FirstPoint

The 5 greatest threats to mobile cyber security today

A FirstPoint e-book

March 2020

The 5 greatest threats to mobile cyber security today

Mobile security is very high on the list of what keeps organizations' information security and IT managers up at night. There's a good reason for their loss of sleep. Recent events make it clear - everyone is vulnerable to a mobile hacking attack.

Consider the high-profile hack of Amazon founder Jeff Bezos' phone in May 2018 that made headlines in recent months. This attack was launched using an infected WhatsApp video file allegedly sent from Saudi Arabian hackers. To mobile security experts, this came as no surprise. In its 2018 Android Security Report Google noted an increase in pre-installed PHAs (Potentially Harmful Applications) like trojans, spyware, and phishing apps. More recently, BGR published a report indicating that numerous popular Android apps were secretly feeding large amounts of data back to servers in China.

As a result, **enterprises and government agencies are deploying mobile device management solutions to maintain some kind of control over the most challenging type of end-point devices - employee smartphones.**

Not as well publicized as PHAs, sophisticated attacks exploiting mobile infrastructure vulnerabilities are on the rise. Exploiting legacy cellular network security flaws, these attacks are particularly hard to detect and prevent.

FirstPoint Mobile Guard (FirstPoint), as a cellular cybersecurity company that's been extensively researching mobile threats and their prevention, presents you with this e-book. In it, we detail the most devastating threats to cellular devices today and propose the best approach to mitigating them.

Adam Weinberg

CTO and Co-founder, FirstPoint Mobile Guard

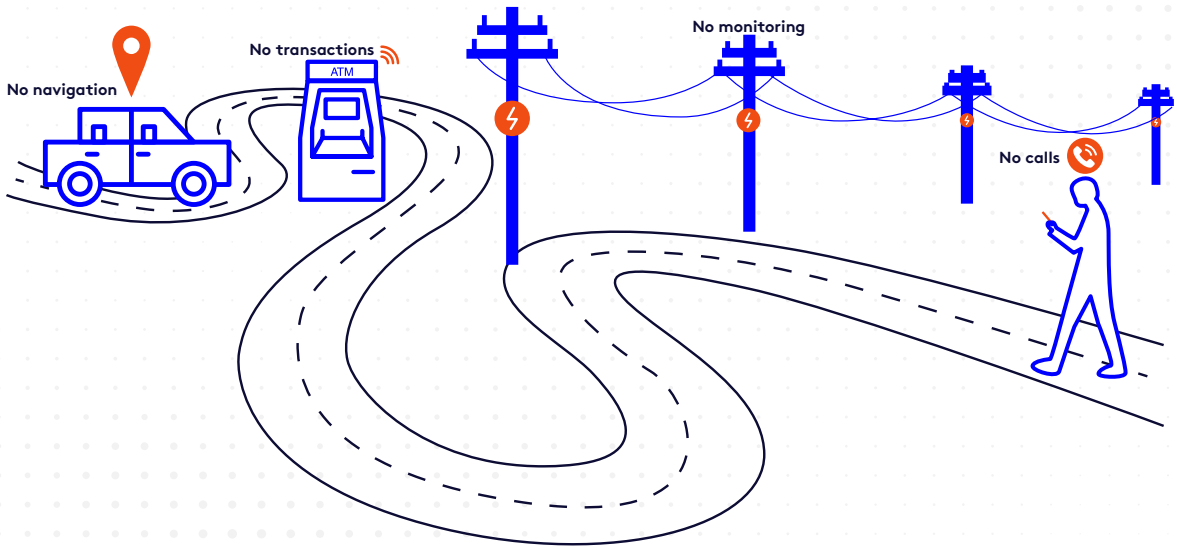
(1) Denial of Service (DoS) attacks

If users ever encounter degraded or lack of cellular connectivity when trying to access online resources, then their connection could be the victim of a denial of service (DoS) attack.

Signs of a DoS attack

- Suddenly no cellular coverage
- Your device has been quite longer than usual
- People around you have service and you don't
- Phone rings, but no calls received
- Expected SMS are not received

DoS attacks are a danger to mission-critical connected devices and users. Users may suddenly have no way to make calls, access online resources, send or receive instant messages, and IoT device cannot access information or perform transactions.



How do hackers launch a DoS attack

An attacker can deny a device cellular service by using a fake cell tower or by executing a signaling attack on the network. There are additional methods to perform a denial of service in the data domain, which we will not review in this ebook.

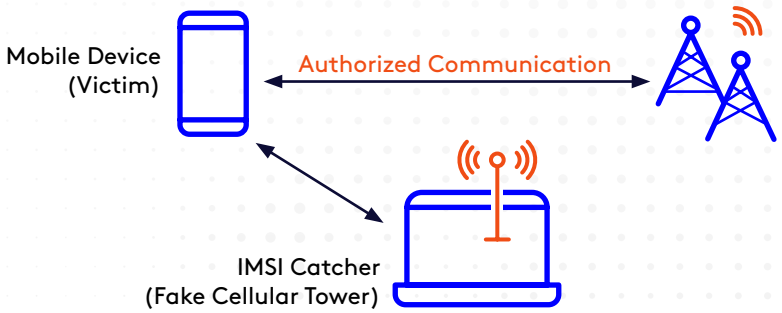
Fake cell towers

Choose me for the best connectivity – and the dire consequences.

Fake cell-tower attacks, also known as IMSI catcher, are based on the attacker operating a device that **pretends to be a genuine cell tower of the cellular network**. Such attacks can also include a jammer, jamming some of the radio frequencies bands of the cellular network.

Fake cell tower attacks are relevant in all generations of cellular networks.

5G networks are no different from 2G, 3G, and 4G networks in this regard. Despite the considerable efforts devoted to increasing security, recent publications describe methods of implementing 5G false cell tower attacks by several means including manipulation of the device's registration process on the network and implementing sophisticated impersonation attacks.



Signaling based attacks

Abusing network trust

Mobile operators have been using the SS7 protocol and the newer 4G Diameter protocol to provide uninterrupted phone conversations and messages, as well as roaming on partner networks and other services.

These protocols, however, are based on trust, where **it is assumed that mobile operators would not exploit them for malicious reasons.**

In Signaling based attacks, the attacker, having gained access to the internal links of the cellular network, maliciously manipulates some signaling messages flows, eventually creating a denial of service situation for specific devices.

The advantage (from the attacker point of view) of such attacks is that they can be performed practically remotely – the attacker can even be located in a different country then the attacked device, and still initiate very effective DoS attacks against targeted devices.

Why do attackers initiate a DoS attack

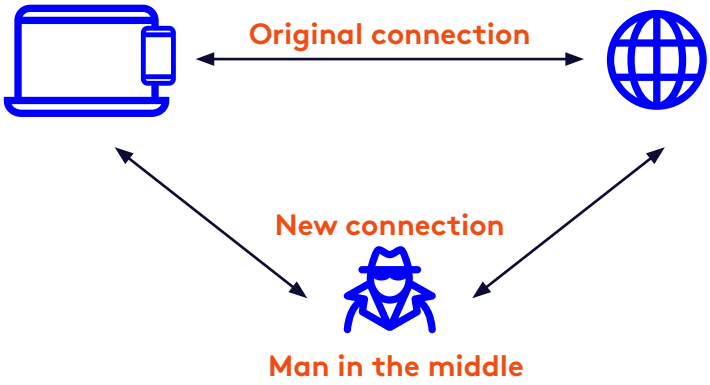
Interrupting critical communications	Preventing devices or users from accessing crucial services at specific times such as emergencies
Hijacking for ransom	Interruption to services like remotely connected medical devices and infrastructure IoT systems can be potentially catastrophic, and hackers capitalize on this to extort businesses
Hacktivism/political motivation	Attacks on infrastructure in specific regions and communities can serve as a political tool, limiting the access of specific groups to online services
Cyberwarfare	Governments often sponsor, whether openly or not, groups of hackers to launch attacks on enemy state infrastructure. A well known example, though not mobile network related, is a DoS attack on the Iranian Internet, that impaired connectivity country-wide.
Just for fun	Amateur hackers – teenagers, too – want to show they can create chaos

(2) Communication Interception

This particularly nasty attack "sits in" on two-way communications, and can **listen in on voice communication, SMS and IP/data transfer.**

Worst of all, **some interception attacks are not easy to detect, because as the traffic is intercepted, no trace is left by the attacker to indicate that it ever took place**. They can usually only be uncovered when the hacker piggybacks on the connection to send their data packets.

Rarely, these attacks are publicly showcased. However, such is the case of private investigators in London using IMSI catchers to track journalists for a foreign government, as well as MitM attacks being used in the Russian - Ukraine conflict of the last several years.



How do hackers intercept communication

- **Passive mobile base station monitoring** - accompanied in many cases with some active measures (jamming or more sophisticated manipulations) aimed at downgrading the connectivity of the device to less protected protocol.
- **Fake cell tower-based eavesdropping** - implementing a MitM attack: the attacker operates equipment which on one hand pretends to be the network towards the attacked device, while on the other hand, it pretends to be the target device towards the true network. In the middle – the attacker has full access to the communication of the attacked device.
- **Signaling based attack** – having gained access to the signaling network interconnecting the mobile operators, the attacker manipulates the flow of the communication of the target device so it passes through a destination operated by the attacker. One possible example of such an attack: maliciously applying Call Forward.
- **IP network-based attack** – malicious manipulation of IP protocols, causing the IP/data communication to be routed to a false destination, operated by the attacker. This is the case in DNS spoofing attacks for example.

Why do attackers intercept communication

Espionage

Mostly utilized against targeted people or devices. Governments, terrorists, private investigators and criminals can perform MitM attacks to gather sensitive intelligence about their targets' business, movements, actions and plans.

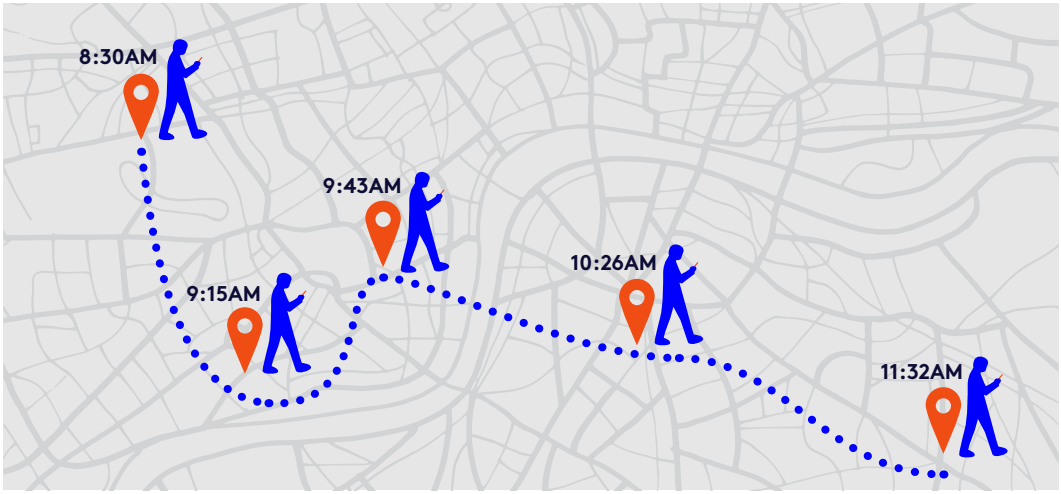
Financial gain

By intercepting banking activity or gaining access to user credentials for banking services, attackers can easily transfer funds to their accounts. Once an attacker obtains private information about an individual they can use this data to exploit, extort or blackmail.

(3) Location Tracking

Anyone can track a device location, as long as it's on and transmitting signals. Applications like Apple's Find My Friends or Google's Trusted Contacts for Androids make it easy, by using GPS signals– with your permission, of course.

However, mobile device location can be identified and historically reviewed through the mobile network, regardless of GPS use. This is enabled so operators can locate devices by cell towers to deliver calls and SMS. Law enforcement organizations use this capability to track criminals, terrorists or even missing persons by submitting a warrant to local mobile operators. But, attackers maliciously utilize this powerful tracking capability to remotely track any mobile device globally. The Dark Web has become a "trusted" source, even offering tiered plans to reveal a device's location.



How do hackers track locations

- **Signaling based attack** – SS7 is a legacy communications protocol that brokers calls and text messages between mobile networks. The attacker maliciously gains access to this global signaling network and extracts the position of the target using messages pretending to legitimate. This involves also specially crafted messages (typically called "silent SMS" which leave no trace on the target device) sent toward the target device, causing it to start a radio frequency (RF) activity that discloses its current position to network.

- **Malware based** – a more commonly known attack vector is the use of malware installed on the device to perform criminal acts. It's possible to use malware for device tracking as well, sometimes by gaining access the device's GPS location. This is done by crafting malware, sometimes even adopted for a specific device type and then using it to report the location to the attacker.

Why do attackers perform location tracking attacks?

Espionage	Track individual's locations locally or abroad to identify where they are traveling to and who they are meeting. This is a useful tool for corporate espionage to gain knowledge about competitor whereabouts.
Intelligence	Follow military forces, for example, to identify where they are gathering and which locations they are headed for.
Criminal	Identify an individual's car's locations to break into their house while they are away or follow an individual to rob or physically attack them.

Espionage Intelligence Criminal

(4) Information Theft

Mobile phone's microphone, camera, GPS and screenshot feature allow real time intel gathering when active. This makes mobiles a prime target for information theft by attackers that gain aim to access private or business data on the device through applications, stolen credentials and more. Recent well-known cases include "coronavirus map" to steal confidential data, including bank account details and passwords, fake dating apps aimed to insert trojans, and a fake Netflix site amidst the surge in home isolation streaming.

How do hackers steal information

- **Malware** – specially crafted malicious code delivered to the target device by various methods, is used for harvesting the required information from the device and delivering it covertly to the attacker.
- **Malicious site** - using social engineering techniques, the target is convinced to access a malicious site using a tempting message, email or link. The site, either operated by the attacker, or a legitimate site compromised by the attacker, activates a tool to access the device's browser (usually) causing is to manipulate the device operation as defined by the attacker. This includes operating the camera, operating the microphone and more.

(5) Account Hijacking

This category of attacks includes a variety of methods enabling the attacker to overcome all security measures, and access private accounts of the attacked user on their behalf, by impersonating the target. Well known examples are penetrating bank accounts and performing money transfers, or accessing email accounts and private information and SIM swap bitcoin thefts.

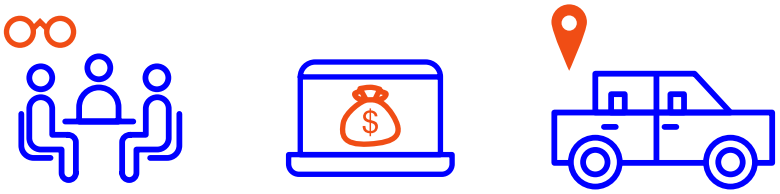
Another goal of such attacks is penetrating internal private networks through the attacked device to extract information or deliver dangerous malware to internal servers.

How do attackers hijack accounts

- **Social engineering** – not a cyber-attack per se, attackers convince users to provide their account credentials via well crafted emails, phone calls or texts urging the victim to provide their account info for some "legitimate" reason.
- **Fake site link** – using email or SMS including tempting or alarming messages the target is convinced to click a link to a site that looks like a well-known company's real site, but is actually fake and controlled by the attacker. Once the victim enters his/her credentials into the fake cell, the attacker copies them and can use them to access the real site. This can even include triggering a one-time password (OTP) from the real site to the attacked device.
- **2FA hijacking** – in many cases sensitive accounts use multi- or two-factor authentication (2FA) that's sent as an SMS to the account owner upon entering accurate credentials. Hijacking these one-time passwords (OTPs) can be performed as an additional step to access
- **SIM swapping** – the mobile operator is tricked by the attacker to issue them a new SIM card with the identity of the attacked device. This is achieved by taking advantage of pure security procedures and human errors of the MNO personal. Once the new SIM is operated by the attacker – all SMSs sent to the target are actually received by the attacker including 2FA SMS for accessing accounts.

Why do attackers steal information & hijack accounts

Corporate espionage	By targeting specific users, attackers can gain access to privileged corporate information which can then be traded on the dark web or used as a first step to cause greater harm to the organization.
Extortion	Access to compromising or personal photos and info on a user's device can be used as a tool to blackmail or shame.
Criminal	Obtaining bank account credentials, application passwords, live location and other info can be utilized to steal money or other assets.



Is there a cure for all these vulnerabilities?

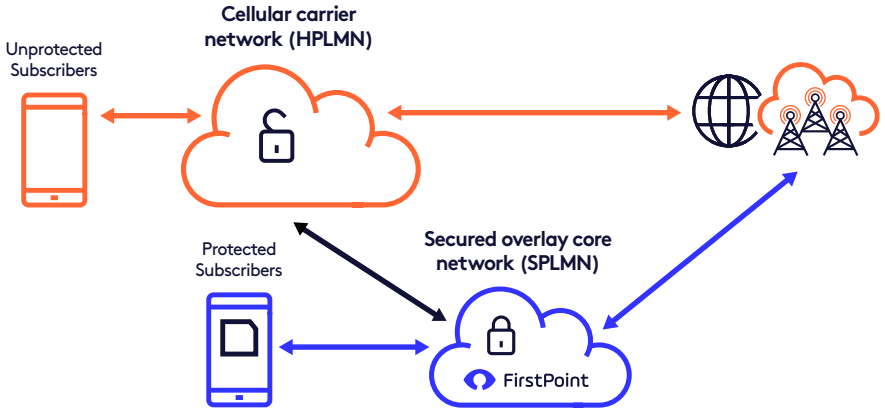
Reading about these cybersecurity threats to cellular devices provides food for thought. Nearly all solutions out there may solve some of these attacks, or partially solve some, but cannot solve all of them.

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 a network-based solution?

3G and 4G network vulnerabilities are known, and yet, solutions do not focus on some of the five greatest cell phone threats: Denial-of-Service, communication interception, location tracking, information theft and account hijacking.

Despite boosted security in 5G networks, users remain exposed to these vicious attacks. **A network-level solution is by far superior to one installed on the device not only because it is much harder to hack. It is also significantly easier to deploy and maintain with minimal user interaction.**



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 without user-activated updating.

Detects and prevents cyber-attacks at the network level

Blocks cyber threats with individually controlled security policies

Protects and conceals device network identity

Provides a dedicated SOC

Activates real-time alerts of cyber-attacks

What organizations get when they use FirstPoint

- 360° cellular cyber security
- Protection for any mobile phone or cellular IoT device, cars, modems: any make, model, version or OS - even while roaming
- One-dashboard management: per-device profiles
- Hassle-free, safe experience: simple implementation, no installation, no slowdowns, no battery/performance hits

The FirstPoint Advantage

Network based solution:
- Supports all cellular devices
- No battery drain
- No CPU load
- No need to update

2G-5G compatibility

Flexible platform deployment

Organization-level policy management

Full anonymity

Real-time alerts

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 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.