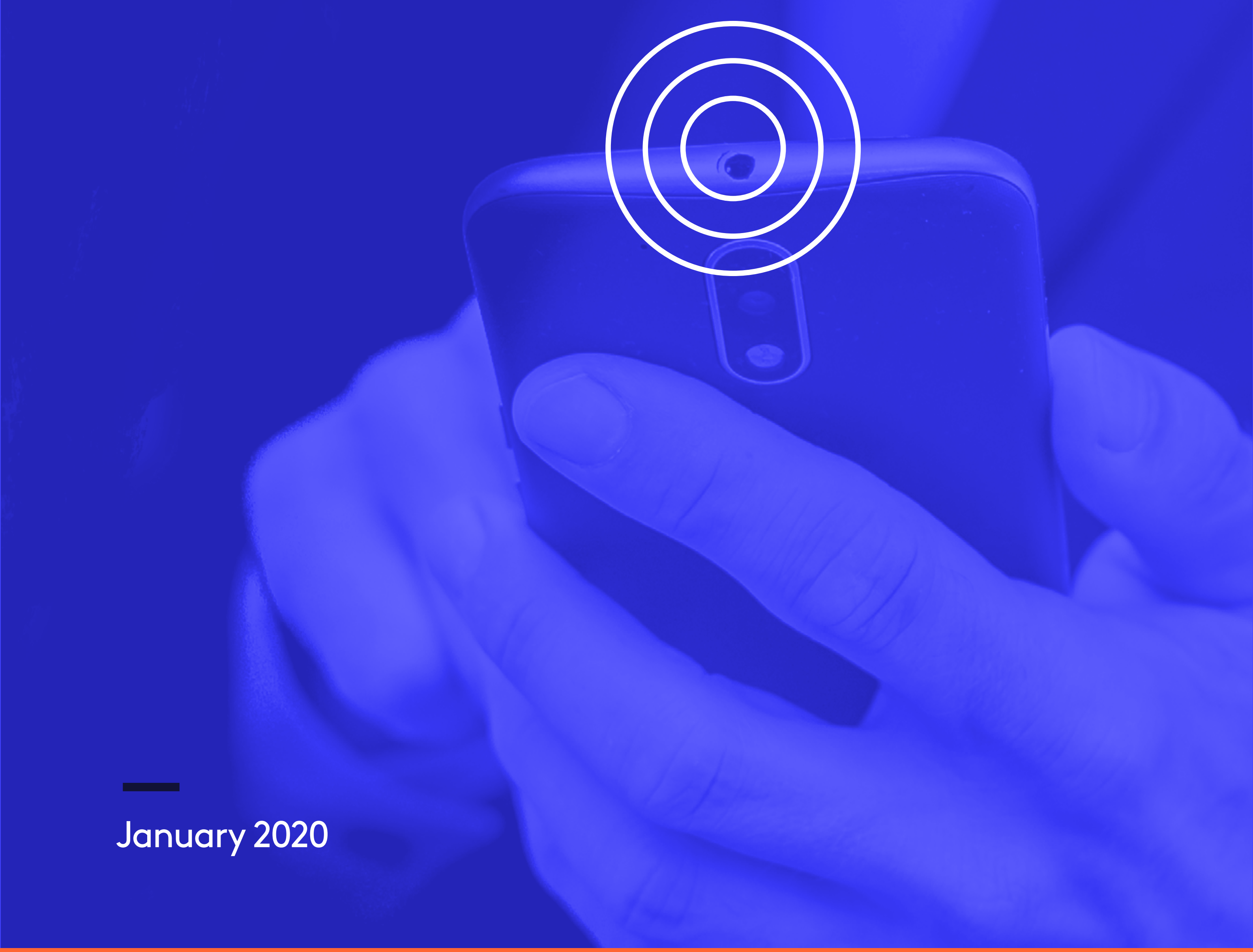
FirstPoint

Mitigating cellular cyber risks on connected devices

A FirstPoint Mobile Guard white paper



January 2020

Contents

Introduction

Cellular devices now outnumber the world population by about 19%.
The overwhelming popularity of cellular devices demonstrates that cellular devices are probably the most important cog in the digital transformation machine taking over the world.

However, even though cellular devices deliver technology to even the most remote corner of the world, they also introduce new cyber security risks and vulnerabilities. In fact, the speed of mobile connectivity growth **and adoption of cellular connectivity for crucial communication** has been nearly matched by the speed of new mobile cyber security vulnerabilities.

Mobile network operators (MNOs), as well as enterprises concerned with data safety, are discovering that they must hurry to catch up with the pace of technology and the cyber attacks that follow. We can expect to see a direct correlation between the growing popularity and increased reliance on connected devices, and an increase in the number and quality of mobile cyber attacks.
To stay ahead of present and future attacks, there is a growing need for a solution that continuously protects against network-based cyber attacks on the almost infinite number of cellular devices. I expect to see network based cyber security solutions, like FirstPoint, adopted by every MNO and cellular IoT network in the coming years.

Adam Weinberg
CTO and Co-founder, FirstPoint Mobile Guard

The state of mobile cyber attacks and 5G

> “Cybercriminals are now taking a mobile-first approach to hacking the enterprise”

Reports the *ThreatPost*, an IT and business security news site. However, one does not need to read news reports to realize that attackers continue to come up with new ways to penetrate cellular devices. In fact, one of the most anticipated mobile technologies in recent years has been 5G, designed with cyber security in mind. The 5G AKA (authentication and key agreement) rollout was supposed to provide new and innovative defenses from mobile cyber attacks.

In fact, there has never been a network overhaul like 5G. What has always been done in hardware will now be accomplished in software, a faster, more efficient alternative. Thanks to IP (internet protocol), 5G (software) can run multiple application layers simultaneously, unlike legacy networks (hardware), which could only perform sequentially. This allows 5G additional cloud computing capabilities and opens up a whole new field, ripe for innovation.

Nevertheless, being software rather than hardware-based does not mean the network is not vulnerable to old, as well as new, cyber attacks. Since earlier generations relied on hardware functionality, they could count on the network’s centralized nature to enhance their security. The 5G distributed, software-based system is more vulnerable.

Despite the definitions and standardization efforts toward privacy protection, research reports have shown that several possible attacks are still possible, even with and because of 5G's location and identity protection features. The most prevalent are location tracking, identity hijacking, content re-routing and 2FA hijacking.

Naturally, MNOs and enterprises are going to great lengths, and making sincere efforts, to thwart cyber attacks. According to an Allied Market Research report, investment in mobile cyber security is growing 41% year-over-year and is expected to reach $35 billion by 2020. On the other hand, cyber attackers are becoming increasingly sophisticated and finding new, elaborate and robust methods of beating current mobile cyber security defenses, especially with new and sophisticated cellular surveillance tools.

Types of Cellular Cyber Attacks

The cyber security industry is renowned for being a tremendously innovative industry, no doubt due to its “cat-and-mouse”- like nature. As the communication industry and cyber security companies develop new defensive solutions, attackers - often cybercriminals or state-sponsored organizations - find inventive attack vectors. They exploit new vulnerabilities or find new ways to attack older defenses.

Therefore, a core focus of cyber security should be to always stay relevant and up-to-date on the latest cyber attack vectors. When it comes to mobile cyber security, the issue is compound, because of the incredible innovative leaps in recent mobile technology. The bottom line is that technological innovation also comes with a side effect of increased vulnerability to cyber attacks.

Let’s look at some of the most common cellular Cyber Attacks, which take advantage of security vulnerabilities in 3G, 4G, and even 5G networks.

MiTM Attacks

MiTM (Man-in-The-Middle) attacks are Cyber Attacks where, as the name implies, the attacker places itself between the attacked mobile and the true network. MiTM attackers "eavesdrop” on cellular communications and can modify communications.

There are generally two types of MiTM attacks:

1. Close-proximity MiTM Attacks

Usually based on an attacker using fake cell-tower equipment (see more below) to create an attack physically nearby the victim.

2. Network Based MiTM attacks

The attacker impersonates a legitimate core network equipment to launch the MiTM attack.

On some occasions, the orchestration of MiTM attacks includes utilizing global signaling connectivity (SS7 based) loopholes between mobile operators. These loopholes are accessed to acquire credentials or otherwise manipulate the target communication. Attackers using this method will then hijack a victim’s network traffic, where they are able to inflict continuous damage.

Fake Cell Tower Attacks

Fake cell tower attacks are launched by hackers operating equipment that pretends to be a legitimate cellular base station.

The rogue base station attracts target cellular devices to connect to it. It does this by transmitting the proper radio frequency (RF) signals, and tricking the target devices into accepting the (fake) base station as the preferred choice.

Once the target cellular device is connected to this fake base station, the attacker can launch various attacks such as:

- DoS Attacks - A Denial-of-Service attack denies access to the network for calls, data, or text messaging
- Device Impersonation
- False Messages
- Malware Delivery

As previously mentioned, hackers can leverage fake cell towers to launch a "Man-in-The-Middle" (MiTM) attack, providing network connectivity to the attacked device while monitoring all the traffic.

DDoS

A **Distributed Denial-of-Service Attack (DDoS)** is a type of cyber attack where multiple computers or devices, usually infected with malware, act as a network of bots and attack a server - rendering it unusable.

In general, mobile apps are a threat to come under DDoS attacks. In fact, mobile apps have been used to control mobile devices, which are then used to perform a DDoS attack. One of the reasons why these apps are susceptible to DDoS attacks is because it is easy for an attacker to profile the user itself, and that tremendously increases the probability of successfully performing DDoS attacks on mobile apps.

DDoS hackers will set up a security loophole and use it to launch an attack. Once launched, the attacker has complete control over the cellular device. Then they can use it, in conjunction with other devices, to create a botnet and shut down the entire network - creating a massive denial-of-service attack.

SMS-based Attacks

SMS-based attacks are launched when attackers recognize specific functionalities and flaws in the SMS delivery process to launch dedicated attacks.

One such attack is through malicious use of the mobile operator to deliver specific SMS's with binary content (Binary SMS). These SMS messages are typically used legitimately by mobile operators to activate or modify various services.

Attackers can inject binary content into the device's memory by leveraging specific loopholes in the information flow process of the SMS content to applications on the device.

The Simjacker attack, recently made public, is a similar attack of this type, in which the attackers target the SIM card processor. The attack is accomplished by sending a specifically crafted message to the device aimed at the S@T browser, which controls the SIM card's stored commands. The attackers use the S@T library to launch such actions as requesting a device's IMEI number and location.

Another type of SMS-based attack is called the Type Zero SMS message. As part of a location tracking (see below) attack, the type zero SMS, not apparent on the device, generates RF device activity. This causes the location of the device to be registered on the network. The attacker is then able to harvest this data in an additional phase.

SMS Hijacking

SMS hijacking attacks take advantage of several attack methods to maliciously intervene in the flow of SMS messages. Messages aimed for specific users are eventually "hijacked" and reach the attacker instead.

This type of attack is especially dangerous when the SMS message carries sensitive information. An example of this might be a one-time password utilized as a 2FA (two-factor authentication) enhanced security process, used for accessing sensitive resources (such as a bank account or personal email account).

Attackers are using several schemes for implementing SMS hijacking attacks. Recent SMS hijacking attacks take advantage of vulnerabilities launch attacks such as:

1. Maliciously convincing the target user to use a fake website.
2. "Tricking" the network operator to issue a replacement SIM with the identity of the target user.
3. Manipulating network signaling messages, forcing the network to route messages to devices controlled by the operator.
4. Leveraging a fake cell tower (MiTM) attack.

SS7 and Diameter Signaling-based Attacks

Signaling-based attacks occur when attackers have gained access to the cellular networks' internal links, or to links interconnecting mobile operators. The attackers then manipulate some signaling messages flows, enabling an eventual attack.

Such attacks are implemented in 2G/3G networks, manipulating MAP/SS7 messages; and in 4G networks, manipulating Diameter protocol messages. Recent reports also indicate the vulnerability of 5G networks to such attacks.

Among the numerous signaling-based attacks are DoS, location tracking, supporting other type of attacks (like fake cell towers), SMS hijacking, and eavesdropping.

Location Tracking Attacks

A very fundamental feature of cellular communication is the ability to receive communication services regardless of geographical location. This capability is maintained when the user is within the coverage of their home mobile operator, and also when the user is roaming globally. This is how MNOs can route calls and messages anywhere in the world.

However, to perform this function, the mobile operator collects and maintains user location information from other network elements, and globally from other mobile operators. User location information is exchanged over signaling links, using SS7 and Diameter protocols. These protocols have limited authentication and authorization, opening them up to abuse.

Attackers take advantage of the relative openness of these protocols to implement **location tracking** attacks. These attacks are specifically capable of remotely locating and tracking the position of any mobile subscriber in real-time, simply by knowing the phone number; while the victim is never made aware of such queries

Mobile Phishing Attacks

Mobile phishing attacks are a simple but effective attack vector. The attack is launched by delivering specific messages (usually SMS or another messaging service like WhatsApp) to target devices.

Commonly, the content is "clickbait" with messaging designed to solicit an action. For example, the user may be requested to click a URL link in the message.

Attackers apply various human engineering tactics to get users to click through, such as sending warning messages that claim users' accounts have been hacked and they need to reset their passwords.
More elaborate attack schemes include messages capable of impersonating messages sent from contacts of the target user, increasing their credibility. Once the link is clicked, the attack carried out.
Typical phishing attack scenarios may include:

- **Downloading an infected application.**
- **Connecting to an infected site** (launching a "drive-by" attack that attacks the device's browser application)
- **Connecting to a site that impersonates a trusted site** (Most recently, when over 100 government websites were "spoofed").

Malicious Attacks Threaten the Most Advanced Networks

3G technology opened faster internet and data downloads for mobile users. But hackers easily slipped through the cracks, due to SS7 signaling protocol vulnerabilities. The protocol, designed to set up and route calls, had hardly any authentication or authorization because it was considered closed and trusted.

This faith was misplaced, as hackers take advantage of the loose security to track device locations for espionage or other activities; and for DoS and other attacks.
The newer Diameter signaling protocol for 4G networks was meant to correct this inadequacy, including encryption and authentication.

Yet similar cyber security issues plague this protocol, too. The lack of end-to-end security allows hackers to break-in and launch attacks like those plaguing 3G networks. They also intercept conversations and text messages - which could easily contain sensitive subscriber information. Additionally, hackers could downgrade a user's device to 3G or even to 2G in some cases, circumventing the Diameter protocol's somewhat better security safeguards.

5G Vulnerabilities

Threats are also forecast for the vastly faster 5G network.

In fact, a recent vulnerability was discovered by SINTEF Digital Norway, ETH Zurich, and the Technical University in Berlin. This new vulnerability impacts the authentication and key agreement (AKA) protocol, which negotiates and establishes keys to encrypt communications between a device and the cellular network.

Apparently, IMSI catchers can exploit AKA vulnerabilities to downgrade AKA to a weaker state, allowing location tracking and metadata mobile phone traffic interception.

Even though a new, stronger authentication negotiation system was created for 5G called 5G-AKA, researchers found a new vulnerability that reveals a user's mobile activity, such as the number of sent and received texts and calls. This lets IMSI-catcher operators create profiles for each cellphone holder.

Hackers can also monitor users' whereabouts, even when they move away from the IMSI catcher (fake cell tower); and can continue to monitor them remotely for a long time. This capability exposes devices to surveillance threats and to ad targeting.

Network-Based Cellular Protection

With 3G, 4G and 5G networks still vulnerable to such damaging attacks as fake cell towers (IMSI catchers), MiTM and location tracking, organizations are challenged to protect their cellular networks. Other solutions mainly provide protection against data leakage and do not have any visibility into cellular attack vectors.

The most effective way to protect cellular network and data leakage protection is a full, proven, network-based solution that is agnostic to the device type, future generation technologies and hacker tactics.

	IMSI catchers	Network loopholes	Malicious SMS	Malware	Device types
FirstPoint	✓	✓	✓	✓	ALL
Secured hardware on device	✗	✗	✗	✓	Limited
Cloud-based solutions	✗	✗	✗	✓	ALL
Security SW on-device	✗	✗	✗	✓	Limited
SS7/SMS firewalls	✗	✓	✓	✗	ALL
Network-based data protection	✗	✗	✗	✓	ALL

FirstPoint offers a seamless platform that covers all cellular device threats on any SIM/eSIM-based device. This mobile network solution identifies, alerts and protects against any hidden cellular network risks to connected devices; e.g., IMSI catcher detectors, network loopholes, malicious SMS, malware, SMS hijacking and location tracking. The platform delivers continuous, updated, network-based security anywhere, on any device – even when users roam.

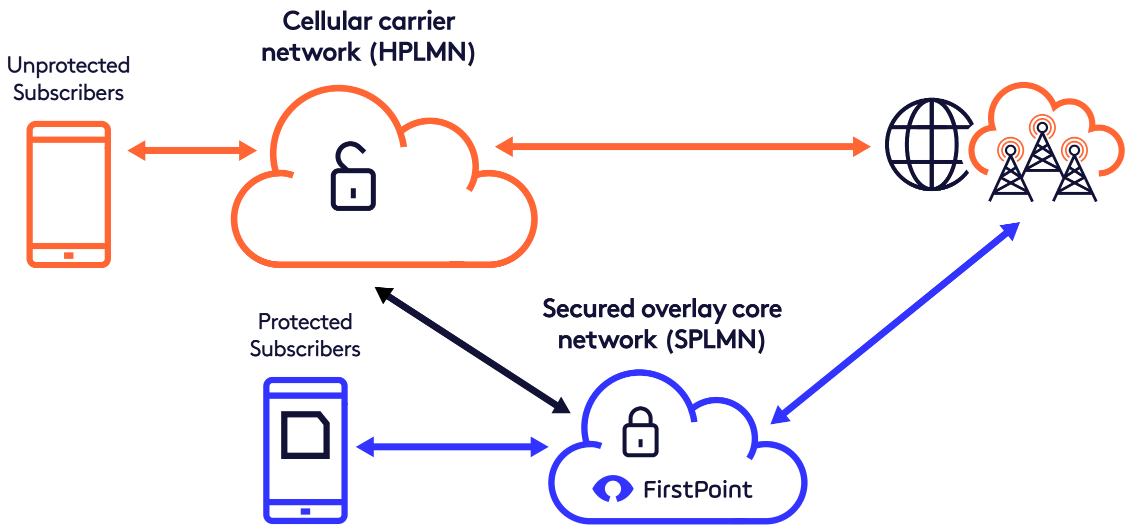
Management can specify security by policy, scenario, location or custom grouping and can monitor all devices from one dashboard.

Users enjoy a consistent, secure experience: no hardware, software or updates to install, no slowdowns and no battery/performance impact.

How does it work?

The platform comprises:

- A secured overlay core network, which is operated side-by-side with the MNO's original core network
- A dedicated applet, installed on the protected device's SIM
- Communication routing through the secure environment
- Novel security measures



Cellular carrier network (HPLMN)
Unprotected Subscribers
Protected Subscribers
Secured overlay core network (SPLMN)
FirstPoint

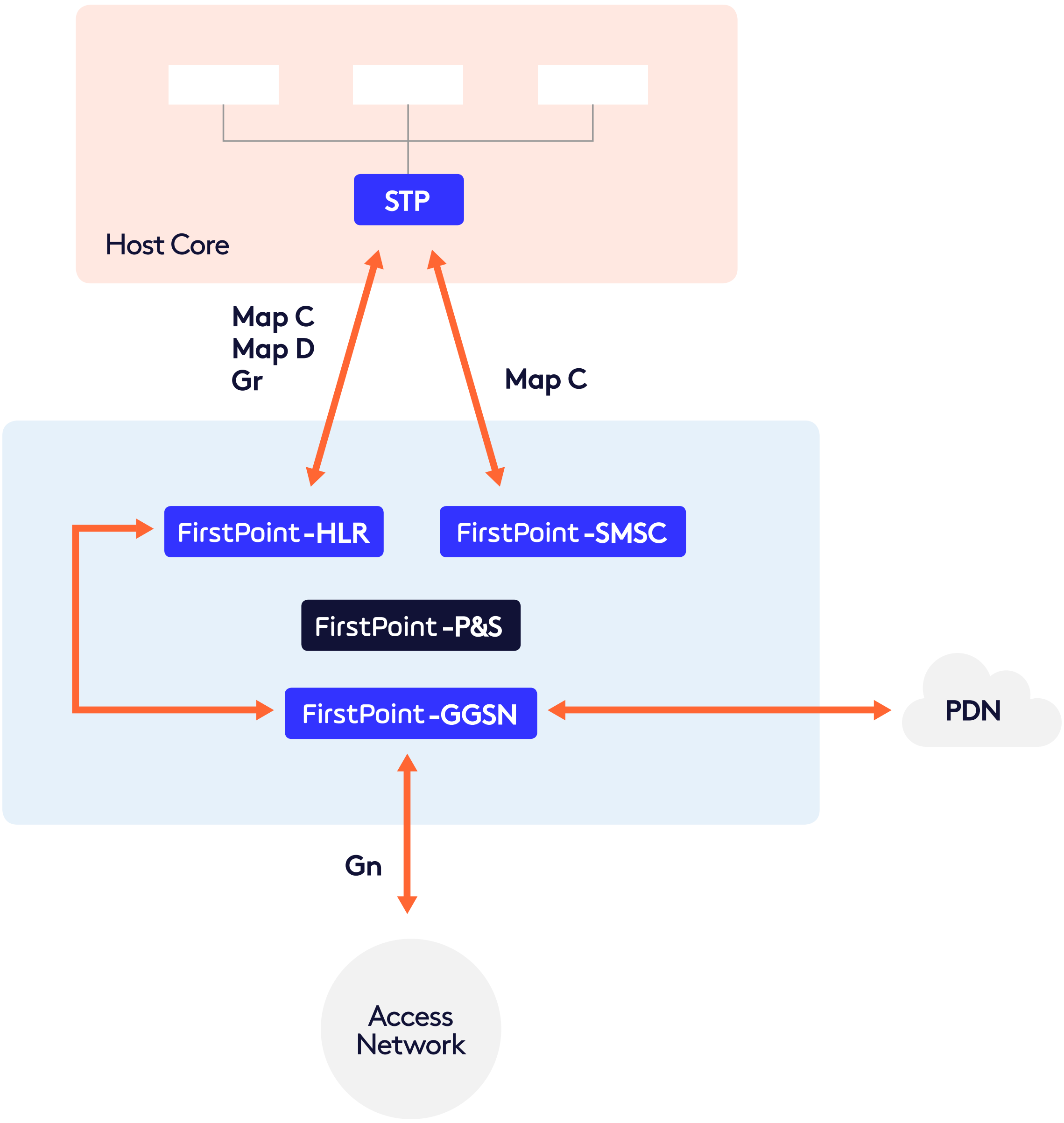
Deployment

Deployment is simple and straightforward:

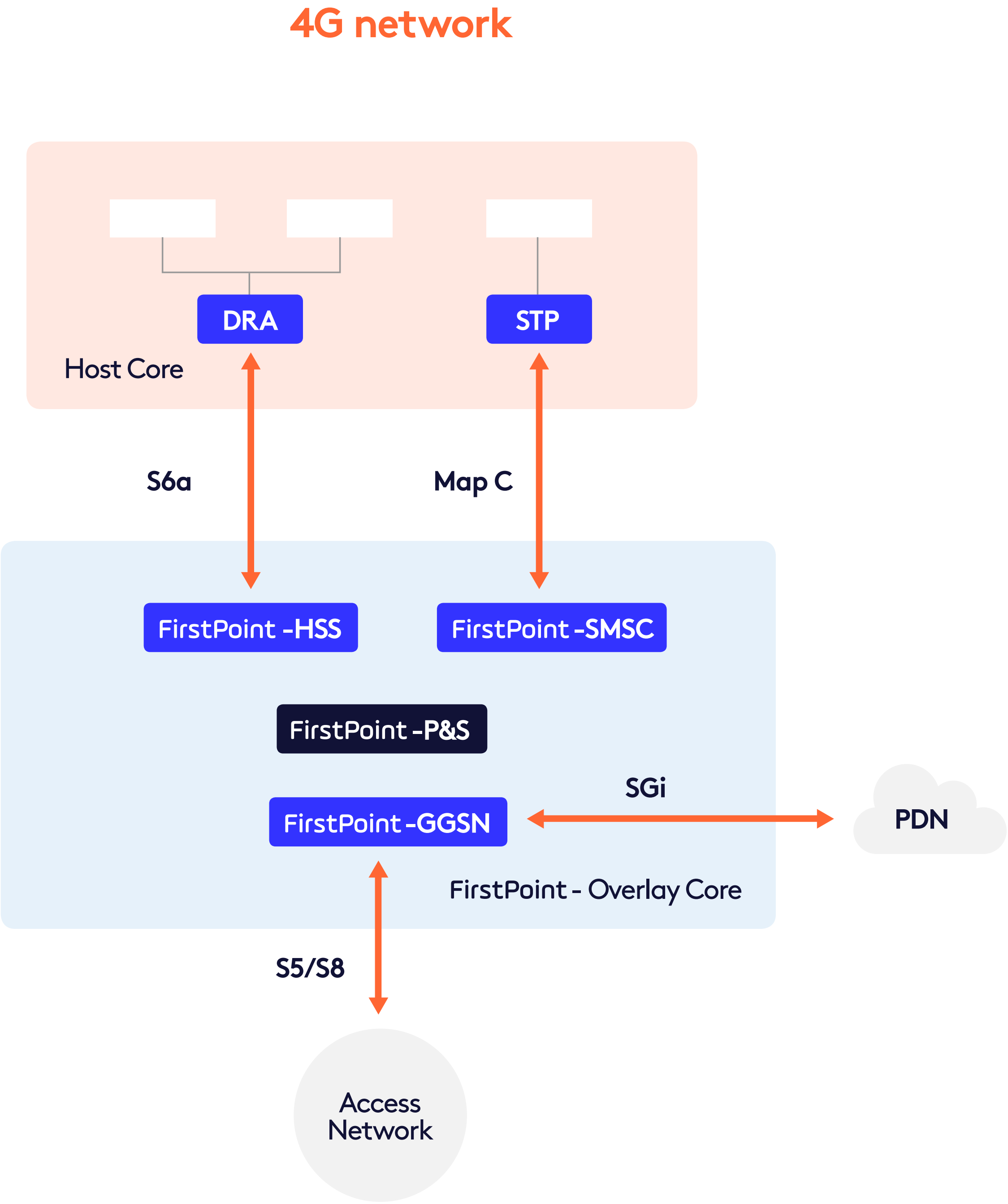
1. Define a list of devices to protect;
2. Deliver a SIM applet via OTA, or with new SIMs;
3. Users operate their devices as usual; organizations receive event alerts and health summaries.

System architecture

2G-3G network



System architecture



Conclusion

Despite the best efforts by the Telecom industry to improve cyber security and protect MNO cellular subscribers, cyber attackers still find new and innovative ways to launch attacks.

At **FirstPoint Mobile Guard,** we have made it our mission to stay in front of cyber attackers by providing cutting-edge cellular cyber security.

Feel free to contact our team to discover more:

FirstPoint

✉ secure@firstpoint-mg.com

Follow us!

f 🐦 in

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 known and unknown attacks 24/7, instantly activating protective measures.
Solutions are completely transparent to the user/device, with no device installations, updates or slowdowns, protecting any device; e.g., mobile phones, M2M, security-sensitive IoT devices and connected systems.