



Mobile Telecommunications Security Threat Landscape

January 2019

Contents

The State of the Mobile Telecommunications Industry	2
Introduction	4
Supply Chain Threats	5
Privacy and Data Protection	7
Signalling Service Threats	9
Cloud Threats	11
The Internet of Things Threats	13
Human Threats	15
Device Threats	17
Looking Forward	19
Conclusion	20

The State of the Mobile Telecommunications Industry

The mobile telecommunications industry is under significant threat.

Today's threats are a realisation of traditional IP based threats within the all-IP 4G network combined with insecure legacy 2/3G generations. Moving into the 5G era the threat landscape will increase due to the new services and technologies being introduced.

Continued underinvestment in appropriate technology, processes, and people has resulted in numerous threats being realised against operators. These threats will only increase as the industry diversifies its services.

With intensified press coverage and increasing legislation representing the new reality, the only mitigation against regulatory or customer based costs will be demonstrable due diligence practices with regard to cyber risk. Therefore the Executive level of an organisation must be properly briefed on the cyber security risk associated with their network. This will allow them to drive specific strategic investment with regard to securing the network.

The GSMA predict that the threat to industry will increase over time.

The following topics impacted the mobile telecommunication industry in 2018. The impact of these threats should be managed effectively through the operator's strategic risk management process. This process should include regular reporting on security controls, which are aligned to strategic goals of the operator. Risks not currently on the strategic risk register should be added and assessed based on the local controls in place. Resulting gaps should drive remedial action.

Figure 1: Main threat impacting mobile telecommunications networks in 2018

Supply Chain

- The threat is the unknown, suppliers manage their own security controls and their risk appetite may not align.
- This should be managed via contractual controls regarding security and governance within the supplier organisation. This should start at the ITT/RFI stage and include in life due diligence checks.

Privacy and Data Protection

- Different jurisdictions call for different controls, failing to understand how this impacts consumer data may result in regulatory fines.
- Operators must map their global data footprint, including data flows, and overlay local controls and regulation. Once this is understood a data framework should be used to effectively protect data.

Signalling

- Aging protocols cannot be easily replaced and therefore compensating controls should be implemented. In tandem strategic planning to move away from legacy technology must be considered.
- Technology must be implemented, at the right locations and supported with the right rules and skillsets to reduce this threat.

Cloud

- Cloud adoption presents risk within supply chain and deployment areas, as the operators outsource service management, but not accountability, to the provider.
- Supply chain controls as well as data protection needs to be considered. As well as this secure deployment and management need to be implemented.

Internet of Things

- This threat is twofold, consumer driven with masses of insecure IoT devices and Enterprise driven where critical services are managed via IoT devices.
- Both must be managed by defining and managing a secure lifecycle for the devices. Consumers must also be educated regarding the threats their IoT devices pose to the ecosystem when insecure.

Human

- Insider threats come from intentional attacks and unintentional mistakes. Both need to be accounted for.
- Employee checks and controls must be put in place to identify malicious insiders. Technology should be used to automate and audit processes and configurations to remove the opportunity for human driven mistakes.

Device

- Vulnerable devices are attached to the network introducing numerous threats to the operators.
- Operators must work with the industry to improve device security, at manufacturing source, to reduce the impact to the network. Consumers must be educated in ways to protect themselves and their devices.

Introduction

The mobile telecommunications industry is facing significant threats, the GSMA aims to balance remediation with prevention

Mobile operators provide the backbone for technologies that the world relies upon. At enterprise level the industry offers a wide array of services, diversifying from traditional connectivity into content and managed services. At the same time 5.1 billion¹ consumers depend on operators to maintain their connectivity; an item considered a basic human right under UN Article 19². At a government level, many operators provide critical national infrastructure. These services are currently provided and managed via four distinct generations of mobile telecommunications technologies. This vast array of technologies results in a mixed threat landscape of traditional IT, radio and mobile network related threats.

With cyberattacks now being considered the third highest global risk, according to the World Economic Forum (WEF)³, the industry must recognise that operators are a major target for attackers. In order to respond to this threat the mobile ecosystem needs to focus its efforts to prevent as well as respond to the increasing threat.

As we move towards the 5G era, of intelligent connectivity, the threat posed by cyberattacks is increasing.

In this report the GSMA review 2018 and highlight the main threats impacting the industry. The purpose of this report is to support our members in understanding and managing the threats faced. Based on this purpose, our focus is providing remedial advice as well as highlighting the threat.

Each section in this report covers a class of threat, however the audience is reminded that threats often intersect to create blended threats⁴; often with increased impact. This highlights the importance of an operator having a holistic view of implemented security controls.

Figure 2: Main threats of 2018



Supply Chain Threats



Privacy and Data Protection



Signalling Service Threats



Cloud Threats



Internet of Things Threats



Human Threats



Device Threats

¹ <https://www.gsmainelligence.com/research/2018/09/global-mobile-trends/694/>

² https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

³ <https://www.weforum.org/reports/the-global-risks-report-2018>

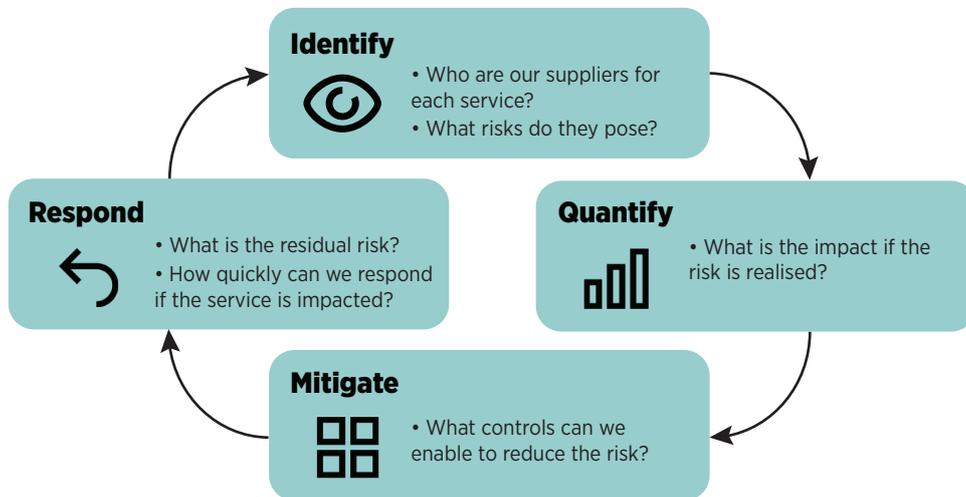
⁴ An example of a blended threat would be where signalling security controls are provided via a vendor managed service, this vendor is part of a supply chain being used to protect a consumer's privacy.

Supply Chain Threats

Knowing who you do business with

Mobile operators rely on numerous external suppliers to deliver infrastructure, products and services. This enables and complements their own. In turn operators' customers, enterprise or consumer, rely on these to manage and enable their lives and businesses. This represents a complex supply chain where downstream links inherit risks and vulnerabilities from suppliers if they are not properly mitigated (see figure 3); making the supply chain increasingly attractive to attackers.

Figure 3: Supply chain risk management



Attackers do not need to compromise their intended target directly but in many cases can achieve their aim by compromising the supply chain where it is least secure. This potential threat highlights the importance of managing the supply chain holistically and driving out or mitigating insecure elements.

2018 has provided several examples of supply chain threats, including tampering with chipsets^{5,6}, vendors releasing devices in an insecure state⁷, and government decisions impacting supply chain resilience⁸. All of which make up an operator's supply chain. This highlights the importance of understanding how products are developed and introduced into the ecosystem as well as managed throughout their lifecycle.

⁵ <https://www.computing.co.uk/ctg/news/3060992/security-researcher-claims-via-c3-x86-cpus-contain-hidden-god-mode>

⁶ <https://www.networkworld.com/article/3262976/security/13-flaws-found-in-amd-processors-amd-given-little-warning.html>

⁷ <https://www.wired.com/story/android-smartphones-vulnerable-out-of-the-box/>

⁸ <https://www.bbc.co.uk/news/technology-43784990>

The software supply chain is in a similar state and arguably more complex. According to the 2018 DevSecOps Community Survey⁹ there was a 55% increase in breaches caused by vulnerable open source software. Many mistake open source for being secure, believing the fallacy that the software has been peer reviewed by the community and is therefore safe to use. Others are not aware which vendors use open source software in their applications. This causes issues with regard to mitigating vulnerabilities as they are disclosed. Any given software 'stack' can contain many sources of components and libraries in differing versions, increasing the need to assess, test, and patch carefully.

Failure to manage the supply chain can result in erosion of brand and trust, regulatory action and major costs to the operator. A recent case caused an operator's availability to be impacted; this was reportedly due to a supplier product¹⁰.

Recommendations

Based on the high impact of this threat the GSMA recommend the following with regard to supply chain security:

- Understand who you do business with, prioritise and risk assess the security requirements for each relationship.
- Map and assess the criticality of any component / service offering within the supply chain and plan and manage in life security (along with reliability etc) accordingly.
- Outline security controls during any Request for Information (RFI) or Invitation to Tender (ITT) processes.
- Actively manage the supply chain security throughout the supplier lifecycle. This may include audits and regular risk assessments.
- Participate in existing industry defined security certification schemes.
- Where independent certification schemes do not exist contractual agreements should be reached; these agreements should include a way of carrying out due diligence checks on the supplier security. In addition, security incident reporting and breach liabilities should be agreed between all parties.
- Vendors and solution providers should model potential threats to assess the incoming software or hardware components before deployment. Partnerships with vendors can allow them the opportunity to improve the service they provide, where desired.

⁹ <https://www.sonatype.com/2018-ssc>

¹⁰ <https://inews.co.uk/news/o2-down-mobile-network-outage-customer-compensation/>

Privacy and Data Protection

Understanding where data resides and flows

Operators must collect, process and store data to operate effectively. This requires the appropriate handling of customer data with required consideration based on the location of the data. Laws that restrict the flow of data reduce the operator's overarching view of their network, which can cause inefficiencies for the network, and increase the opportunity for an attacker to go undetected. A future threat is that, to protect the privacy and security of citizens' data, legislative bodies will develop legislation resulting in data flows being restricted.

In September 2018 the GSMA highlighted that 'striking the right balance in the region's [Asia] data privacy regulations could significantly enhance economic activity and future innovation in 5G, the Internet of Things (IoT) and artificial intelligence (AI)'¹¹. This is because the right privacy regulations could foster consumer trust, while also promoting cross-border data flows. Over and above operational efficiency data flows have a direct impact on GDP¹², according to McKinsey Global Institute data flows represented an estimated \$2.8 trillion in 2014¹³. The GSMA published 6 recommendations for governments regarding data localisation, these are shown in figure 4.

Figure 4: GSMA recommendations for cross border data controls

Recommendation 1:	Recommendation 2:	Recommendation 3:	Recommendation 4:	Recommendation 5:	Recommendation 6:
 Commit to facilitating cross-border data flows and removing unnecessary localisation measures	 Ensure privacy frameworks are fit for a digital age	 Review legacy sector-specific privacy rules	 Encourage regional data privacy initiatives	 Avoid localisation by addressing foreign surveillance concerns pragmatically	 Avoid localisation by addressing law enforcement and national security concerns pragmatically

In 2018 the European Union's (EU) General Data Protection Regulation (GDPR) led the way to regulating data collection, generation, processing and storage. Although the GDPR is making a leading impact, numerous other legislative bodies are reviewing their current or are drafting new legislation to protect consumers privacy.

¹¹ <https://www.gsma.com/newsroom/press-release/gsma-free-flow-of-data-across-borders-essential-for-asias-digital-economies/>

¹² Gross domestic product

¹³ https://www.gsma.com/publicpolicy/wp-content/uploads/2017/10/GSMA-Cross-Border-Data-Flows_4pp_2017_WEB.pdf

Figure 5: GDPR Privacy Controls¹⁴



Failure to consider consumer privacy, regardless of legislative requirements, may result in brand impacting backlash, as seen with the LocationSmart service in the US¹⁵. This highlighted that consumers now expect organisations to protect their personal data and not share it unnecessarily.

In the 5G era big data and operators will be synonymous. The volumes of data created, compiled, stored, and processed to meet business demands will increase. Failure to protect consumer data will result in customer distrust, regulatory issues or legislative fines for the operator. Operators need to build privacy controls into their organisations' processes. Management and meta data will also be produced, consumed and used to facilitate effective operations. This needs adequate protection to stop an attacker using it as reconnaissance material prior to and during , and after their attack.

Recommendations

Based on this global threat, the GSMA recommend the following with regard to data privacy:

- Identify where data is generated, stored, and which jurisdictions it traverses. This map should be assessed against legislative obligations.
- Align to the GSMA's Mobile Privacy Principles¹⁶, reducing the risk of collecting and processing data in an irresponsible way.
- Ensure data frameworks outline the classification of data. The framework should identify who is accountable for protecting each data classification.
- Devise and practice data breach scenarios. This ensures incident management plans are understood by stakeholders impacted by a potential breach. A recent survey by the European Commission outlined this as one of the main issues experienced when enforcing GDPR internally¹⁷.

¹⁴ <https://www.onelogin.com/compliance/gdpr>

¹⁵ https://www.zdnet.com/google-amp/article/us-cell-carriers-selling-access-to-real-time-location-data/?__twitter_impression=true

¹⁶ <https://www.gsma.com/publicpolicy/mobile-privacy-principles>

¹⁷ Multi-stakeholder expert group to support the application of Regulation (EU) 2016/679,

Signalling Service Threats

Aging protocols causing industry wide breaches

Signalling exchange is required to establish/maintain a communication channel or session on mobile telecommunications networks as well as allocate resources and manage networks holistically. 2/3G uses SS7¹⁸ and SIGTRAN¹⁹ and 4G relies on Diameter²⁰; all generations use SIP²¹ and GTP²². Many fundamental services, such as short messaging service (SMS), are managed by these protocols. Many of these protocols are dated and were implemented without an authority model but relied on assumed trust within a closed industry. Couple this insecurity with their essential nature to operate many network functions and any security threats realised against these services will have a high impact.

Researchers and press publications regarding the vulnerabilities in SS7 have been circulating since 2014. In 2017 an incident in Washington DC, close to the White House saw attackers use a fake base station and SS7 access to obtain subscriber information²³. 2018 has seen an increased number of attacks utilising SIP flaws; a specific example was observed where Cisco equipment was used to cause a denial of service (DoS) using malformed SIP traffic^{24,25}. The current media focus is SMS not being a secure means of verification²⁶ for such things as consumer banking.

Successful attacks against the control plane allow an attacker to locate consumers, intercept traffic, and carry out fraud attacks. Predominantly these attacks are targeting consumers and may be considered a breach of privacy under local legislation; increasing the impact and resulting in potential regulatory action and reputational damage.

Appropriate controls to protect against well-known signalling attacks are available from vendors. In addition, research published by ENISA²⁷ in March 2018 reported operators' awareness of the threat and means of protecting their networks. Therefore, the industry must reflect on how effective their internal controls are and understand why the vulnerabilities remain.

ENISA went on to elaborate that there are many difficulties in enabling the controls within an operator's network. Several of these issues are outlined in figure 6. With the complexity of an operator's network and the aging nature of the protocols 'point' fixes are not suitable. A strategic plan of action must be defined to mitigate successful attacks and involve configuration, firewalls and detection / action measures.

QUESTIONS TO PREPARE THE STOCK-TAKING EXERCISE OF JUNE 2019 ON THE APPLICATION OF GDPR

¹⁸ 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.

¹⁹ Signalling Transport (SIGTRAN) is the standard telephony protocol used to transport Signalling System 7 (SS7) signals over the Internet.

²⁰ Diameter protocol is a subscriber authentication, authorisation and accounting protocol created to replace SS7.

²¹ Session Initiation Protocol (SIP) is one of the main request and response application layer signalling protocols in IP Multimedia Subsystem (IMS) and voice over IP (VoIP).

²² GPRS Tunnelling Protocol (GTP) is a group of IP-based communications protocols used to carry general packet radio service (GPRS) mobile telecommunication networks

²³ https://www.theregister.co.uk/2018/06/01/wyden_ss7_stingray_fcc_homeland_security/

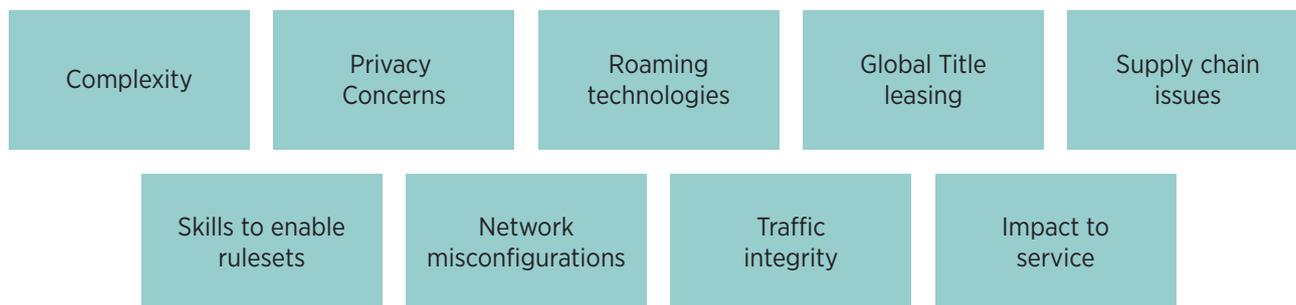
²⁴ <https://www.itpro.co.uk/security/32286/attackers-target-sip-flaws-in-cisco-firewalls-to-overload-devices>

²⁵ https://www.theregister.co.uk/2018/11/02/cisco_sip_warning/

²⁶ <https://www.bankinfosecurity.com/heres-account-authentication-shouldnt-use-sms-a-11708>

²⁷ https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport

Figure 6: Issues cited regarding implementing signalling controls



Although this would appear bleak, slow progress is being made. For example, each year vendors work with mobile operators to highlight insecurities in the Diameter²⁸ and SS7²⁹ networks. This year it has reported that the operators monitored have shown marked improvement in protecting SS7 from successful attacks; compared with 2015 where every network was prone to all types of interconnect threats, a positive trend has emerged in network security over the past two years hence³⁰.

Recommendations

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

- Implement signalling controls outlined in the GSMA Fraud and Security Group³¹ (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.

²⁸ <https://www.ptsecurity.com/ww-en/analytics/diameter-2018/>

²⁹ <https://www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerability-2018-eng.pdf>

³⁰ <https://www.ptsecurity.com/upload/corporate/ww-en/analytics/SS7-Vulnerability-2018-eng.pdf>

³¹ <https://infocentre2.gsma.com/gp/wg/FSG/AFS/Pages/Default.aspx>

Cloud Threats

Scale and flexibility shouldn't undermine security

The network perimeter is disappearing, and cloud computing is now used regularly to support operators' operations either as direct service capability or 'offline' capability – e.g. billing generation. The cloud is where network, storage, compute resources, and applications are managed by an external supplier. Depending on the deployment model this could mean utilising the cloud provider's equipment and, potentially, a service offering. The use of cloud services shows that traditional IT and operator's operations are conjoining and the demarcation is not as clear as it once was.

The loss of direct control of such operations, as they are devolved to the cloud provider, may reduce the operator's level of control over the network performance, optimisation, data and quality of services. Additionally the operator loses the ability to evaluate and mitigate security threats directly, relying solely on contractual or service level agreements with a provider. Therefore cloud services pose a potential combination of threats relating to network availability, supply chain, and privacy.

Such a situation occurred in January 2018 when Meltdown and Spectre³² were disclosed, whereby a weakness in the physical processor design could allow reading of data from one process to another. A successful exploitation of these vulnerabilities on a single server could lead to the compromise of multiple virtual machines running on that server³³ which may be different for customers when using public cloud. Although this caused large scale patching initiatives, in reality the exploit required a high skillset and no known exploit has been detected.

In addition to supply chain and privacy threats the cloud can be misconfigured. Tesla³⁴ was a victim of this where the root cause was that the organisation's Amazon Web Services (AWS) was infected with malware. This attack was successful as AWS had not been deployed securely and as a result the Amazon Simple Storage Service (Amazon S3) was available from the internet.

Although many threats can be realised there appears to be a changing viewpoint on cloud security controls. In 2017 Check Point C-Level Perspective Survey stated that 78% of companies considered IaaS³⁵ and SaaS³⁶ cloud security to be their main concern³⁷. More recently this viewpoint appears to have altered with the Cisco Security Capabilities Benchmark Study 2018³⁸. This outlined that 57% of responders stated they felt cloud offered them better control (see figure 7). This may be

³² <https://meltdownattack.com/>

³³ <https://www.symantec.com/security-center/threat-report>

³⁴ <https://redlock.io/blog/cryptojacking-tesla>

³⁵ Infrastructure as a service (IaaS), is where a cloud provider hosts the infrastructure components traditionally present in an on-premises data centre, including servers, storage and networking hardware, as well as the virtualisation or hypervisor layer.

³⁶ Software as a service, (SaaS) refers to a subscription based model where the software is hosted in the cloud and accessed via the internet for example Office 365

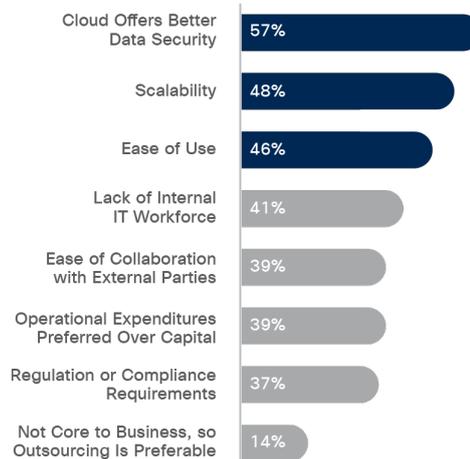
³⁷ <https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf>

³⁸ https://www.cisco.com/c/en_uk/products/security/security-reports.html

due to the differing questionnaire, alternatively the cloud providers may have responded to consumer expectation with regard to security.

Figure 7: iCloud security, Cisco Security Capabilities Benchmark Study 2018³⁹

Fifty-seven percent believe the cloud offers better data security
Source: Cisco 2018 Security Capabilities Benchmark Study



For more info visit: [cisco.com/go/acr2018](https://www.cisco.com/go/acr2018)



Recommendations

Cloud computing is now used as an integral component of operator service delivery. Based on this the GSMA recommend that the threats posed by these outsourced services should be managed via the following controls:

- Understand the supply chain with regard to cloud services and enforce the controls outlined in the Supply Chain Threats section. Specific controls may relate to data storage locations, data management, and destruction and threat detection services.
- Build local policy covering all cloud delivery and deployment models,
- Outline how cloud services can be purchased and what corporate data classification can be shared.
- Confirm cloud suppliers hold appropriate compliance to industry-standard certifications to assure the provider is following industry best-practices and regulations.
- Ensure that you have appropriate skillsets in place to manage cloud deployments.
- Consider the use of private cloud⁴⁰ services.

³⁹ https://www.cisco.com/c/en_uk/products/security/security-reports.html

⁴⁰ A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate.

The Internet of Things Threats

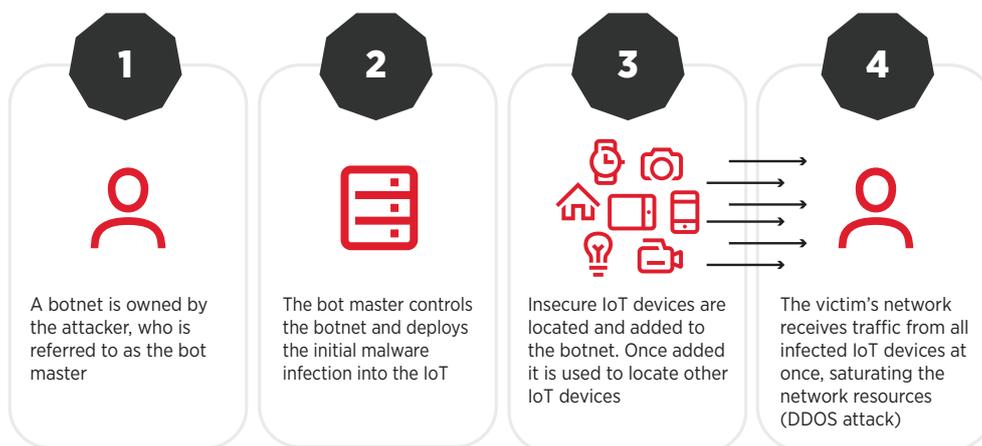
Internet of Things (IoT), insecure by design (or choice?)

The IoT has been embraced by consumer and enterprise. This year industry has been focused on dealing with the security issues generated by this growing industry. The industry has recognised that many of the consumer device manufacturers have no regard for, or competency in, security. They are handing off the responsibility to secure the device to the uneducated consumer whilst offering no security instruction. When these devices are deployed they are also attached to an operator's network and the impact of attacking the network using these devices could potentially hurt the operators. This impact remains regardless of the communication method used by the device.

Most IoT threats come from attackers abusing factory default or poorly configured devices. IoT devices are a desirable target as many of them use commodity components and the volume of devices means many potential victims. An attacker can use the same technique to attack different types of devices regardless of their primary function, leading to a large surface subject to attack with minimal effort on the part of the attacker.

For example, smart home IoT devices use the Message Queuing Telemetry Transport (MQTT) protocol. A recent search on shodan⁴¹ showed 64,567 MQTT servers⁴² that were not securely configured; many of them without passwords. Constrained Application Protocol (CoAP) is reported to be in a similar insecure state⁴³. Consequently, these devices could become part of an IoT botnet⁴⁴.

Figure 8: An IoT botnet



⁴¹ Shodan is a search engine for Internet-connected devices.

⁴² <https://www.shodan.io/search?query=MQTT>

⁴³ <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mqtt-and-coap-security-and-privacy-issues-in-iiot-and-iiot-communication-protocols>

⁴⁴ A network of devices infected with malicious software, controlled as an attacker (botnet master)

Kaspersky reported a growth in IoT botnets in 2018⁴⁵ and revealed the insecure IoT devices that are compromised. In 2016 the Mirai botnet, mother of many modern IoT botnets hijacking over 600,000⁴⁶ devices. The original attack took down OVH hosting and DynDNS services⁴⁷. The majority of these bots are IP cameras and routers, however, Kaspersky's report points out that vulnerability rises in compromised smart TVs.

Industry 4.0, a target for state sponsored actors

Automated manufacturing and integration allows efficiency to be driven through automation and data exchange within manufacturing. Although on a dedicated network, these devices face similar threats to the consumer IoT; however the attacker often has different motivations. The attacker does not want to disrupt the network, they desire persistent access to the network for information disclosure.

The first reported attack against industrial devices was in 2009, when Stuxnet was used to attack Iran's nuclear centrifuges⁴⁸. More recently Nokia has reported on an IoT botnet named VPNFilter, rumoured to have been created by the Russian espionage group Fancy Bear⁴⁹. If correct, a botnet controlled by a state sponsored group would constitute a major threat to national security. Many operators manage various critical national infrastructure (CNI) services, such as water, energy, and emergency etc. Therefore, these CNI IoT devices must be secured, this was referenced by Fortinet's Senior Channel Manager⁵⁰ in a recent interview. He predicted this advanced level of threat will be realised in 2019; the GSMA agree with this prediction.

Recommendations

Based on the combined threats of the IoT, failure to implement security of these devices at their inception, and throughout their life expectancy, will result in successful attacks. These will potentially impact availability of the network or information being disclosed to unauthorised users. Therefore, the GSMA recommends operators:

- Educate consumers regarding IoT security, provide consumers and enterprises with resources and education on securing their smart homes and IoT devices.
- Secure internal IoT devices; the GSMA provide a flexible framework and IoT security Assessment⁵¹.
- Prepare an incident response plan when the network is attacked by a botnet.
- Segment and monitor the network, enable segment blocking in the event of an attack.
- Understand how the physical supply chain transposes to the digital supply chain and confirm you have the right supply chain controls in place.

⁴⁵ <https://ics-cert.kaspersky.com/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/>

⁴⁶ <https://elie.net/blog/security/inside-mirai-the-infamous-iot-botnet-a-retrospective-analysis/>

⁴⁷ <https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html>

⁴⁸ <https://www.bbc.com/timelines/zc6fbk7>

⁴⁹ <https://www.nokia.com/about-us/news/releases/2018/12/04/nokias-threat-intelligence-report-2019>

⁵⁰ <https://www.bangkokpost.com/business/news/1595390/cybersecurity-spending-to-rise>

⁵¹ <https://www.gsma.com/iot/iot-security-assessment/>

Human Threats

Recognising the threat posed by human nature

So far, this report has focused on the technical or regulatory threats that impact operators, however attacks, are often successful due to human nature. Humans make mistakes, these are often leveraged by attackers, providing them with a foothold into the operator's network. Human's also have emotions, and may become disgruntled, leading to a desire to attack the operators.

Internal human threats come in many forms, some malicious, others are not. Figure 9 outlines the 4 main human threats impacting an operator.

Figure 9: Human threats

<p>Social engineering attacks </p>	<p>Misconfiguration </p>	<p>Disregarding processes </p>	<p>Insider threat </p>
<p>Where the attacker manipulates the user into doing something. These are highly successful due to lack of awareness by the user.</p>	<p>Often dubbed the 'fat finger attack' this is where devices are left in an insecure default state or configured insecurely by mistake. This is then leveraged by an attacker.</p>	<p>Processes are often outlined but not followed. Humans will step outside of a process if it does not suit them or they find it laborious.</p>	<p>This is when someone internal intentionally acts in a malicious way. These are difficult to monitor for and insider threats pose a major threat as they have insider knowledge of the way the organisation is managed.</p>

Each of these attacks have been successful in 2018^{52, 53, 54, 55}.

Figure 10: Human threats

<p>Social engineering attacks </p>	<p>Misconfiguration </p>	<p>Disregarding processes </p>	<p>Insider threat </p>
<p>The iPhone launch, in July 2018, was linked with a Fear of Missing Out (FOMO) phishing campaign. FOMO campaigns are successful as they target something coveted within society.</p>	<p>120 million Brazilians were impacted when Apache was misconfigured by Cadastro de Pessoas Físicas resulting in sensitive identity data being disclosed to the internet in July 2018.</p>	<p>In October 2018, an undercover reporter filmed staff at mobile operators' stores in the UK failing to follow the correct process prior to performing SIM card swap requests.</p>	<p>Tesla acknowledged that they had located an insider exporting intellectual property in October 2018.</p>

⁵² <https://www.itpro.co.uk/security/22631/iphone-6-launch-emails-disguising-phishing-scams>

⁵³ <https://www.infosecurity-magazine.com/news/apache-misconfig-leaks-data-120/>

⁵⁴ <https://www.bbc.co.uk/news/business-46047714>

⁵⁵ <https://www.electronicdesign.com/automotive/hiding-plain-sight-dangers-insider-threats>

When an operator employs or contracts an internal resource they have more prescript control over their actions. Contractual based controls with defined repercussions are a way to enforce security within an organisation. However, these must be supplemented with controls to identify breaches. This control begins with an organisation's culture with regard to security; internal teams need to feel comfortable reporting security concerns. Other controls include:

- Policy driven controls, such as pre-employment checks, attempt to reduce the potential threats before they enter the organisation.
- Education for employees regarding phishing and other threats that may target them.
- Technology controls, including data leakage prevention (DLP), to reduce the risk of sensitive information leaving the network
- Auditing controls to highlight when processes are not being followed.
- Auditing configurations to locate misconfigurations prior to them being leveraged by an attacker.
- Monitoring controls specifically targeting insider threat type behaviour, for example unusual file access and use of dormant user accounts.
- Reporting controls where all internal entities know where to report suspicious situations.
- Process reviews should be conducted with the objective of automating as much of the process as possible. This reduces the potential for misconfiguration and makes the process less laborious for the employee; meaning they are less likely to step outside of it.

Recommendations

GSMA recognises that consumers are humans and manage their own security. However, as it has been identified in the IoT threats, their behaviour has an impact on the operator's network. This has also been seen when consumers are duped by scams on the internet and blame their provider as the source of the issues. This threat will remain until consumers understand how their behaviour impacts the wider ecosystem. In response to consumer based human threats the GSMA recommend that operators develop their consumer's security maturity by taking practical steps; specifically:

- Educate consumers regarding fraud and scams such as phishing, malware, the importance of patching, and password management. Use current communication channels to socialise the education.
- Build an incentive scheme for being a secure consumer; for example data allowances or vouchers if they act in a secure way.
- Deliver products to customers in a secure state by default.

Device Threats

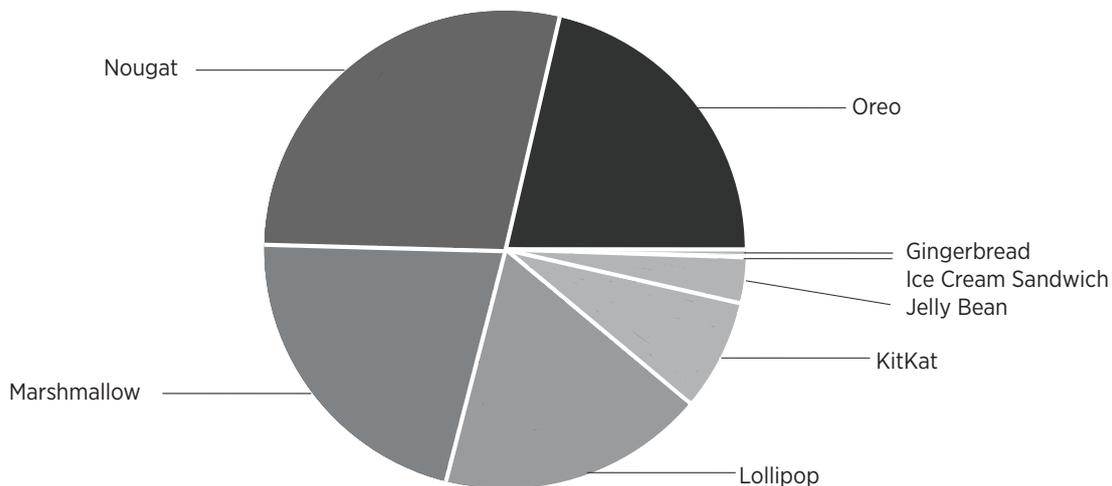
Human threats collide with insecure devices

Not all consumers understand the threats their devices introduce to the ecosystem. However, suppliers of the device, software (app) developers and over the top service (OTT) providers introduce and increase the threat to the device and therefore device owner to manage. Due to the long term nature of the consumer relationship many operators inherit and manage many of the device threats. This threat was recently recognised in the threat landscape report for the UAE region where devices were listed as the fourth highest risk⁵⁶.

In April 2018 hacktivist group WikiLeaks released Vault 7. This collection of hacking tools, purported to be from the Central Intelligence Agency (CIA) in the US, 'contained dozens of zero-day weaponized exploits [sic] thought to be targeted against a wide range of US and European company products, including Apple's iPhone, Google's Android, Samsung TVs and Microsoft Windows'⁵⁷. Once released these were available to attackers to use against devices.

Assisting the hacking tool is the software supply chain of the device. Android's development site indicates device owners are not receiving operating system updates in a timely manner, these updates are often security related. In October 2018, figure 11 reveals less than ¼ of Android devices were on the most up to date operating system. Clearly, those outdated operating system devices are in a vulnerable state. Software updates for applications may be as poorly maintained.

Figure 11: Android operating system, October 2018⁵⁸



⁵⁶ <https://www.darkmatter.ae/media/1676/darkmatter-cyber-security-report-november-2018.pdf>

⁵⁷ <https://www.checkpoint.com/downloads/product-related/report/2018-security-report.pdf>

⁵⁸ Data collected during a 7-day period ending on October 26, 2018. Any versions with less than 0.1% distribution are not shown <https://developer.android.com/about/dashboards/>

Android holds a 70% market share⁵⁹ and is installed on numerous handsets manufactured globally. Nokia reports that Android devices were responsible for '47.15% of the observed malware infections in 2018' and is the 'most commonly targeted' operating system⁶⁰.

This threat is being compounded by the hand-off mentality with consumers where older vulnerable devices will remain active in the ecosystem with their 2nd, 3rd or 4th owner⁶¹.

Recommendations

With smartphone adoption rates due to reach 77% saturation globally by 2025⁶² operators must find ways to work within the ecosystem to improve device security. The GSMA recommends that operators:

- Participate in industry initiatives that enable handset manufacturers to converse with operators with the aim of improving device security. The GSMA manages a Device Security Group (DSG), this group work to improve the security of mobile devices.
- Participate in threat intelligence partnerships with other operators, sharing suspect device information within the industry. The GSMA Telecommunication Information Sharing and Analysis Centre (T-ISAC)⁶³ is available to support this activity.
- Confirm that consumer terms and conditions allow the operators to block a device if it poses a threat to the network.
- Educate consumers on the importance of applying updates to their devices and recommending that they only visit reputable app stores, such as Google Play and Apple's App Store. Both these app stores attempt to identify and remove malicious applications from their library.
- Develop a reporting mechanism for researchers and consumers to contact the operators with issues.

Security researchers are advised to participate in responsible disclosure via one of the industry's Coordinated Vulnerability Disclosure (CVD) programmes. The GSMA manage a programme such as this for industry wide vulnerabilities⁶⁴. Google manages the Android Security Awards⁶⁵ scheme which receives vulnerabilities relating to the Android operating system.

⁵⁹ <https://www.netmarketshare.com/operating-system-market-share>

⁶⁰ <https://www.nokia.com/about-us/news/releases/2018/12/04/nokias-threat-intelligence-report-2019-warns-on-the-fast-growing-and-evolving-threat-of-malicious-software-targeting-internet-of-things-iot-devices/>

⁶¹ <https://www.gsmaintelligence.com/research/?file=061ad2d2417d6ed1ab002da0dbc9ce22&download>

⁶² <https://www.gsma.com/mobileeconomy/wp-content/uploads/2018/02/The-Mobile-Economy-Global-2018.pdf>

⁶³ <https://www.gsma.com/aboutus/t-isac>

⁶⁴ <https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/gsma-coordinated-vulnerability-disclosure-programme>

⁶⁵ <https://www.google.co.uk/about/appsecurity/android-rewards/>

Looking Forward

Predicted threats of 2019 and beyond

AI used against the industry

Operator's use AI technologies to enhance their services. Cloud providers are starting to deliver AI as a service, providing this technology to all consumers. Compromising an operator provides value to the attacker and AI usage would be seen as a way of increasing their success rate. Therefore the GSMA expect to see this happening in the near future.

IoT attacks on the rise

As previously discussed the rate at which the IoT is developing is exponential. The GSMA predict an increase in:

- IoT botnet based DDoS attacks, this is supported by the prediction that machine to machine (M2M) communications over cellular networks is due to grow by 10% between 2010 and 2020⁶⁶.
- Targeted state sponsored attacks on IoT devices managing CNI services. Industry 4.0 is enabling IoT devices on networks supporting CNI, consequently there is likely to be interest in compromising these networks to gain intelligence about foreign services. With cyberwarfare being more widely used we predict that this will increase over the coming years.

Uneducated overreliance on cloud

With cloud becoming synonymous with operators there is the potential threat that an incident impacting a cloud provider may have implications impacted many operators who

use the same provider. Managing suppliers and understanding the provider's resilience to attack will be the only way to limit the impact of these predicted incidents.

5G threats

5G standards outline standardised security architecture that offers controls far surpassing those of previous generations. However, we face the threat of repeating mistakes of the past. The use of Diameter in 4G resulted in numerous vulnerabilities being introduced to the operator's networks. With the intention to use IP based protocols in 5G we face the threat of choosing an insecure signalling service protocol.

The GSMA predict that the additional complexity 5G will add to the network will increase alarm fatigue⁶⁷ within security operations teams; leading to attackers going unnoticed for longer periods of time.

Quantum and the Public Key Infrastructure (PKI)

Looking further ahead the GSMA predict that quantum computing will be a destabiliser for the industry. This is due to the fact that a quantum powered computer will allow the PKI to be broken. The PKI underpins a vast amount of security within the mobile telecommunications industry; therefore the impact of this prediction is vast. Quantum safe cryptography must be implemented in order to mitigate this threat.

⁶⁶ GSMA Intelligence, global growth of cellular M2M

⁶⁷ Alarm fatigue is sensory overload when security personnel are exposed to an excessive number of security tooling alarms, this results in alarms being ignored or missed.

Conclusion

The threat landscape is varied and complex, the industry must take a strategic view to protect itself

Based on the increase in threats being realised it is unlikely that the WEF will remove cyberattacks as a global risk for several years to come. Whilst the mobile telecommunications industry provides such fundamental services the GSMA predict operators will remain targets for cyberattacks.

Alongside the increased threat is increased attention from legislators, press agencies and consumers. This results in increased public scrutiny of the industry's response to the threat. Based on the increased attention the mobile ecosystem must focus its efforts to prevent as well as respond to the increasing threat. This is why the GSMA advise that all operators implement a strategic response to security.

The GSMA recommend that operators implement the controls outlined above; with a holistic view on technology, process, and people. These internal controls, coupled with consumer education and industry engagement should result in protected services for enterprise and consumer alike.

Our intention is to update this brief on an annual basis. In-depth studies of specific topics may be published as supplemental reports, these will depend on the industry's needs as the security threat dynamics change.

The GSMA welcomes feedback and suggestions to improve its approach to address industry wide security issues. To start a dialogue, please contact the GSMA Fraud and Security Team on security@gsma.com.

About GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 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 represent the mobile telecommunications industry with regard to Fraud and Security. 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: <https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group>



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

