GSMA

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.

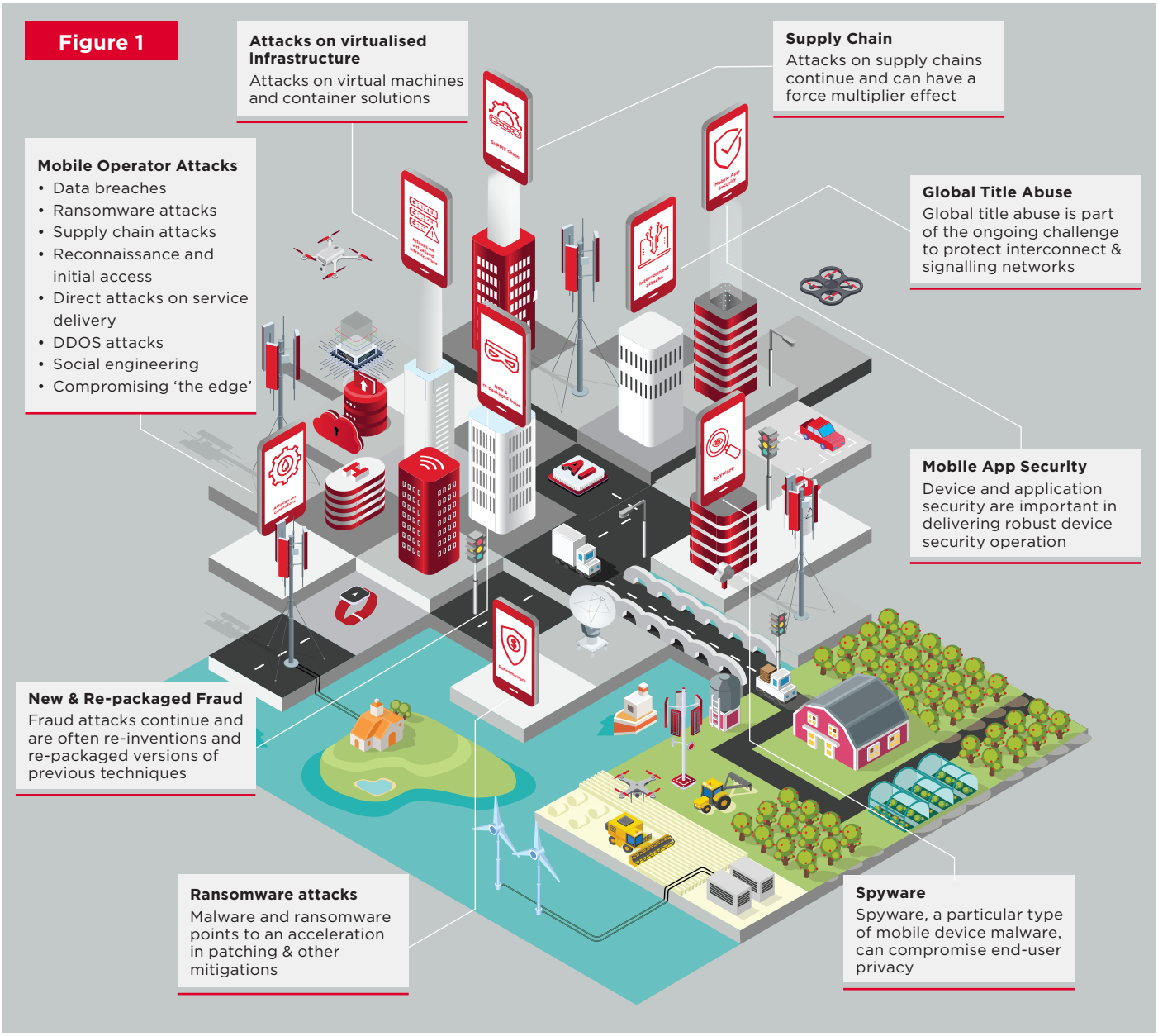
David Rogers MBE - Chair, GSMA Fraud and Security Group & CEO, Copper Horse Ltd

1.0

Key Points

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

Figure 1



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.

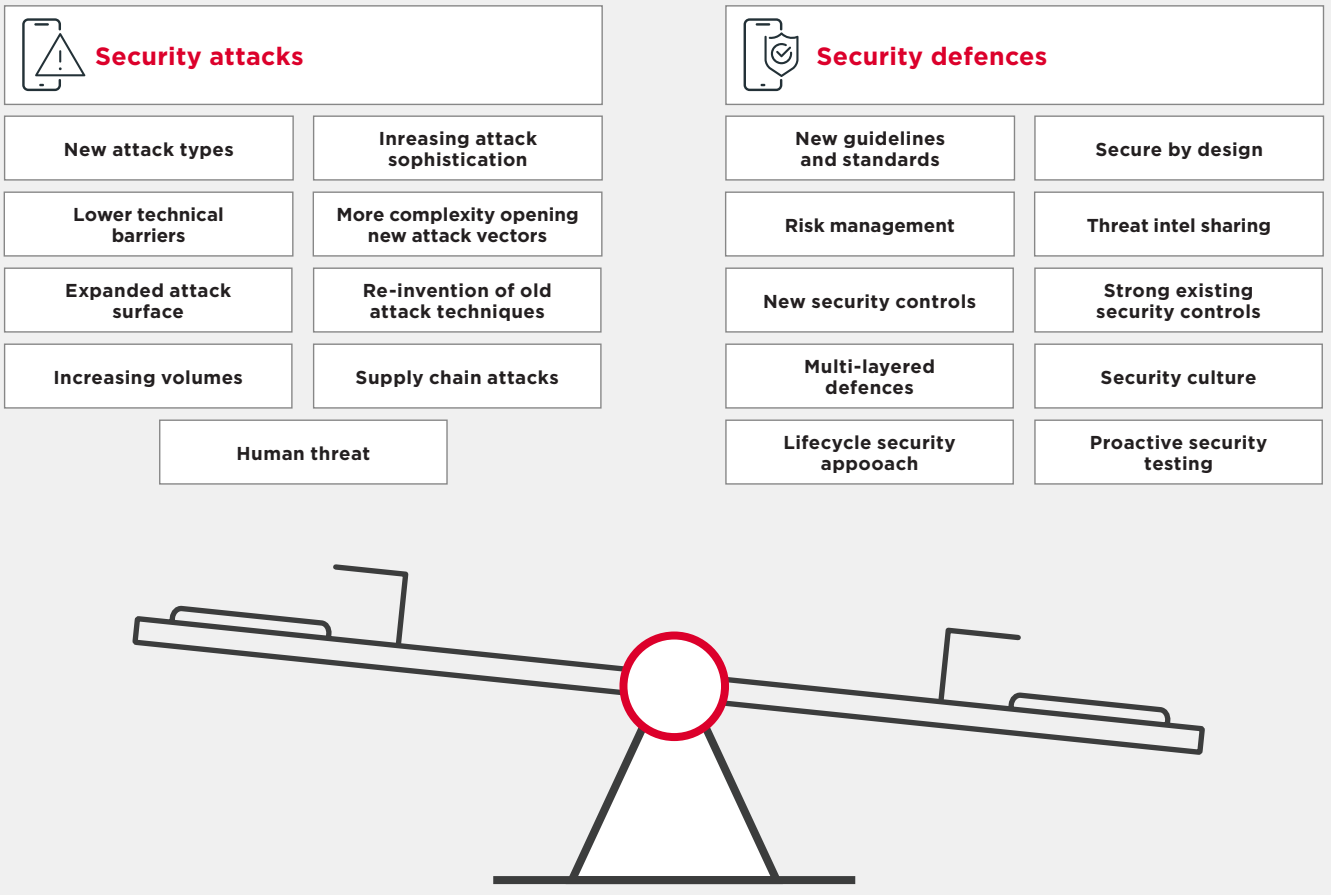
2.0

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.

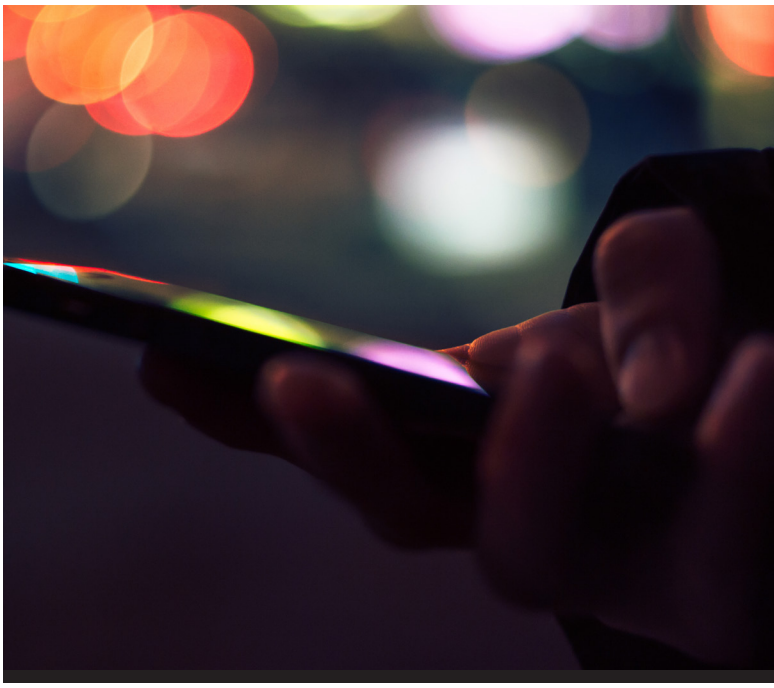
Figure 2



[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