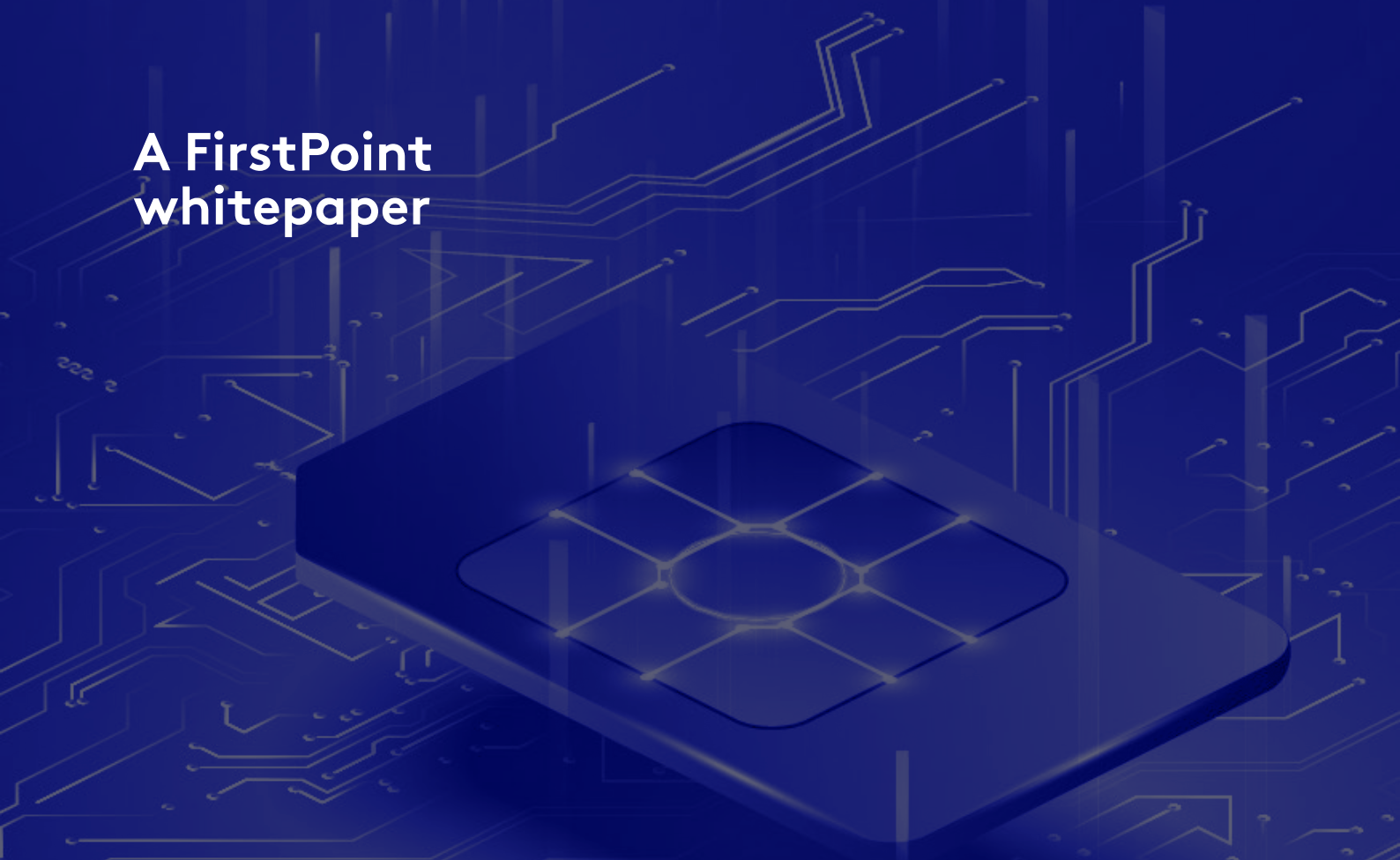
FirstPoint

Cellular IoT security
A 360° overview

A FirstPoint whitepaper



August 2020

Contents

Introduction

Internet of Things (IoT) solutions have the potential to revolutionize whole industries. From enabling smart cities and connected supply chains, to powering Industry 4.0 and Agritech innovation. Today, it all depends greatly on cellular connectivity and 5G adoption, and results in the introduction of new and unprotected endpoints into cellular networks.

It is easy to dismiss cyber vulnerabilities for cellular IoT devices as being the same risks already being addressed when protecting smartphones. Another flawed assumption is that cellular IoT devices are only vulnerable to the same attacks on IoT devices using LAN or WLAN connections. In reality, it is the combination of cellular connectivity and IoT-specific vulnerabilities that make for a highly dynamic threat landscape that can jeopardize mobile network operators, enterprises, government agencies, and, of course, the cellular subscribers themselves.

If you were to drop a cellular IoT expert from 2019 in 2020 they would be amazed to observe the evolution of cellular IoT in a single year. New use cases are being introduced with more industries adopting the technology, and new devices being developed to serve the needs of enterprises and end-users alike. As a result, there is an upward trend in the number of connected devices and a growing need for infrastructure to support it.

You may think that the COVID-19 crisis slowed down the adoption and deployment of IoT devices and networks in enterprises. This is only partially true. In reality, the rate of cellular IoT deployment was impacted only in the short term, mostly due to the effects of the crisis on supply chains and manpower operations[1]. The true effect of the COVID-19 crisis on the IoT market is that of a catalyst[2]. Connected medical IoT devices and the urgent need for a digital transformation of supply chains through IoT are just two of the drivers for the upcoming exponential growth in demand for cellular IoT in 2021.

Adam Weinberg

CTO and Co-founder, FirstPoint Mobile Guard

[1] "GSMA MIT Enterprise Forum Cambridge 5G IoT Covid 19" - GSMA, Published June 2020

[2] "Covid-19 is a catalyst speeding up the IoT adoption trend" - SiliconRepublic, Published 22 May 2020

Connecting the Internet of Things

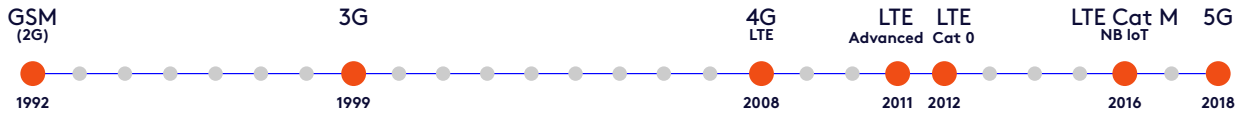
> To enable and support the massive growth of IoT and connected devices, cellular network infrastructure technology has evolved and adapted to various use cases as they appeared.

Cellular IoT is not a new concept. In fact, there are still cellular IoT deployments in rural and remote areas[3] making use of almost 30-year-old **2G** networks that have been decommissioned[4] in many countries in the world.

As cellular connectivity technologies evolved, features and capabilities to support IoT applications were added. The needs and demands of cellular IoT deployments and devices were first addressed in the **LTE Cat.0**[5] standard that appeared in 3GPP release 12 in 2012. It introduced a power saving mode that allowed for longer battery life on battery-dependent devices.

Though **LTE Cat M**[6] and **Narrowband IoT (NB-IoT)**[7] further improved battery life, increased range and added in-vehicle handover[8], it wasn't until 5G was introduced that cellular IoT was finally given the connectivity necessary for mass adoption.

In addition to significantly increased speed and greater coverage, **5G** introduced network slicing and various methods to secure the network and the devices on it.



3GPP standards initial "release" per network.

One thing that is common to all types of networks and all types of connected devices is the risk they face from external threats. Threats that become a valid concern the instant any device is connected to any network.

[3] "Germany's rural 4G users still spend one-fourth of their time on 3G and 2G networks" - OpenSignal, Published 30 June 2019
[4] "Legacy mobile network rationalisation" - GSMA, Published May 2020
[5] "Release 12" - 3GPP, Published March 2015
[6,7] "Release 13" - 3GPP, Published 2015
[8] "IOT Vehicle Telematics is The only Option" - Altair, Published 27 March 2018

The state of cellular IoT device cyber threats

Any time you connect a device to the internet, regardless of the type of connection you employ to do so, you put it at risk. These devices can be used by attackers to gain access to confidential business data, impact business services or even public infrastructure.

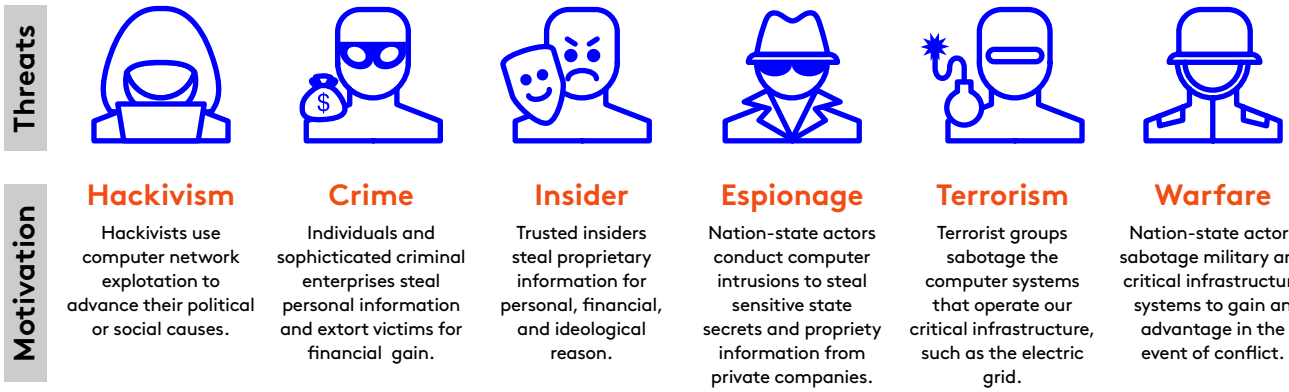
Because IoT is a relatively new and versatile domain, some challenges need to be addressed. Among them is the dual challenge of understanding the possible attack vectors for every specific device, and deciding what security measures are needed to mitigate them. Cyber risks are a major topic to address.

The main culprits in attacks on cellular IoT devices are your classic cybercriminals: hackers, national hacker groups, terrorists, criminals, and script kiddies. Each group has their motivation. Hackers are usually driven by a mix of fun and money, although sometimes their only motivation is simply the challenge of it. Criminals can have a mix of reasons, usually focused around money.

Terrorists and government-sanctioned cybercriminals are looking to disrupt businesses or governments and gather intelligence. The recent cyberattacks on the water supply systems in Israel[9] are a real-world example that highlights just how much can be at risk without the proper levels of security in place.

And, of course, there are always the "script kiddies" who are just out to cause trouble and have fun while honing their skills.

The FBI Cyber Division defines 6 main threat actors[9A].



[9] "Cyber Attack Targets Israel's Water Supply – Analysis and Mitigation Recommendations" - Radiflow, Published April 2020
Source: Figure 1: The Cyber Threat Spectru

[9A] "Your Data At Risk: FBI Cyber Division Shares Top Emerging Cyber Threats To Your Enterprise" - Digital Shadows, Published September 2019

General attacks landscape

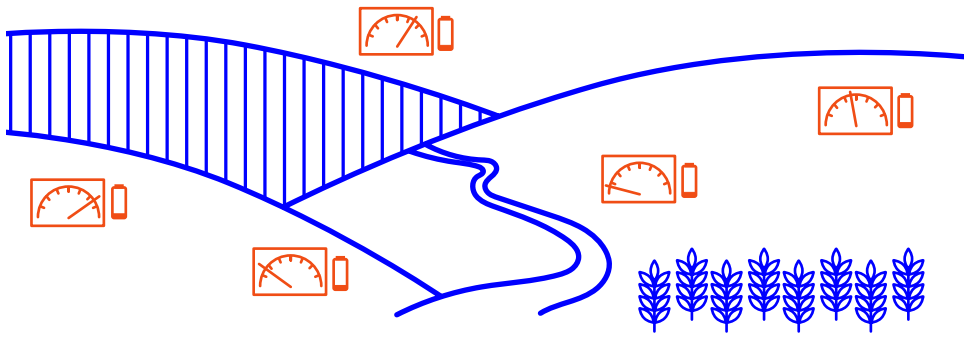
As mentioned previously, one of the greatest challenges with cellular IoT devices is that they are vulnerable on multiple fronts.

The following is by no means a complete list of attacks as new ones are discovered in the wild almost every day. It does, however, provide a thorough overview of some of the biggest and most common threats to cellular IoT devices.

Device manipulation

- **Battery drain attacks**[10] - Because IoT devices rely on battery power to function, these attacks can end up being pretty costly. This is especially true when, as a result, company employees are forced to go out and replace batteries in potentially remote or dangerous locations.

  One method involves "waking up" a component within the system far more frequently than is necessary, which drains the battery of the device. Attackers can execute this attack by gaining access to the network gateway upon which the device resides.



- **Attacking functionality**[11] - These attacks exploit loopholes in the device or network systems to gain access to control functions. Those can be unintentional but can also be inserted deliberately by saboteurs during the manufacturing process.

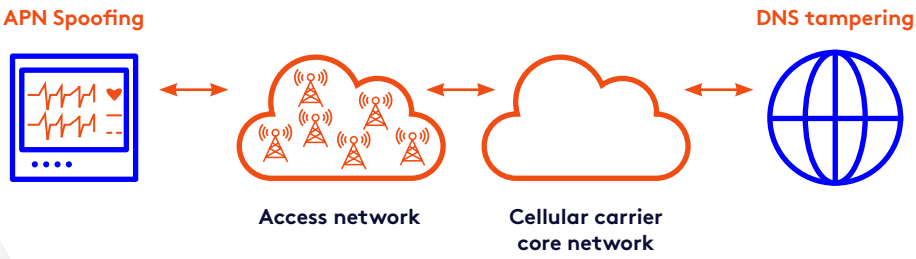
  Such exploits can be used to impact service operation, spread botnets, or implement denial-of-service attacks, which overwhelm an IoT device and network.

[10] "Battery draining attacks against edge computing nodes in IoT networks" - Cornell University, Published 4 Febuary 2020
[11] "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights" - IEEE.org, Published 12 May 2016

Data channel rerouting attacks

To capture sensitive information and tamper with commands sent to IoT devices and services on the network, attackers can modify the path of data to and from the attacked device in the cellular network. Once in control of this path, attackers can use it to sniff data and tamper with data sent to and from the device.

There are a variety of attack schemes used to accomplish this. In most cases, it involves maliciously altering the APN (Access Point Name) registered on the device[12] (which defines the gateway from the cellular network to the open Internet) or the intervention in DNS (Domain Name Server) resolution to control what IP address is resolved for the APN. Another example is the aLTEr attack. Utilizing a Man-in-the-Middle fake cell tower, the attacker can change the IP address of the requested DNS server[13].

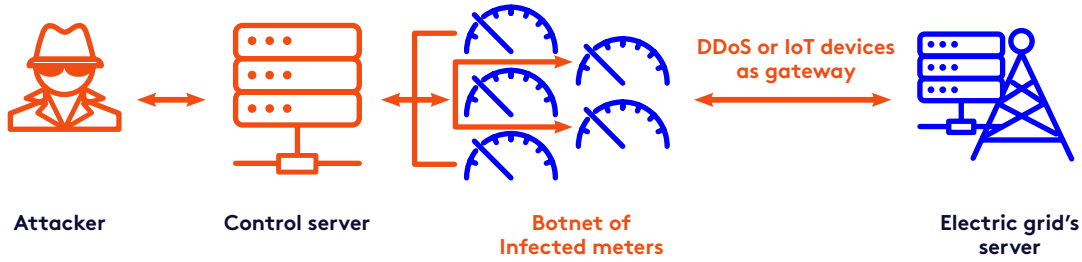


Eavesdropping attacks enabled by data channel rerouting can put at risk sensitive business data. Data tampering can have even more significant repercussions, leading to massive disruptions in supply chains or even risk lives.

Using IoT devices as tools in an attack

- **IoT devices as a gateway**[14] - IoT devices themselves can be used as a way to gain access to the internal systems of a company. Hackers exploit vulnerabilities within the device and use that device to get into the other zones in the networks of the company. This lets attackers effectively steal data, trade secrets, and other critical information.

- **DDoS attacks**[15] - In addition to using IoT devices to gain access to data, attackers can employ them to launch Distributed Denial of Service attacks. These can shut down some or all aspects of operations. These attacks are an increasing problem for IoT devices, as attackers typically exploit devices that are poorly protected due to leaving security "holes" in the perimeter, such as factory default passwords.



[12] "Advanced SMS Phishing Attacks Against Modern Android-based Smartphones" - CheckPoint, Published 4 September 2019
[13] "LTE and 5G Integrity attacks – An in-depth briefing" - FirstPoint, Published 13 April 2020
[14] "The Hunt for IoT: The Opportunity and Impact of Hacked IoT" - F5, Published 15 July 2019
[15] "Routers Exploited to Attack Gaming Servers" - Palo Alto Networks, Published 31 October 2019

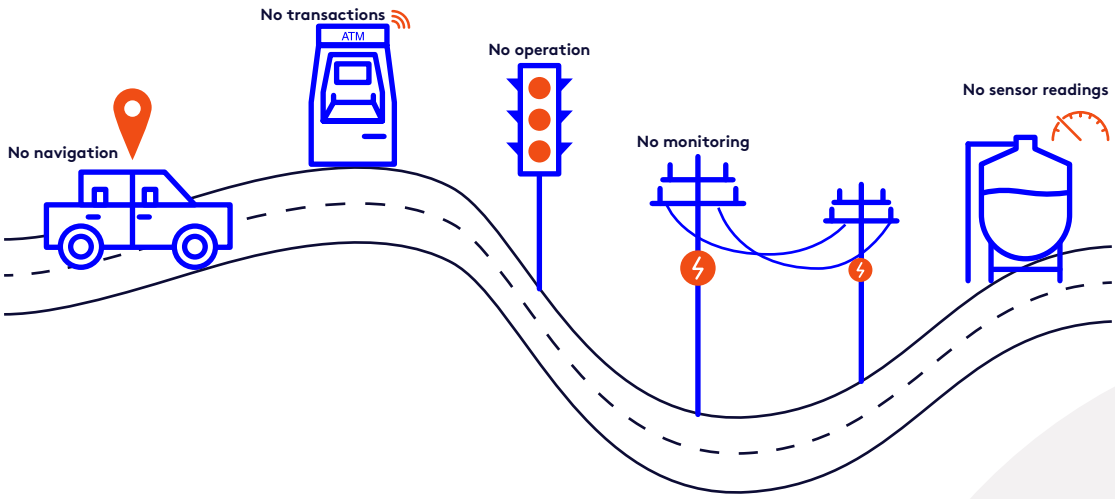
Denial of service (DoS)

- **Targeted DoS attacks** - These attacks are designed to single out a specific connected device or a group of such devices and take it offline. This can be done by flooding the device with information that triggers a crash[16]. Alternatively, fake cell towers and exploitation of SS7 network vulnerabilities can deny the device connectivity to the mobile network at the attacker's will. These attacks can disconnect manufacturing and monitoring systems, halt the production of electricity, all while preventing administrators from accessing their systems.

- **Non-targeted DoS attacks** - Non-targeted DoS attacks aim to knock down everything on a network rather than disrupt the service of a specific device. While the attack method can be very similar to that of a targeted DoS attack, non-targeted DoS attacks are often executed by attackers aiming to disrupt an organization (or even a whole nation) impacting devices and services indiscriminately.

  In cellular networks, such attacks are often launched by exploiting flaws in the cellular network's connectivity protocols. These flaws enable attackers to impersonate the identity of another (legitimate) device connected to the service (using the above mentioned IMP4GT attacks, for example). Which in turn lets them flood the network to deny service to other endpoints.

- **Service DoS attacks** - Similar to other DoS attacks, but with the intent of disabling business or national services and not specific devices. For example, such an attack can disable the logging service of an IoT device while leaving functionality intact to be used in the next stage of a multi-layered attack.

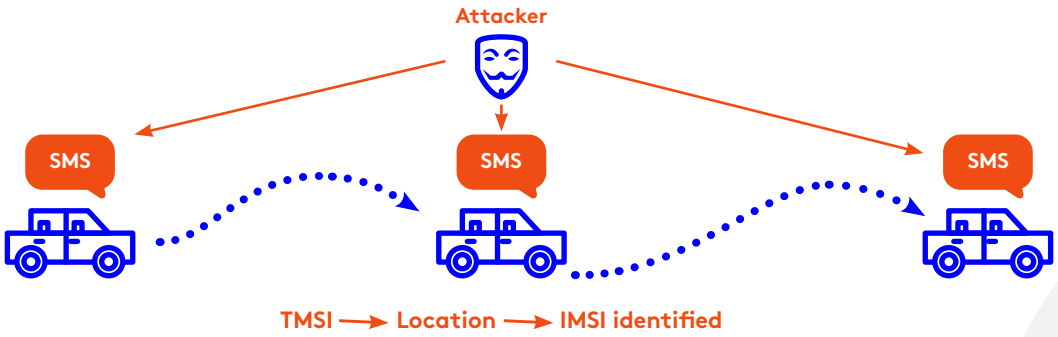


[16] "User-targeted Denial-of-Service Attacks in LTE Mobile Networks" - ResearchGate, Published October 2018

Identity compromise

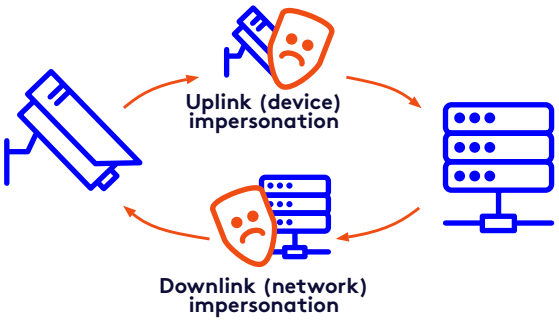
ToRPEDO attacks[17] - ToRPEDO (TRacking via Paging mEssage DistributiOn) attacks, allow hackers to determine the identity of the device, where it is located within a geographical region, and can even be used to identify the device owner.

Hackers make repeated attempts to, send multiple SMS messages or service requests to a device in a short period of time. They then sniff the paging message to determine the Temporary Mobile Subscriber Identity (TMSI) of a device and subsequently learn its location and even its International Mobile Subscriber Identity (IMSI). This, in turn, can reveal the device owner's identity.



- **IMP4GT attacks**[18] - IMP4GT attacks allow cybercriminals to impersonate devices or users by exploiting integrity protection flaws in the cellular connectivity protocol[13]. The attack can be used for uplink and downlink impersonation according to the attacker's objectives and opportunities enabled by flawed security policies on the network.

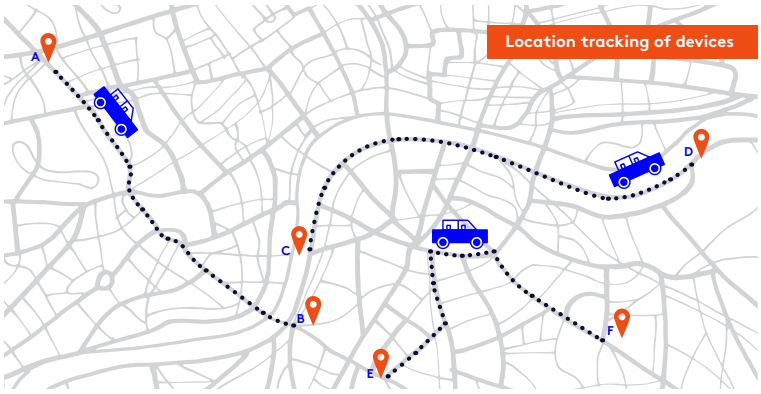
  Though somewhat complex to deploy and implement, this type of attack can modify the IP identities of each of the parties: the target device (uplink impersonation) or the network server identity (downlink impersonation). As a result, the attacker can then access any service on the network while assuming the victim's identity. Alternatively, they may mimic the communications with the service of a legitimate service provider the target device may connect to.



[17] "Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information" - NDSS Symposium May 2019
[18] "IMP4GT: IMPersonation Attacks in 4G NeTworks" - IMP4GT, Published February 2020

Location data exposure

- **Location tracking** - All cellular devices communicate with the network they are connected to. Among the data they transmit and is necessary for uninterrupted service is the physical location of a device. By exploiting existing flaws in communication protocols like SS7 and Diameter[19], attackers can gain access to the location of a device. While not very significant in static cellular IoT deployment scenarios, such attacks can put at risk valuable assets transported in connected vehicles.



- **Location checking**[20] - Unlike location tracking which follows a device around, location checking lets attackers know when a specific device enters a certain geographic location. This can be, for example, a trigger as part of a wider attack to harm devices or business operations in a specific area.

With the sheer variety of possible attacks out there that threaten cellular IoT devices, organizations need to take a proactive approach to security. Data isn't the only thing at risk. Billion-dollar systems and national infrastructure can be taken down by nefarious rivals or someone who's just out to prove their hacking skills.

Fortunately, it's possible to be proactive around cellular IoT security. Let's take a closer look at how you can protect IoT devices from cyber threats today.

[19] "A Step by Step Guide to SS7 Attacks" - FirstPoint, Published 26 January 2020
[20] "On Location Privacy in LTE Networks" - IEEE.org, Published 20 January 2017

Tackling IoT device cybersecurity

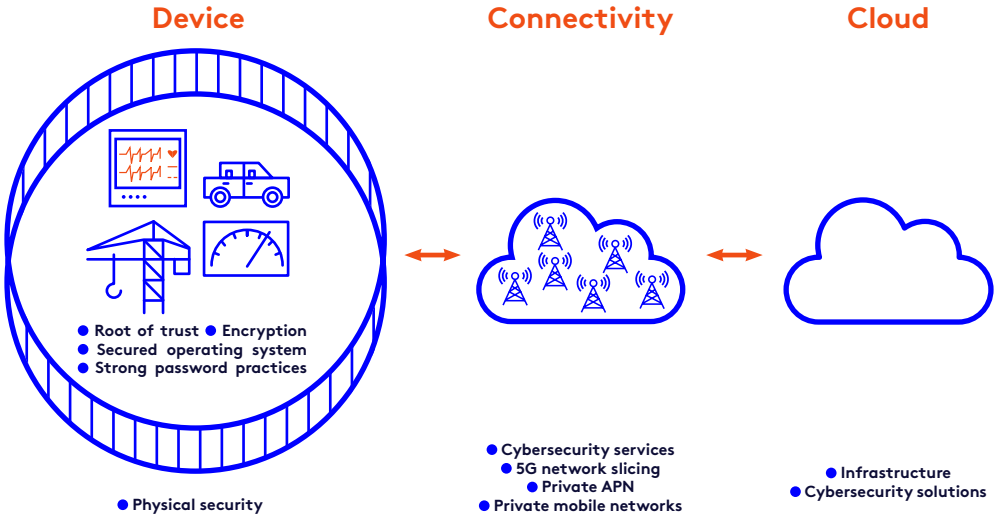
How organizations protect cellular IoT devices depends heavily on the use case. Different use cases open devices up to different kinds of attacks that must be mitigated through a layered approach.

Cellular IoT devices are uniquely different from other types of endpoint devices. Unlike mobile phones or laptops, IoT devices' operating systems, communication protocols and applications are versatile. For example, securing power-meters and water-meters is very different from protecting a connected insulin pump, though both are technically cellular IoT devices.

This presents a challenge for service providers and organizations that need to secure both client deployments or services and their own infrastructure from potential intrusions and disruptions.

The strategy to secure cellular IoT devices is addressing issues from the core of the device outward. The base is hardware security as well as perimeter protection. With those protections in place, the IoT device can then come online, which leads to the need for a layer of protection between the device, the cellular network, and other devices on the network. The last layer, that's aimed at securing the data transmitted and protecting cloud-connected IoT devices is especially critical with devices that are highly dependent on cloud services to function properly.

The connectivity of cellular IoT devices is both their strength and their weakness. The services and applications enabled by cellular IoT connectivity are, at the end of the day, what makes the impact on the bottom line of a business. At the same time, it is that same connectivity that puts the devices, the networks upon which they operate and the businesses at risk.



What this means for both businesses and service providers is that **by securing the connectivity layer they can scalably mitigate threats to all devices, regardless of hardware, software or usage changes.**

Is there a single solution to deal with these Vulnerabilities ?

FirstPoint - all-in-one Mobile Network-based cybersecurity

Reading about these cybersecurity threats to cellular devices provides food for thought. Nearly all solutions out there may solve some of these attacks, or partially solve some, but cannot solve all of them.

At FirstPoint, we believe that the mobile network, not only encompasses risks, but is also a core component in mitigation of cyber attacks. By understanding the complexities and limitations of mobile networks, we've been able to build a solution, based on the network that tackles the entire cyber threat landscape.

To mitigate attacks threatening cellular devices, **there is only one solution – identifying and protecting cellular communication at the first point of entry, before it reaches the device, with a network based solution.** FirstPoint, the cyber security-as-a-service that identifies, monitors and protects from network-based threats, innovatively provides just this.

Why FirstPoint cybersecurity-as-a-service?

FirstPoint delivers continuous, updated protection in one cybersecurity platform. **This network-level solution bypasses any cellular vulnerability, keeping device identifies private and safe from all cyber-attack methods.** As a service, we continuously monitor new and evolving threats and update the system accordingly. As a network-based solution, updates of the system are immediately applied to all network traffic thus protecting all devices (of any make or model, new or old, with or without an operating system, SIM or eSIM based) without user-activated updating.

360 cellular security
Fake cell towers,
SMS, signaling
& data plane

Ready for growth
Simple deployment
Infinite scaleup
Always up to date

Closes mobile network gaps
Overcome vulnerabilities
in 2G, 3G, 4G, 5G

Device-agnostic
For any SIM/eSIM-based device
With/without operating system
"One-stop-shop" management

Ease of use
Hassel-free
Zero-impact on users
Boosts adoption

Tackling all cellular threat vectors, for any device

Detect, alert, protect, manage, deceive

Fake cell towers
Mobile identity compromise
Denial-of-Service
Man-in-the-Middle
Impersonation
Malware delivery

Malicious SMS
Malicious origin
Malware delivery
SMishing
Malicious content

Data-channel attacks
DNS manipulation
Data traffic redirection
Malicious URLs
Malware connectivity

Signaling loopholes (SS7/Diameter)
Location tracking
Man-in-the-Middle
Denial of Service

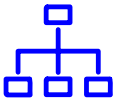
Boosting the cellular advantage

By adhering to a mobile network-based approach, FirstPoint upholds the same advantages that drive users and organizations to choose cellular connectivity for their IoT deployments in the first place.

Scalable
as easy as scaling connectivity, and even easier

Centralized
easy to update and roll out changes

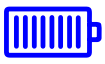
Widespread
as far as the network can reach



Managed
in one central platform for all connected device

Agnostic
for any device with mobile connectivity

Critical
dealing with the most sensitive use cases



Hassle-free
no impact on operations or battery, invisible

Evolving
designed for 2G-5G and ready for the future

Feel free to contact our team to discover more:

FirstPoint

secure@firstpoint-mg.com

Follow us!

About FirstPoint

FirstPoint is a mobile security platform that protects any cellular or connected device against hidden vulnerabilities in the network. Our agentless, cellular network-based approach to cyber security identifies know and unknown attacks 24/7, instantly activating protective measures.

Our solutions are completely transparent to the user/device, with no device installations, updates or slowdowns, protecting any device; e.g., M2M, security-sensitive IoT devices, connected systems and mobile phones.