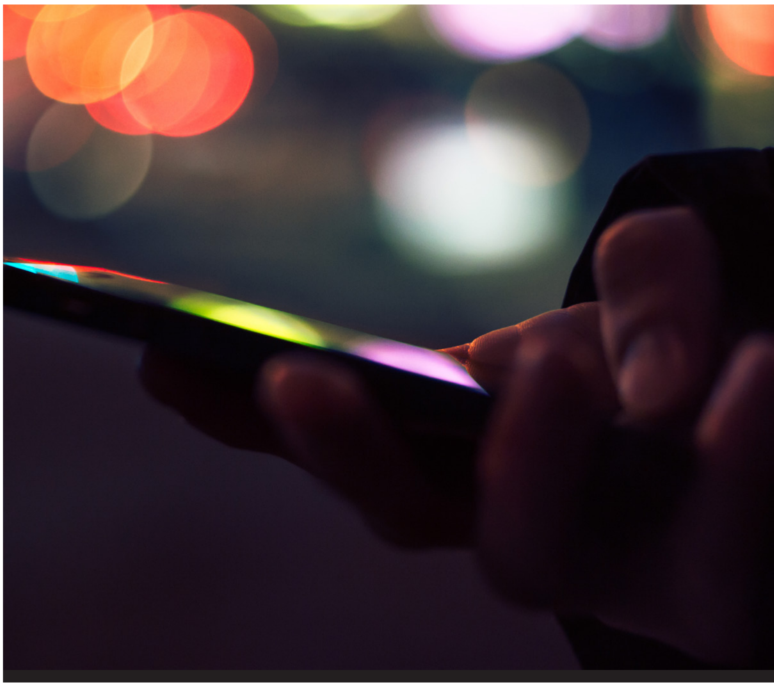
Security defences

- New guidelines and standards
- Secure by design
- Risk management
- Threat intel sharing
- New security controls
- Strong existing security controls
- Multi-layered defences
- Security culture
- Lifecycle security appoach
- Proactive security testing

[1] See GSMA | Publications - Security

This mobile security landscape report does not exist in isolation. Other highly-relevant security landscape reports include:

- The European Union Agency for Cybersecurity (ENISA) Threat Landscape[2]
- The Crowdstrike 2023 Global Threat Report[3]
- The ANSSI State of the threat targeting the telecommunications sector[4]
- IBM Security X-Force Threat Intelligence Index 2023[5]
- The ETIS Security Landscape 2023[6]
- The Zimperium Global Telecom Threat Report 2023[7]



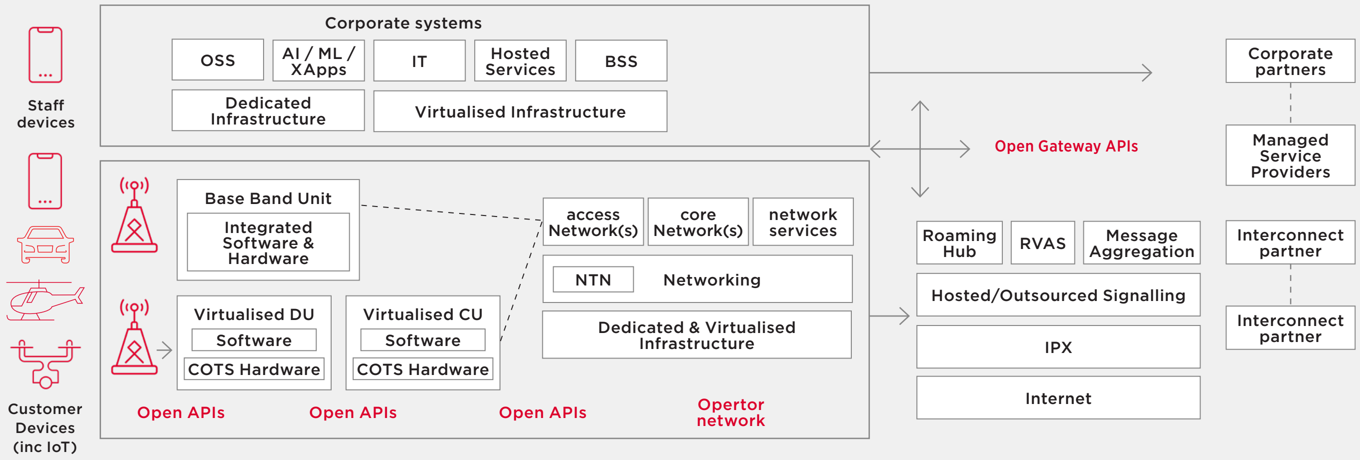
[2] ENISA Threat Landscape 2023 — ENISA (europa.eu)
[3] https://www.crowdstrike.com/global-threat-report
[4] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-010.pdf
[5] https://www.ibm.com/reports/threat-intelligence
[6] https://www.etis.org/sites/default/files/content-files/ETIS-Papers/telco_sec_landscape_2023_published.pdf
[7] https://go.zimperium.com/2023-global-mobile-threat-report

3.0

Attacks on Operators

In order to establish and operate effective security defences, it is necessary to understand the assets that make up the network's attack surface. This includes all the systems (development and operational), people and processes used to operate, design and maintain the network. Network attack surfaces are expanding. There are increasing numbers of connected devices (for example, connected vehicles and IoT equipment), new 5G standalone cores, network application programming interfaces (APIs), open-radio access network (RAN) architectures and new artificial intelligence-enabled services. The diagram below, which illustrates a high-level view of a typical mobile network, provides context for the following sections of this report.

Figure 3



The operational attack surface is wide and complex. Attacks can be launched at many different points externally and from within the network. Mobile network operators (MNOs) have been targeted for many years and these attacks continued in 2023. We can group these attacks into eight types:

- Data breaches
- Ransomware attacks
- Supply chain attacks
- Reconnaissance and initial access
- Direct attacks on service delivery
- DDOS attacks
- Social engineering
- Compromising 'the edge'

A significant number of attacks have primarily targeted customer and staff data that can be further exploited, sold or leveraged. Ransomware attacks can impact access to essential network resources and data, internal servers and communications systems and can result in the unauthorised extraction of data from IT systems. Direct attacks[8], including DDoS attempts, can compromise the availability of services on a temporary or prolonged basis[9]. Operators' employees have been targeted and manipulated into giving attackers access to sensitive systems. Threat actors also seek to compromise 'the edge' of enabling systems (see more on this later). As MNOs have strengthened network security controls and improved end-point detection and response, attackers have pivoted to target devices that support the underlying network infrastructure[10].

Analysis

The attractiveness of both customer and staff data and information makes it an obvious ongoing target for prospective attackers. Other attacks seek to obtain reconnaissance information or an initial network access from which to launch later attacks or gain further access through privilege escalation and lateral movement (in fact the full range of MITRE ATT&CK® adversary tactics[11]).

DDoS attacks[12] aim to overwhelm internet services with more traffic than they can handle, with the goal to disrupt them and make them unavailable to legitimate users. Such attacks have been launched (often with high frequency and large bandwidths[13]) against MNOs[14]. DDoS attacks can be launched via a variety of protocols, including the application layer, network layers, such as IP, transport layers, such as UDP, and via signalling routes. Services are emerging that seek to make launching a DDoS attack easier[15]. Defensive DDoS tools form an important part of network defence and should keep pace with the increasing range and methods of attacks. A common defensive control is to drop packets by routing them to a 'sinkhole' (i.e. the traffic routing is changed such that the packets are dropped rather than allowing onward connection to the target network).

Security controls, such as customisation of defensive tools and proactive security testing, can all play an important role in mounting a successful defence. Attacks via third parties highlight the need to consider the total attack surface for both insourced and outsourced products and services.

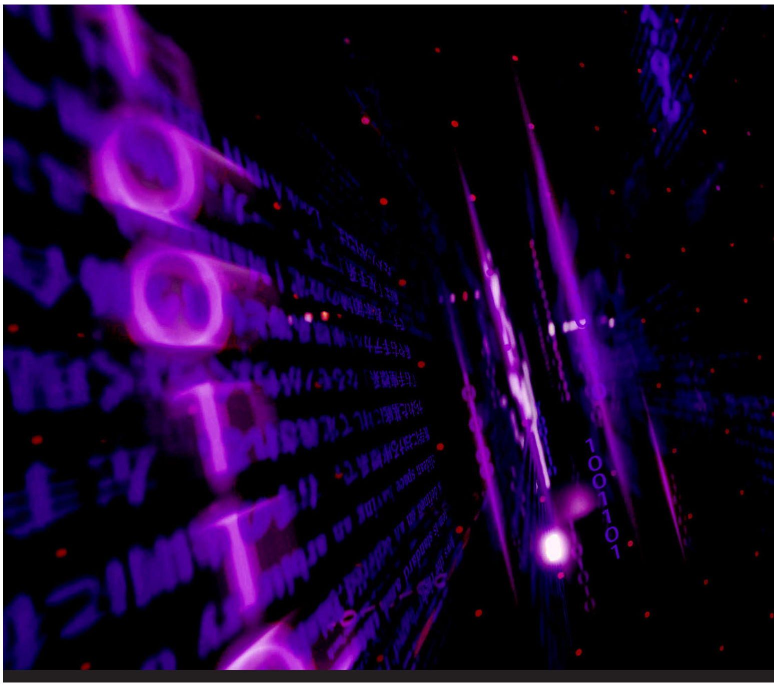
[8] Eg https://www.euractiv.com/section/europe-s-east/news/russian-hackers-were-inside-ukraine-telecoms-giant-for-months-cyber-spy-chief/
[9] For example, the French Cybersecurity agency ANSSI observed an "increase in compromises affecting equipment, particularly routers at the core of operators' networks. These attacks, of a high level of sophistication, are often carried out over a long period of time and are difficult to detect." See full report at https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-010.pdf
[10] Explored more fully in https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02
[11] MITRE ATT&CK®
[12] https://www.imperva.com/resources/resource-library/reports/ddos-threat-landscape-report-2023/
[13] DDoS threat report for 2023 Q3 (cloudflare.com)
[14] For example Ukraine's biggest mobile operator suffers massive hacker attack -statement (msn.com)
[15] German Police Raid DDoS-Friendly Host 'FlyHosting' – Krebs on Security

The extended supply chain continues to be an attractive target (as discussed in a later section) for those intent on inflicting damage.

Attacks that seek to compromise 'the edge' can involve targeting devices such as VPNs, firewalls, Citrix environments, 'jump' boxes, load balancers, proxies, end-points and out-of-band server management interfaces; especially where their management interfaces are connected directly to publicly accessible internet connectivity. These attack types highlight the ongoing need to build strong security defences, including supporting infrastructure and those provided by third parties and managed service providers, and across the whole attack surface and service inventory.

It is vital to build and maintain an accurate and complete inventory of assets and services in order to defend the full attack surface. Resources, such as the Cybersecurity & Infrastructure Agency (CISA) Known Exploited Vulnerability Catalogue[16], can provide useful intelligence on attack vectors that have actually been exploited, rather than more theoretical attack methods.

More broadly, there are extensive existing security defence guidelines available from the GSMA's Fraud and Security Group (FASG). The GSMA has recently comprehensively updated its baseline controls document FS.31[17], which describes a set of effective and proven security controls that have been developed by GSMA members.
More broadly, some interesting new tools can help design the security defence posture. For example, MITRE has released[18] a 'Navigator' tool to assist in the design of cyber resilient systems and the 'Decider' tool to help analysts map adversary behaviour to the MITRE ATT&CK framework.



[16] https://www.cisa.gov/known-exploited-vulnerabilities-catalog
[17] GSMA | FS.31 GSMA Baseline Security Controls - Security
[18] MITRE Releases Tool to Design Cyber-Resilient Systems (darkreading.com) & https://crefnavigator.mitre.org/navigator

4.0

Attacks on virtualised infrastructure

With the rollout of 5G, the industry is migrating to cloud-based network elements and infrastructure. This virtualised infrastructure can be implemented through 'virtual machines' and 'containers'. Containers can provide a process-level separation between workloads that make them quick and cheap to deploy.

As product and function-related software can now run on a range of non-proprietary platforms, operators ensure that whatever combination of hardware and software they use, it stays secure. This includes ensuring that the software is up to date, is running on original and authentic hardware and that it hasn't been altered by an unauthorised party.

Here are some recent examples of attacks on virtualised infrastructure.

- Mandiant reported[19] an incident in Microsoft Azure whereby the attacker employed malicious use of the Serial Console on Azure Virtual Machines (VM) to install third-party remote management software within client environments.
- SentinelLabs reported[20] a threat activity, labelled 'WIP26', targeting telecommunication providers in the Middle East. WIP26 was characterised by the abuse of public cloud infrastructure – Microsoft 365 Mail, Microsoft Azure, Google Firebase, and Dropbox – for malware delivery, data exfiltration and command & control (C2) purposes.
- The Ermetic research team reported three vulnerabilities in the Azure API Management service[21]: two Server-Side Request Forgery (SSRF) vulnerabilities and a file upload path traversal on an internal Azure workload. As the vulnerabilities were shared via coordinated disclosure, they have been fully patched. The GSMA encourages disclosure of vulnerabilities to CVD schemes to enable them to be assessed and patched (where required) before the vulnerabilities are more widely disclosed. The GSMA's CVD scheme[22] provides a mechanism for reporting and addressing industry-wide vulnerabilities that do not affect a single vendor or company.

Analysis

5G is designed to be cloud-native and 6G is likely to further rely on cloud and virtualised network infrastructure. As such, virtualised infrastructure is an important and growing component of mobile networks, as demonstrated by:

- The specification for emerging 5G standalone core networks relying on cloud and virtualised infrastructure
- The O-RAN Alliance specifications[23] include the concept of supporting 'O-Cloud' infrastructure.
- Mobile Edge Compute (MEC) solutions, which move core functions closer to the network edge, usually entailing the use of virtualised infrastructure.

[19] https://www.darkreading.com/cloud/microsoft-azure-vms-highjacked-in-cloud-cyberattack

[20] https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/

[21] The Azure API Management service is a fully managed platform that enables organizations to create, manage, secure and analyse their APIs across all environments

[22] GSMA | CVD Programme

[23] O-RAN Specifications

Correspondingly, some national telecom security regulations have prioritised increased security controls for virtualised and cloud implementations. The cloud providers are responding to these regulations by releasing public documents[24] that demonstrate how their services meet some of the new government mandates.

For containerised deployments, the underlying kernel and resource scheduling is shared between every container running on the host within the same trust domain. However, a single kernel-level vulnerability might allow an attacker to impact the underlying host and, therefore, all concurrent containers. This force-multiplier means that identified vulnerabilities must be remediated as quickly as possible to minimise the attack window and the attack impact. 2023 saw reports[25] from hosting providers and the French Computer Emergency Response Team (CERT-FR) warn that attackers were continuing to target VMware ESXi servers that were unpatched against a two-year-old remote code execution vulnerability to deploy ransomware.

A virtualised, multi-vendor solution-stack may result in security considerations moving from being the responsibility of the network vendor to being the responsibility of the MNO. For example, in the case of an integrated product from a single vendor, the internal design and integration of the hardware platform, virtualisation and software modules are the sole responsibility of the vendor. With a disaggregated approach, the underlying virtualised platform, virtualisation code and application code may be sourced from different vendors. The responsibility for these components working together in a secure manner will rest with the operator (or its systems integrator/lead vendor).

The security of virtualised and cloud infrastructure is, and will continue to be, vital. A successful attack on such infrastructure can have widespread effects at significant scale. However, there is substantial guidance available to help secure virtualised solutions, including how to manage distributed trust relationships. The GSMA has recently updated its Baseline Controls[26] adding further guidance specifically on network function virtualisation and there is ongoing activity within the GSMA's Open Infrastructure Group (closely linked to Linux Networking Foundation's Anuket[27] project). GSMA document FS.33[28] Network Function Virtualisation (NFV) Threats Analysis provides a detailed view of identified threats and guidance on appropriate countermeasures.

[24] E.g. https://d1.awsstatic.com/whitepapers/compliance/Considerations_on_the_UK_Telecommunications_Security_Act.pdf and https://docs.aws.amazon.com/pdfs/whitepapers/latest/security-design-of-aws-nitro-system/security-design-of-aws-nitro-system.pdf
[25] https://www.databreaches.net/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide-more-than-500-systems-affected-already/
[26] https://www.gsma.com/security/resources/fs-31-gsma-baseline-security-controls/
[27] https://lfnetworking.org/anuket-orinoco-released/
[28] A GSMA member-only document

5.0 Supply Chains

A MNO’s supply chain can be broken down into a number of components – from hardware to software - the parties involved in putting together products and services and the upkeep and maintenance of a network. Operational and support IT infrastructure networks are often composed of a variety of products and services from a wide range of suppliers.

Many jurisdictions classify mobile infrastructure as critical national infrastructure, and concerns about national security have increased the focus on the security posture of network equipment and the providers of it. National government responses vary from restricting certain vendors to implementing new defensive regulations / security requirements and attempts to broaden existing vendor arrangements via open networking and other non-proprietary technology initiatives.

Given the many opportunities and targets, supply chain attacks vary widely in nature. Some reported attacks include the following:

Attackers reportedly[29] used information obtained in a previous attack on password manager LastPass US to target a senior DevOps engineer with malware to “launch a coordinated second attack” that breached password vaults. This attack illustrates how reconnaissance and attack staging can be exploited at a later time.

A security breach was reported[30] at a third-party marketing partner of US operator AT&T that led to a compromise of customer proprietary network information, but no sensitive personal or financial information was accessed.

Lumen Technologies, which provides an enterprise technology platform that combines networking, cloud, security and collaboration services, has reportedly[31] fallen victim to attacks. A malicious intruder inserted criminal ransomware into some of the company’s servers that support a segmented hosting service. A separate sophisticated intruder accessed some of the company’s internal information technology systems, including conducting reconnaissance of these systems, installing malware and extracting a relatively limited amount of data.

Analysis

In addition to the general pressure to diversify supply chains, restrictions (and in some cases bans) on using certain vendors is driving vendor swaps - so called rip and replace - in some markets. Whilst there may be advantages from a business reliance viewpoint, the origins and provenance of equipment and services are not a guarantee or substitute for good security. Furthermore, there is a need for balance to ensure any scale changes of vendor are achieved in a resilient, cost-effective manner and utilise robust alternative vendors.

[29] https://siliconangle.com/2023/02/28/lastpass-says-malware-used-hack-devops-engineer-2022-password-vault-breach/
[30] https://forums.att.com/conversations/att-mail-features/is-this-cpni-email-a-phishing-scam/64066deaac6ccc24bdf19e05
[31] https://d18rn0p25nwr6d.cloudfront.net/CIK-0000018926/32a7d44f-2b57-4acc-8307-665dedf21348.pdf

The selection and testing of new vendors/products is therefore a key activity. A common way of demonstrating product security is to build products that are independently assessed under globally recognised product security assurance schemes, such as the GSMA's Network Equipment Security Accreditation Scheme[32] (NESAS). These, in turn, can help avert fragmentation of regulatory security requirements by providing a globally-recognised robust security baseline that all stakeholders can adopt and adhere to.

Vendor selection is also important when considering managed service providers and providers of cloud services. It is crucial to understand the business reliance on these vendors, as they increasingly deliver parts of the security and operational models, introducing new threat vectors. The opportunity for indirect attacks through supplier or third-party tooling and services should not be underestimated and requires vigilance about which third-party tools to use, as well as awareness of the security posture of the third party. The potential force multiplier effect for an attacker across all the target's customers can make a vendor an attractive attack proposition.

The variety of significant supply chain incidents and supply chain threats[33] has prompted the publication of best practices that aim to mitigate supply chain risks. These are notably in the managed service provider area where there may have been implied customer/supplier and/or partner trust arrangements, rather than explicit and enforced security requirements. For example, ENISA has released[34] a supply chain cybersecurity good practices guide, and the UK's National Cyber Security Centre (NCSC) has also released a relevant guide[35]. The combination of government regulatory 'push' and the availability of increasingly valuable supply chain guidance ('pull') assist in the production and maintenance of meaningful and in-depth supply chain management plans. Software Bills of Materials[36] (SBOMs) and Hardware Bills of Materials[37] (HBOMs) can be used as a means to deliver, track and maintain clearer equipment and software supply chains, with additional benefits of tracking licensing and responding to any security vulnerabilities that emerge.

[32] GSMA | GSMA Network Equipment Security Assurance Scheme (NESAS) - Security
[33] For example, as reported in previous GSMA Mobile Telecommunications Security Landscape reports and examples earlier in this section
[34] Good Practices for Supply Chain Cybersecurity — ENISA (europa.eu)
[35] https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security
[36] https://media.defense.gov/2023/Nov/09/2003338086/-1/-1/0/SECURING%20THE%20SOFTWARE%20SUPPLY%20CHAIN%20RECOMMENDED%20PRACTICES%20FOR%20SOFTWARE%20BILL%20OF%20MATERIALS%20CONSUMPTION.PDF
[37] https://www.cisa.gov/resources-tools/resources/hardware-bill-materials-hbom-framework-supply-chain-risk-management

6.0

Global Title Abuse and Interconnect

Signalling systems, such as Signalling System #7 (SS7), are required in some mobile networks to route calls, establish location and access account information and are an evolution of the signalling systems designed for older fixed networks but augmented to facilitate mobility and roaming. Traditionally, the interconnect traffic between mobile operators relied on these underlying signalling protocols for effective operation and utilised an inherent trust model that assumed that only those entities that needed signalling access actually had it. For many years, this trust assumption has not been correct, and operators recognise that attacks can come through their signalling network and their connections to other operators and partners.

The ecosystem[38] supporting the provision of roaming and interconnect services is large, diverse and has complex interactions. Compromised interconnect services have the potential to expose customer data, user data traffic and the intermediaries associated with interconnection and roaming services[39]. The actors involved range from MNOs and MVNOs to transit carriers, GRX/IPX providers, firewall management providers, roaming hubs, roaming Value Add Service providers and messaging aggregators.

In accordance with the recommendations of the International Telecommunications Union (ITU), national numbering plan administrators are responsible for managing their national telecommunications numbering plans. For mobile network signalling purposes, a portion of mobile numbering resources is assigned to a single, unique Global Title (GT) that can then be used for routing signalling messages on telecommunications networks. The practice of leasing GTs (by a “GT lessor” to a “GT lessee”) has enabled additional entities (GT lessees) to gain access to the global SS7 network and to exchange signalling messages using GTs associated with the GT lessor. This reduces routing transparency and has led to concerns that such GT leasing practices can introduce security risks for MNOs and their customers.

During the past year, there have been several reports of GT leasing attacks[40]. It was identified that[41] Fink Telecom was linked to over 100 GTs used to undertake a range of attacks and data compromises, such as those in south east Asia and Israel where the systems were used to take over Telegram messaging accounts and other accounts by redirecting SMS traffic.

[38] More fully described in the earlier Attacks on Operators section
[39] https://citizenlab.ca/2023/10/finding-you-teleco-vulnerabilities-for-location-disclosure/
[40] Finding You: The Network Effect of Telecommunications Vulnerabilities for Location Disclosure - The Citizen Lab
[41] https://www.lighthousereports.com/investigation/ghost-in-the-network/

Analysis

The broader signalling and interconnect security topics (including examples of GT abuse), discussed in the previous edition of the GSMA security landscape report[42], remain very important. Abuse of GTs can also result in the generation of fraudulent artificially inflated traffic (AIT) and the interception of messages used as part of two factor authentication (2FA) to access online accounts. Rather than directly targeting network infrastructure, these attacks can focus on security weaknesses that can compromise end-user privacy.

As part of their efforts to close off routes for attack, GSMA members have developed a GSMA GT Leasing Code of Conduct[43] that describes expected practices from GT lessors. The code is accompanied by explanatory materials to aid understanding[44]. GT lessors and transit carriers involved in GT leasing arrangements are encouraged to voluntarily declare to their partners that they adhere to the GT Leasing Code of Conduct, as evidence of their commitment to routing transparency and to reduce the risks for MNOs and their customers. Operators and carriers that do not lease GTs are also encouraged to publicly declare their support for the Code of Conduct and request compliance by their suppliers and partners (including certain sub-leasing scenarios that are explicitly expected to be prohibited).

[42] GSMA | GSMA Mobile Telecommunications Security Landscape 2023 - Security, pp 23-24
[43] https://www.gsma.com/newsroom/wp-content/uploads//FS.52-v1.0.pdf
[44] GSMA | GSMA Global Title Leasing Code of Conduct - Security

7.0

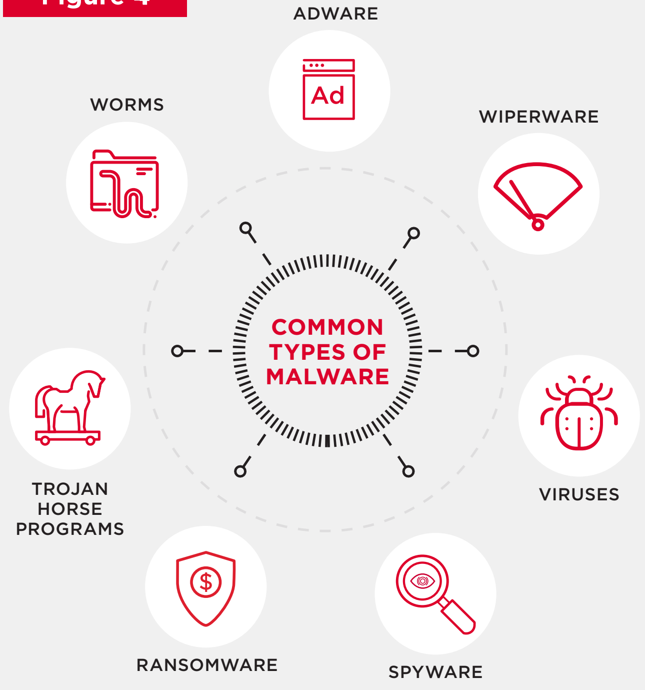
Malware & Ransomware

The wide reporting and severe nature of many malware[45] and ransomware[46] attacks mean this threat continues to be a major security consideration for MNOs and other enterprises. Common types of malware are shown in the diagram below.

A joint report[47] provided a technical analysis of the Infamous Chisel malware that targeted Android devices used by the Ukrainian military[48]. Infamous Chisel comprises a collection of components designed to enable remote access and to exfiltrate information from Android devices (see the joint report[49] by national agencies that provides a technical analysis of the malware). When successfully deployed, it undertakes periodic scanning of files and network information for subsequent exfiltration.

Malware can be engineered to undertake remote code execution and propagate wider fraud attacks by sending smishing messages, as well as other fraud schemes, such as SMS AIT (where large volumes of SMS are sent to high cost destinations) and abuse of direct carrier billing (where the customer's account is used to pay for digital goods and services).

Figure 4



[45] Malware' is short for 'malicious software' and is the generic term for any computer programme that is written with the intent of performing acts on a computing device without the knowledge or permission of the owner or user of that device

[46] Ransomware is a type of remote malware-enabled cybercrime whereby the attacker initiates a successful compromise of a target system, then seeks to extort a ransom payment in return for restoring data, or not exposing or deleting data.

[47] https://www.cisa.gov/news-events/analysis-reports/ar23-243a

[48] https://ssu.gov.ua/en/novyny/sbu-exposes-russian-intelligence-attempts-to-penetrate-armed-forces-planning-operations-system

[49] https://www.cisa.gov/news-events/analysis-reports/ar23-243a

Below are some examples of malware and ransomware attacks in 2023:

- Dish reported[50] a ransomware attack that caused a network outage that affected internal servers and IT telephony and extracted certain data from the corporation's IT systems.
- Lumen reported[51] that a malicious intruder had inserted ransomware into some of the company's servers that support a segmented hosting service.
- Attributed[52] to a campaign named 'Operation Triangulation', one form of malware utilises an undisclosed zero-day exploit in Apple's iMessage platform, enabling it to execute code without user interaction or elevated privileges. Once the device is infiltrated, the malware proceeds to download additional malicious payloads to the compromised device, allowing for further C2 and data collection.
- Roaming Mantis group campaigns have targeted every continent[53], with Africa, Asia, and Europe the most impacted. Additionally, 14 MoqHao[54] malware family C2 servers have been identified, according to some reports. Whilst MoqHao's delivery infrastructure has a short shelf life, its C2 infrastructure has been used for extended periods of time and, in some cases, reused after periods of inactivity.
- Reportedly[55] a new version of a Mirai (IoT botnet) variant called RapperBot has been identified that focuses on installing malware. RapperBot appears to contain large chunks of Mirai source code, but modified to include a new protocol for C2 communications and a built-in feature for brute-forcing SSH servers.

Analysis

Malware and ransomware represent a significant, enduring and ongoing threat to the mobile industry, its customers and wider service provider supply chains. The mobile industry (along with all others) has to accelerate its ability to patch and mitigate vulnerabilities. The time it takes to exploit a vulnerability has moved from weeks to days and there are skilled and motivated groups who are including newly published exploits in their toolkits. Although an accelerated patching process is not a panacea, making this a company priority will mitigate a large number of commonly-exploited attacks.

Related defences include:

- 'sinkholing' known malware download sites,
- ensuring fallback and off-site data recovery arrangements are fully tested and operational,
- implementing network segmentation to make lateral movement harder to achieve,
- deploying technical solutions to detect and block malicious inbound SMS spam to the network
- and providing a well-established route for reporting malware issues to operators where the information should flow through to the cyber-security and fraud teams.

Government action has stepped up too, for example:

- the advent of the StopRansomware[56] initiative and joint advisories[57] for network defenders that detail various ransomware variants and ransomware threat actors.
- UK NCSC Guidance: Mitigating malware and ransomware attacks[58].
- CISA Advisory aimed at stopping ransomware[59] [60].

[50] https://www.sec.gov/ix?doc=/Archives/edgar/data/1001082/000155837023002254/dish-20230223x8k.htm
[51] https://d18rn0p25nwr6d.cloudfront.net/CIK-0000018926/32a7d44f-2b57-4acc-8307-665dedf21348.pdf
[52] https://www.blackhatethicalhacking.com/news/operation-triangulation-malware-strikes-ios-devices-worldwide/
[53] https://www.team-cymru.com/post/moqhao-part-3-recent-global-targeting-trends
[54] This Chinese threat actor is known for its DNS hijacking campaigns, where they "redirect" visitors from websites
[55] https://www.darkreading.com/remote-workforce/new-mirai-variant-employs-uncommon-tactics-to-distribute-malware
[56] https://www.gov.uk/government/news/efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware-joint-statement
[57] For example, this advisory providing known Royal ransomware IOCs and TTPs https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a
[58] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
[59] https://www.cisa.gov/stopransomware
[60] https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware

8.0 Spyware

Commercial spyware[61] is a form of malware that is designed to steal confidential data from the device or appliance it is running on or to access real-time service on the device. Commercial spyware can be used to access a range of personal information and other data to enable threat actors to gain unauthorised access to the services that these credentials are intended to protect. For example, mobile device spyware can steal location data, which then enables tracking of device user location and movement.

This topic was explored in the 2023 GSMA Mobile Telecommunications Security Landscape report and the past year has seen a continuation of this attack type[62]. Spyware has, again, been seen to be deployed against political targets, as reported[63] when an Egyptian presidential candidate was targeted with Cytrox's Predator spyware via links sent on SMS and WhatsApp. This attack reportedly also involved the mobile connection being persistently selected for targeting via network injection attacks (a method to deploy malware including spyware).

Separately, it was reported[64] that at least five civil society victims of QuaDream's spyware had been identified in North America, Central Asia, Southeast Asia, Europe, and the Middle East. The victims included journalists, political opposition figures, and a Non-Governmental Organisation (NGO) worker. Spyware masquerading as modified versions of Telegram have been reportedly[65] identified in the Google Play Store and have been downloaded millions of times. The apps have since been removed by Google. The package name associated with the Play Store version of Telegram is "org.telegram.messenger," whereas the package name for the file directly downloaded from Telegram's website is "org.telegram.messenger.web." The use of "wab" "wcb" and "wob" for the malicious package names highlights typo squatting techniques to fraudulently position the application as the legitimate Telegram app.

Analysis

A range of national and regional responses have been taken including a joint declaration[66] by the governments of Australia, Canada, Costa Rica, Denmark, France, New Zealand, Norway, Sweden, Switzerland, the United Kingdom, and the United States, recognising the threat posed by the use of commercial spyware and the need for strict domestic and international controls on its proliferation and use. The EU's PEGA Committee concluded its spyware investigation[67] and identified eight recommendations[68] (including revoking the licenses of (2G – 5G) service providers found to be facilitating unlawful access to mobile signalling infrastructure and regulating the processes through which malicious actors can create new phone numbers).

[61] Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)
[62] https://www.brusselstimes.com/729331/european-parliament-president-targeted-by-predator-spyware
[63] https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/
[64] Sweet QuaDreams: A First Look at Spyware Vendor QuaDream's Exploits, Victims, and Customers - The Citizen Lab
[65] Millions Infected by Spyware Hidden in Fake Telegram Apps on Google Play (thehackernews.com)
[66] Efforts to counter the proliferation and misuse of commercial spyware: joint statement - GOV.UK (www.gov.uk)
[67] EUROPEAN PARLIAMENT DRAFT RECOMMENDATION TO THE COUNCIL AND THE COMMISSION following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware | B9-0260/2023 | European Parliament (europa.eu)
[68] EU's PEGA Committee Adopts 8 Recommendations on Telecom Networks | Enea

Investigations by journalists and Google's Threat Assessment Group[69] (TAG) have also assisted in identifying and constraining this threat.

This is an ongoing threat that significantly impacts device user privacy and even individuals' personal safety if they are targeted. Whilst it is challenging for the mobile industry to respond to the most sophisticated attacks, GSMA and industry activity is focused on the underlying security arrangements in order to make mobile networks hostile environments for threat actors to operate within (as outlined in the mobile app security, malware and ransomware sections of this report). The supporting security controls and approaches described therein can deliver wide-ranging and enduring operational security benefits to counter the spyware threat.

[69] E.g. https://blog.google/threat-analysis-group/0-days-exploited-by-commercial-surveillance-vendor-in-egypt/

9.0

Mobile App Security

Now there are more than 6.7 billion smartphones in use worldwide, with 5% growth year-on-year[70], the need for a strengthened mobile application security posture is more evident than ever. When consumers purchase a new smartphone, many give consideration to security, privacy and data protection[71]. Overall smartphone security can be considered as a combination of the security of the operating system, the device platform and interfaces, the security of installed software, mobile network security services and the user actions in operating the device.

Smartphones typically run both pre-installed and user-loaded applications. Software application security is therefore an important factor in the overall secure operation of the device. Smartphones usually contain up to four types of apps:

- pre-installed system permission apps which cannot be uninstalled by the device user
- pre-installed non-system permission apps which can be uninstalled by the device user
- Device user apps installed from a controlled source (e.g., the App Store or Google Play)
- Device user apps 'sideloaded' directly to the device[72]

Google evaluates apps on the Google Play Store and estimates[73] that less than 1% of all downloads from Google Play are potentially harmful applications (PHAs). One way in which bad actors attempt to circumvent Google Play's security controls is through versioning. Versioning occurs when a developer releases an initial version of an app on the Google Play Store that appears legitimate, but later an update is pushed from an attacker-controlled server, changing the code on the end user device that enables malicious activity. Another example from the same report[74] highlights dynamic code loading (DCL) as an attack method that enables attackers to download and execute code not included in the original application after installation. This technique enables an attacker to evade static analysis and pre-publication checks. One malware variant using this technique is SharkBot, which initiates money transfers from compromised devices.

Meanwhile, the Open Worldwide Application Security Project (OWASP) has published[75] its initial release of the top 10 mobile risks, which include inadequate supply chain security, improper credential usage and insufficient data storage. The OWASP[76] Mobile Application Security Verification Standard[77] (MASVS) is a community-led initiative for mobile app security. It can be used by mobile software architects and developers seeking to develop secure mobile applications, as well as security testers to aid completeness and consistency of test results.

[70] From GSMAi statistics and forecasts
[71] 7 things you need to know before you buy a mobile phone - Which? News
[72] Google Online Security Blog: Enhanced Google Play Protect real-time scanning for app installs (googleblog.com)
[73] https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf
[74] https://services.google.com/fh/files/blogs/gcat_threathorizons_full_jul2023.pdf
[75] https://owasp.org/www-project-mobile-top-10/
[76] a nonprofit foundation that works to improve the security of software
[77] https://github.com/OWASP/owasp-masvs/releases

Following a consultation in 2023, the UK government will request that the app industry sign-up to a new code of practice that aims to boost security and privacy requirements on all apps and app stores available in the UK. The voluntary code of practice[78] for app developers and operators aims to protect the UK's app market.

Analysis

Robust device security operation is important given the high volume of smartphones and apps in use. The GSMA has established a Mobile Device Security Certification (MDSCert) working party to start assessing this topic. This MDSCert group has:

- analysed existing device certification programmes.
- investigated the market/regulatory needs for varying assurance levels by conducting a gap analysis.
- liaised with ETSI TC Cyber and provided input into a revised version of ETSI's consumer mobile device protection profile specification[79].
- conducted a consumer-focused study that was run across 11 markets with over 22,000 participants.
- documented the essential requirements and methodologies for a smartphone security certification scheme.

Device certification and labelling have significant potential to raise consumer awareness of device security capabilities. As this area matures, consumers can expect to see greater device security transparency and additional information that can inform subsequent purchase decisions and in-life device security operation.

In the UK, the voluntary code of conduct for app store operators and developers sets out seven practical steps to protect users. In combination with the MASVS programme and application repository protection services, such as Apple's built-in App Store controls and Google Play Protect[80], there is potential to create a stronger baseline for mobile application security that complements the previously described device security needs.

As side-loaded apps may not have the additional security assurances available from controlled sources, particular care should be applied to side-loaded installations.

[78] https://www.gov.uk/government/news/new-rules-for-apps-to-boost-consumer-security-and-privacy
[79] https://www.etsi.org/deliver/etsi_ts/103700_103799/10373201/02.01.01_60/ts_10373201v020101p.pdf
[80] https://developers.google.com/android/play-protect

10.0

New and Repackaged Fraud Types

Securing mobile infrastructure, devices, services and customers is an evolving activity, as threat actors constantly re-invent previous attack techniques, as well as inventing new attack types. Repackaged and re-imagined attacks seek to build on previous attacks but are disguised in new ways. This section explores a few of these repackaged attack types, which can be categorised as fraud, as they either fraudulently use mobile services or defraud mobile customers directly. Extensive measures are employed to limit the customer impact of fraud and avoid a negative impact on mobile operators' reputations.

Artificial Inflation of Traffic[81] is a type of SMS fraud seeking to generate high volumes of fake traffic via mobile applications or websites and then profit from higher revenue from the artificially-generated SMS traffic. For example, the fraudster exploits application-to-person (A2P) SMS verification, where a one-time password is sent to verify users' phone numbers during the registration process, then takes a share of the profits from the traffic, while the enterprise incurs inflated A2P SMS costs without added value.

An SMS text blast sends a message to a large group of people simultaneously. However, relatively low-cost, portable and easy-to-use fake mobile base transceiver stations (SMS blasters) can be used for fraudulent use[82]. These have been more traditionally used as IMSI-catchers[83] to spam mobile phones located within the transceiver's radio coverage area with fraudulent SMS messages. The relatively low level of technical skill involved in the use of these SMS Blaster devices has resulted in increased deployment of this attack type.

A 'flash SMS' is a special type of text message that displays immediately on the mobile phone screen without the user having to take any action to read it, even if the screen is locked. A Flash SMS also does not leave a record on the customer's phone i.e., it is not visible in the SMS inbox. Whilst there are legitimate uses for flash[84] SMS messages, they can also be used as part of a fraud attack as a 'convincer' aimed at fooling the mobile user into undertaking an action to further an ongoing scam.

Quishing, a combination of quick response (QR) code and phishing, is an attack technique that leverages QR codes to mislead users into interacting with malicious digital content. When a user scans a malicious QR code, it typically redirects them to an attack website[85], which may deploy malware or solicit log-in or personal information. When contained within an email, Quishing can be effective, as QR codes may not be scanned by traditional email security controls.

The GSMA has previously reported[86] on flubot attacks, often observed as blended attacks

[81] https://mobileecosystemforum.com/2023/01/12/artificially-inflated-traffic-the-latest-menace-in-sms/
[82] https://commsrisk.com/criminal-gangs-drive-imsi-catcher-sms-blasters-around-vietnam/
[83] https://commsrisk.com/oslo-imsi-catcher-arrest-suspected-malaysian-spy-now-investigated-for-fraud-with-international-ramifications/
[84] https://thesmsworks.co.uk/blog/flash-sms/
[85] https://www.linkedin.com/pulse/quishing-how-qr-code-phishing-form-social-engineering-ebenezer
[86] GSMA | T-ISAC Insight Report: Flubot - Security

combining smishing and voicemail lures, with banking malware injects. The 'lures' have been frequently framed in a message relating to a fake parcel or package delivery. Although some of the original flubot infrastructure has been taken down, the attack approach appears to have been re-invented on new infrastructure using new fraudulent messages. For example[87], these messages might impersonate family members asking for money or be framed as a Ramadan Competition[88] on WhatsApp.

The Qakbot banking trojan malware was primarily spread through phishing emails and malicious attachments. It was reported[89] that Qakbot has now started using OneNote .one documents in attacks.

Vendor email compromise (VEC) is a type of phishing attack where an attacker gains access to a vendor's business service account, and then, uses that account to spread malicious emails to the vendor's customers[90]. VEC can target entire supply chains by:

- Hijacking email accounts belonging to vendor employees.
- Setting forwarding rules or monitoring the inbox.
- Creating a spoofed domain to resemble the vendor's.
- Sending well timed messages to customers of the vendor, requesting changes to payment details.
- Using Office 365 tools to enhance the look and feel.

Reportedly[91], attackers have used VEC to spread phishing sites and to appear as legitimate as possible. Malicious emails were sent to multiple recipients, who appear to be customers or prospects of the company, and thus they are more likely to trust compromised emails from the vendor.

Analysis

The re-invention and repackaging of previously observed attack types means constant vigilance is required to respond to these new indicators of compromise (IoCs). The GSMA's Telecommunications Information Sharing and Analysis Center (T-ISAC)[92] community delivers a safe and secure platform on which to share new IoCs in real-time. In this way, a defensive force-multiplier can be delivered by sharing new knowledge that can benefit the wider range of stakeholders.

The GSMA's Fraud and Security Group has an intelligence sub-group that reviews and shares a range of reported security and fraud attack types. This regular sharing of attack techniques allows new modus operandi to be identified and evaluations made on the effectiveness of deployed security and fraud controls.

These agile operational security responses can involve tailoring and adapting existing control mechanisms, re-configuring existing security solutions or building the business case to install new capabilities.

[87] https://www.which.co.uk/news/article/notorious-hi-mum-and-dad-scam-spreads-from-whatsapp-to-text-message-an7N34c0gVbP
[88] https://theclearevidence.org/technical-resources/beware-of-ramadan-competition-fraud-messages-on-whatsapp-english/
[89] https://news.sophos.com/en-us/2023/02/06/qakbot-onenote-attacks/
[90] Closely related to Business Email Compromise (BEC). In a BEC attack, the scammer poses as a trusted figure and uses email to trick someone into sending money or divulging confidential company info. A VEC attack, the attacker gains access to a vendor's email account and uses it to send fraudulent emails to the organization.
[91] https://www.paloaltonetworks.com/blog/security-operations/behind-the-curtains-of-a-vendor-email-compromise-vec-attack/
[92] GSMA | - Security

11.0

The emerging security operating context

The appropriate levels of security investment in new areas and maintaining existing controls depend on many factors including the security threat landscape, risk appetite, maturity of existing controls, available budget, skills and the wider operating context.

A review of the security topics, case studies and threats identified[93] in this, and the previous five, security threat landscape reports[94], highlights a number of trends and focus areas that inform security actions:

TOPIC AREA	2024	2023	2022	2021	2020	2019
Signalling	Signalling & interconnect (inc GT)	Signalling & Interconnect (inc GT)	Signalling & Interconnect	Signalling & interconnect	Signalling & interconnect	Signalling & interconnect
Supply Chain	Supply Chain	Supply Chain	Supply Chain	Supply Chain	Supply Chain	Supply Chain
Cloud & virtualisation	Cloud / virtualisation security	Cloud / virtualisation security	Cloud / virtualisation security	Cloud / virtualisation security	Cloud / virtualisation security	Cloud / virtualisation security
Operational attacks	Operator Attacks	CNI Attacks	Operator Security	Operational security		Privacy & data protection
Device & app security	Mobile App Security	Mobile App Security		Device security	Mobile App Security	Device security
IoT			IoT Security	IoT Security	IoT Security	IoT Security
Fraud	New & re-packaged fraud	Fraudulent SIM and eSIM Swap	Fraudulent SIM Swap			
Malware	Malware (inc Ransomware & Spyware)	Malware (inc Ransomware & Spyware)	Malware (inc Ransomware)			
Software security			Software security	Software security	Software security	
Securing 5G			Securing 5G	Securing 5G	Securing 5G	
Smishing	Smishing	Smishing	Smishing			
Human Threat		Human Threat				Human Threat
Security Skills shortage				Security Skills shortage	Security Skills shortage	

[93] Titles modified somewhat to aid in presentation
[94] GSMA | Publications - Security

Signalling, roaming & interconnect security has been an ever-present topic in all reports and is highly likely to remain an important area as established network signalling technologies will be in place for some time. The GSMA has published guidance for its members on how to reduce the risks associated with interconnect signalling, particularly in relation to deploying and using SS7 and DIAMETER signalling firewalls. For 5G, the implementation of security edge protection proxy (SEPP) has the potential to significantly improve roaming security.

Similarly, **supply chain security and cloud/virtualisation security** have featured in every report, and they will continue to be priorities as third party service providers and cloud providers deliver key elements of MNOs' network services. Although **software security** hasn't been highlighted in recent reports (where the focus has been on app security), emerging and future networks will have a number of fundamental components in which software security (including open-source code), binary equivalence, secure roots of trust and software bills of materials will be key components.

Examples of **operational attacks** on mobile networks appear frequently in the reports, with an apparent rise in **malware** (including ransomware, spyware and wiperware) an important recent trend. **Smishing** and **phishing** represent common attack techniques through which **malware** of all types can be delivered.

Topics, such as **fraudulent SIM** and **eSIM swap**, are frequently reported as they have had some success in bypassing multi-factor authentication. **The repackaging of existing fraud** and attack methods (such as phishing, malware and signalling attacks) and the ongoing attractiveness of personal data points to the continuation of these attacks. Current controls can be updated and maintained to address these threats without significant new investments.

Device (including IoT equipment) and app security has regularly featured in the security landscape reports. The growth in device numbers (through increases in mobile adoption, connected vehicles, and IoT devices more generally) mean this area will be an enduring topic in years to come.

The **human threat** has appeared in reports and as technical security controls become more effective; human beings can become the weakest link in the security risk profile. A range of security controls can be established, which should include staff vetting, additional administrator controls, operating a 'least privilege regime' and guidance for staff on what information they make public that could make them a target.

The difficulty in obtaining sufficient **security skills** was referenced in the early landscape reports. The 5G era transforms the way networks work, introducing new skill requirements, yet legacy network technologies will remain in use for years to come; meaning legacy skills and knowledge need to be retained.

All the areas highlighted in the GSMA's mobile telecommunications security landscape reports continue to be important. While security defences and controls are improving, a number of factors are driving an increased threat. These factors include an expanding attack surface, increased numbers of devices, new architectural components, re-invention of fraud and security attack types and lower technical barriers to attack. The net effect is an ongoing requirement to improve network security controls to keep pace with the security challenges. It is a time to push on with improved security defences.

9.1 A Forward Look

Future networks will have a number of fundamental components where security may require a re-evaluation of current controls: cloud infrastructure, software (including open-source code), binary equivalence, secure roots of trust, software and hardware bills of materials, open API and RAN interfaces and AI/ML security and control implementations. This section discusses the nature of these areas and points to their ongoing strategic importance and the need for a re-evaluation of current controls to deliver an enduring and strategic security response. Topics are highlighted in bold font to assist identification.

Secure software coding for virtualised infrastructure will be important, requiring a re-evaluation of current controls from a lifecycle perspective[95], including secure-by-design, secure coding, **DevSecOps** processes, robust management and use of open-source software, configuration management, platform hardening and in-life patching and updates. Mandating and applying secure coding principles will assist in building the security foundations of the operational software.
Binary equivalence of software is an important area where a re-evaluation may be required to ensure the deployed software is identical to that tested and developed previously.

Configuration Management (CM) of infrastructure and code may also require a re-evaluation of current controls. Important CM concepts include having clear records of deployed and connected servers, software and other equipment, including the services that are supported. This can be tracked using machine-readable **hardware bills of material** (HBOM) and **software bills of material** (SBOM) for deployed software (including open-source components). SBOM and HBOM tooling can be used to handle BOMs from multiple components, each potentially changing rapidly. **Open-source software**[96] is a prime component of many software modules and applications and its management will be key.
The need for secure open source code development and maintenance points to the continued involvement of commercial open-source code vendors.

[95] Discussed in detail in the GSMA document Open-Source-Software-Security_v1.0.pdf (gsma.com)
[96] A subject explored in more detail in the GSMA report GSMA | Open Networking & the Security of Open Source Software Deployment - Security

Cloud and virtualisation services security are particularly important for 5G networks in which the architecture has been designed to operate in a virtualised environment. The potentially wide-scale deployment of such virtualised solutions points to the need for a strong control-set to minimise the opportunity for bad actors to effect wide-scale disruption. Establishment and preservation of a secure root of trust is essential to protect the integrity of the solution from 'bottom to top'. The correct workload code should be running through the right virtualisation platform and operating system and through to any underlying trust arrangements (e.g., to support secure boot processes).

Virtualised networks are a key enabler for **network slicing and private 5G solutions**. As such networks are virtually partitioned, they can flex dynamically as required and are able to support differing service levels that match client requirements, including private 5G and mobile edge compute (MEC) solutions. Underlying cloud security is a fundamental enabler for sliced networks. However, the security strategy must also preserve inter-slice security and reflect the shared security responsibility that may be required for private 5G networks. The private networking components must serve to deliver end-to-end security, protecting the mobile infrastructure whilst delivering an end-to-end service.

Artificial intelligence (AI) and **machine learning** (ML) have a wide range of real, potential and emerging mobile telecom security and fraud applications, such as the OpenRAN Alliance's **RAN Intelligent Controller (RIC)** and **XApps**[97]. Securing the AI/ML platform[98], data and algorithms are key protective measures. Beyond that, there is significant potential for generative AI security applications to spot advanced and complex attack types and to counter fraud techniques through advanced analytics. There are a number of more advanced use cases of Large Language Models (LLMs) although currently, there are scalability, cost and production environment challenges. LLMs could be combined with reinforcement learning to train agents to perform tasks (as opposed to language models that mainly support knowledge queries and natural language processing). AI/ML are highly likely to be used to generate advanced attack techniques, pointing to a requirement for teams of generative agents to engage in complex real-time defence. Significant and rapid progress is being made in this field, making it a key area of focus.

Governments and national regulators are responding to the perceived need for increased **vendor diversity** in network infrastructure by placing requirements on all operators to increase the levels of security and controls. This can include new **supply chain requirements** to manage operators' use of 'high risk vendors' or to ensure 'trusted source' suppliers are used. The **internal security maturity of managed service providers** (MSPs) is also a key factor in supply chain security. Supply chain security factors will remain important for the foreseeable future, especially as "as-a-service" solutions become more widely deployed. Hence, robust supply chain security management requirements, processes and audits are fundamental.

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** and point to this area becoming a higher priority.

The **expanding attack surface** includes the supply chains, disaggregated radio access networks (including O-RAN and virtualised RAN) and the increasing number of connected devices, including smartphones, autonomous vehicles and other IoT equipment. The growing deployment of network APIs, such as GSMA's Open Gateway[99] initiative, and the increasing utility and coverage provided by non-terrestrial networks (NTNs) (i.e. satellite connectivity) are also expanding the attack surface and may require a re-evaluation of current controls.

[97] O-RAN Downloads (orandownloadsweb.azurewebsites.net)
[98] GR SAI 009 - V1.1.1 - Securing Artificial Intelligence (SAI); Artificial Intelligence Computing Platform Security Framework (etsi.org)
[99] GSMA | GSMA Open Gateway - Future Networks

The security of submarine cables is an area of focus due to their prime importance for internet and voice connectivity. The negative effects and massive impact of cable failure or sabotage are clear[100]. Hence, a cohesive cable restoration strategy and wider service continuity plan (e.g., using alternative routing and NTNs) are essential in order to protect service delivery should a successful cable attack occur.

The mobile industry has long aimed to deliver robust security arrangements to protect its assets, customers and services, employing a **security lifecycle approach** starting well before a service goes live. The foundations of security are built through architectural design choices, choosing to adopt solutions that utilise internationally-recognised standards and shortlisting vendor solutions that already have a strong baseline security level built in. A recent GSMA report[101] examined how engaging in industry security assurance/certification schemes, defining international standards and developing industry security best practice guidance combine to deliver an enduring long-term benefit. The report highlighted the need for greater mobile operator engagement to ensure industry schemes meet operator needs. Ultimately the operators are the customers of assurance and certification initiatives, and they absorb the costs of these schemes (regional or global), regardless of whether they were initially involved in their creation.

Cryptographically Relevant Quantum Computers (CRQC) could pose potential new threats to telecommunication systems[102] and significant new cybersecurity challenges. They have the potential to disrupt widely-used encryption algorithms and protocols. An important first step is understanding an operator's quantum risk exposure[103] and building a detailed **quantum secure cryptography** (QSC) inventory. This will assist in understanding the current cryptographic usage and the scale of investment that may be necessary to implement a longer-term response plan.
The development of the strategic response may require a re-evaluation of the current status in order that an orderly and efficient QSC roadmap can be planned, developed and delivered.

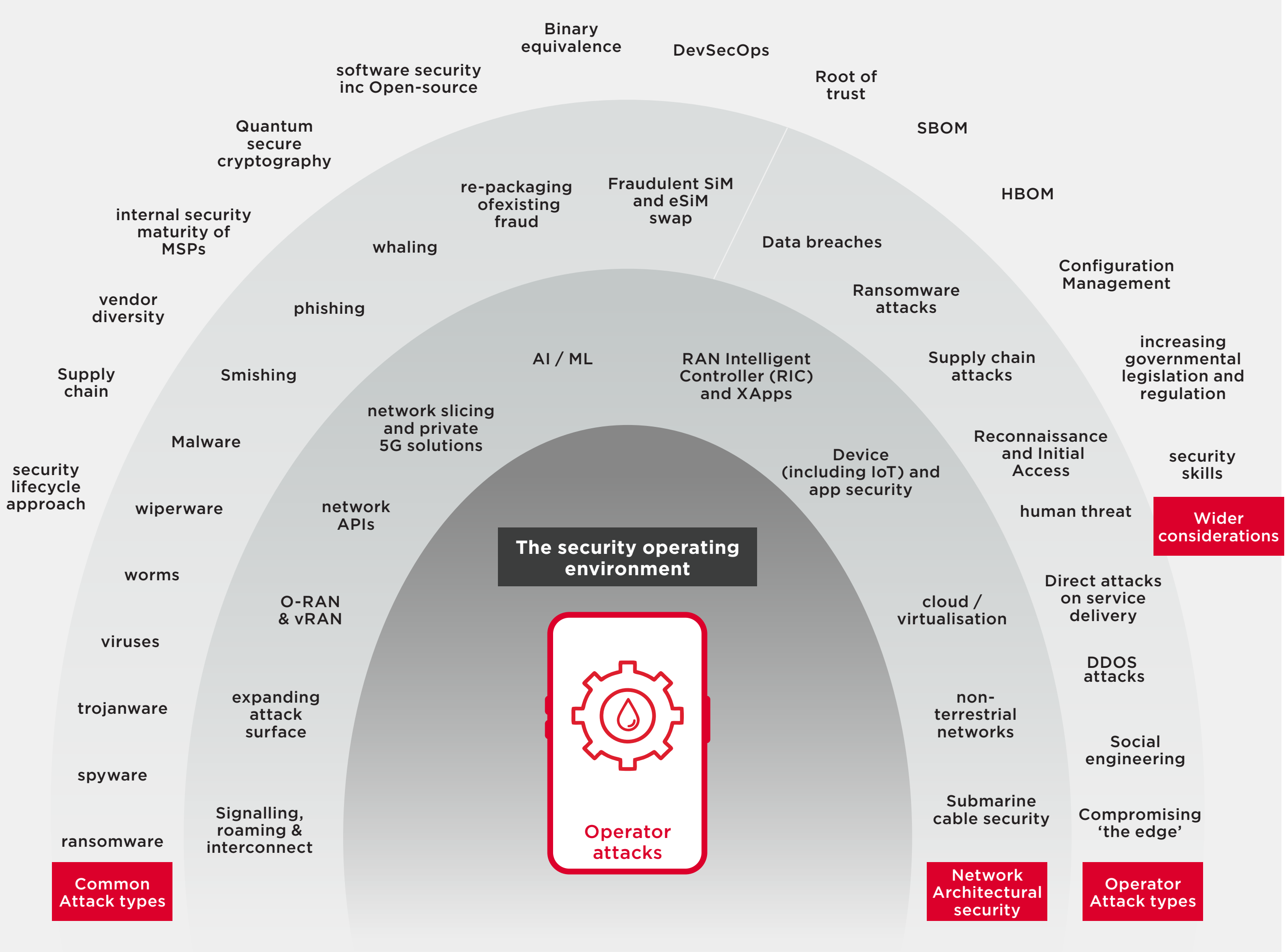
There has been **increasing legislation and regulation** covering supply chains[104] and vendor choice, product security[105], network security[106] and AI[107]. A re-evaluation of current approaches may be required in order to pre-empt future regulatory changes. This can involve proactive engagement with governments on new regulations, vendor selections, outsourcing arrangements, support contacts, future upgrade paths and architectural designs.

[100] Submarine Cable Protection and the Environment (iscpc.org)
[101] https://www.gsma.com/security/wp-content/uploads/2023/06/GSMA-Security-Certification-2023-v1.0.pdf
[102] See https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf
[103] Explored more fully in GSMA | Guidelines for Quantum Risk Management for Telco - Working Groups
[104] E.g. the US Entity Listing, e.g. US restricts trade with 42 Chinese entities over Russia support | Reuters
[105] EU Cyber Resilience Act | Shaping Europe's digital future (europa.eu) & The UK Product Security and Telecommunications Infrastructure (Product Security) regime - GOV.UK (www.gov.uk)
[106] Telecommunications (Security) Act 2021 (legislation.gov.uk)
[107] EU AI Act: first regulation on artificial intelligence | News | European Parliament (europa.eu)

Summary

The wider security operating context described in this section should be allied to the threat topic areas presented earlier in the report. Near-term decisions and investment decisions should be informed both by the current threats and by the emerging wider context. This approach will help ensure investments are efficient and generate longer-term strategic benefits. Strategic security plans should reflect the emerging security operating context described in this section. The breadth of the topics discussed in this report points to a complex operating environment (as illustrated in the diagram below). Partitioning this problem space, understanding likely timescales, working with systems integrators/lead vendors and utilising risk management can help to simplify this complexity.

Figure 5


Binary equivalence
DevSecOps
software security inc Open-source
Root of trust
SBOM
Quantum secure cryptography
HBOM
re-packaging ofexisting fraud
Fraudulent SiM and eSiM swap
internal security maturity of MSPs
whaling
Data breaches
Configuration Management
vendor diversity
phishing
Ransomware attacks
increasing governmental legislation and regulation
Supply chain
Smishing
AI / ML
RAN Intelligent Controller (RIC) and XApps
Supply chain attacks
network slicing and private 5G solutions
Malware
Reconnaissance and Initial Access
security skills
security lifecycle approach
Device (including IoT) and app security
wiperware
network APIs
human threat
Wider considerations
The security operating environment
worms
Direct attacks on service delivery
O-RAN & vRAN
cloud / virtualisation
viruses
DDOS attacks
trojanware
expanding attack surface
non-terrestrial networks
Social engineering
spyware
Operator attacks
Submarine cable security
Signalling, roaming & interconnect
Compromising ‘the edge’
ransomware
Common Attack types
Network Architectural security
Operator Attack types

12.0

Final thoughts

This document provides an overview of the security landscape for the mobile industry in the context of current threats facing MNOs, their customers and the wider ecosystem. This year's report has outlined a range of attacks reported during 2023, highlighting the evolving nature of the attack surface and the threats to which it is exposed.

All the areas highlighted in the GSMA's mobile telecommunications security landscape reports continue to be important. While security defences and controls are improving, a number of factors are driving an increased threat. The net effect is an ongoing requirement to improve network security controls to keep pace with the security challenges: it is time to step up security defences.

Allied to this, the report has also described the emerging security context and explored many of the more forward-looking security topics and consequences. By considering this context, efficient and strategic security investments can be made that complement the shorter-term security necessities.

Over the coming year, the GSMA will continue to support its members on security matters by providing security best practices, services and events that convene the industry.

To get in touch, or to get more closely involved, please email **security@gsma.com**.

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
United Kingdom
Tel: +44 (0)20 7356 0600
Fax: +44 (0)20 7356 0601