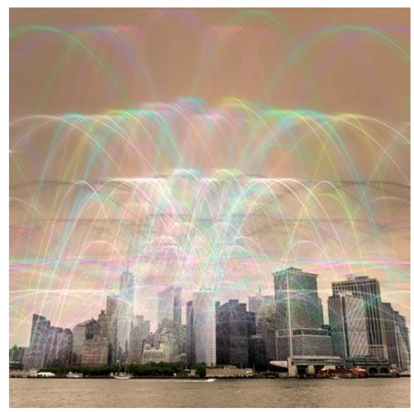
www.pipelinepub.com
Volume 18, Issue 9

Managing Cellular IoT Security Threats to the Enterprise

By: Adam Weinberg



Increasingly, organizations in critical infrastructure, healthcare, utilities, smart cities, point of sale, and other sectors are looking to IoT to enable remote operations and optimize the business benefits of connectivity.

However, enterprises' attempts to accelerate IoT adoption are often stifled by inherent challenges, from security to network reliability. Thanks to 5G and cellular-IoT cybersecurity technology, businesses can more effectively manage their cellular IoT deployments—ensuring more robust cellular connectivity, interoperability, cost reductions, and device security.

What 5G brings to the IoT table

5G alone has boosted the cellular IoT market to remarkable new heights. Connected devices could reach 30.9 billion by 2025. 5G helps enterprises achieve super-speedy data transfers, which allow cellular IoT devices to process, communicate, and share information significantly faster than earlier-generation devices. 5G also brings unsurpassed network reliability and lower latency, resulting in enhanced operations, stable and uninterrupted connections, and the capability to handle numerous IoT-connected devices.

Obstacles to enterprise IoT adoption

In all cellular networks, from 2G to 5G, attackers leverage existing vulnerabilities; simply because wireless devices communicate, they are more susceptible to interception than wired ones.

In addition, IoT devices, by their nature, are driven by low cost. Some devices are not secured because they were created to do a straightforward task and do not include sufficient security features. The result is that such devices often produce security “holes” or vulnerabilities within the enterprise networks. This is one reason that network-level security is so critical.

While 5G offers safer and more dependable connectivity, delivering that promise depends on how dedicated enterprises are to securing their 5G networks. 5G networks—and 2G to 4G, for that matter—operate under a torrent of threats.

Enterprise Cellular IoT Device manipulation

Battery drain attacks

Because IoT devices rely on battery power to function, these attacks can end up being costly. This is especially true when, because of an attack, 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.

Functionality attacks

These attacks exploit loopholes in the device or network systems to gain access to control functions. These 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.

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 objective. In most cases, it involves maliciously altering the APN (Access Point Name) registered on the device, 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 theAPN. 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. See Figure 1.

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

Using IoT devices as tools in an attack

IoT devices as a gateway

IoT devices themselves can be used to gain access to a company’s internal systems. 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.

Enterprise cellular IoT Denial of Service (DoS) attacks

IoT DDoS attacks

In addition to using IoT devices to gain access to data, attackers can employ them to launch Distributed Denial of Service (DDoS) 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.

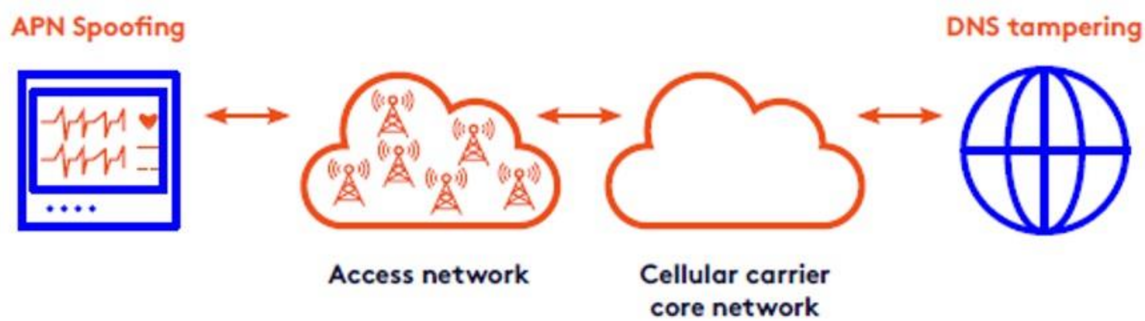


Figure 1: How a data channel rerouting attack works

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. 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, and halt the production of electricity, all while preventing administrators from accessing their systems.

Non-targeted DoS attacks

These 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

These are like other DoS attacks but made 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.

Enterprise cellular IoT identity compromise

ToRPEDO attacks

ToRPEDO (TRacking via Paging mEssage DistributiOn) attacks allow hackers to determine the identity of the device and where it is located within a geographical region. Such attacks 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

These attacks allow cybercriminals to impersonate devices or users by exploiting integrity protection flaws in the cellular connectivity protocol. 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.

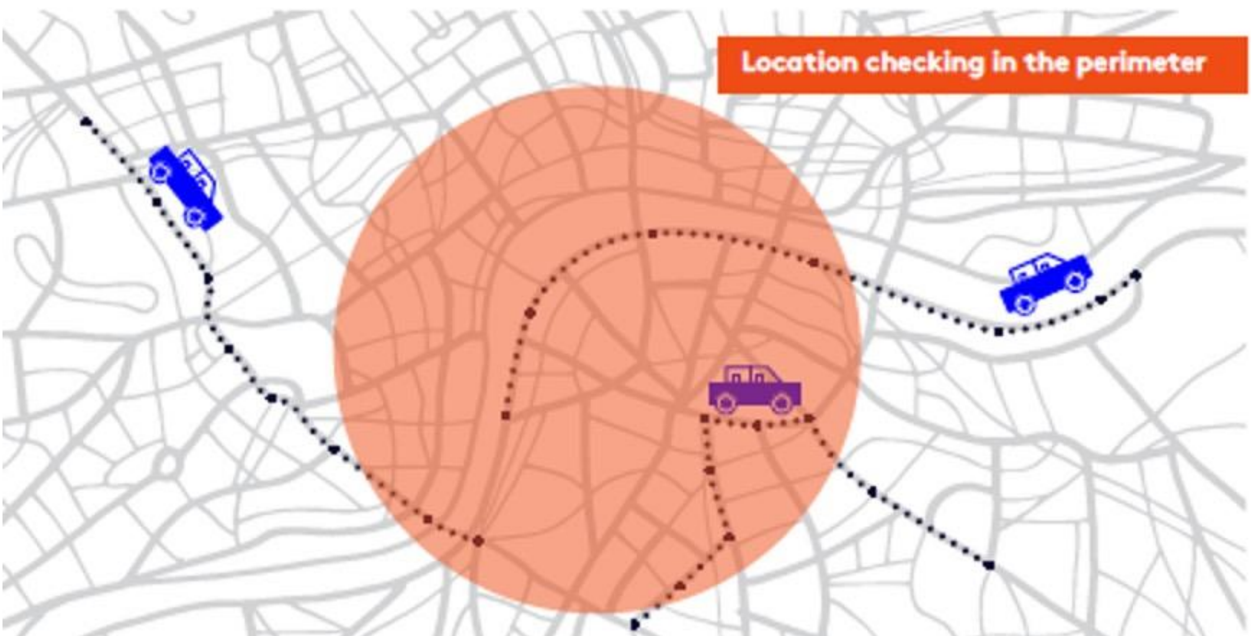


Figure 2: Location checking in action

Enterprise cellular IoT location data exposure

Location tracking

All cellular devices communicate with the network they are connected to. Among the data they transmit—and necessary for uninterrupted service—is the physical location of a device. By exploiting existing flaws in communication protocols like SS7 and Diameter, 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

Unlike location tracking, which follows a device around, location checking lets attackers know when a specific device enters a certain geographic location (see Figure 2, above). This can be, for example, a trigger as part of a wider attack to harm devices or business operations in a specific area.

Authentication attack

International Mobile Subscriber Identity (IMSI) or Subscriber Permanent Identifier (SUPI) attacks are major threats to cellular IoT devices. These attacks can deceive the authentication process, with the cellular provider enabling identity disclosure and impersonation. IMSI attacks are alarmingly easy to carry out: when a device connects to a cell tower, it authenticates to it via its International Mobile Subscriber Identity (IMSI). IMSI is a unique identifier linked to a SIM card and is one of the pieces of data used to authenticate a device to the mobile network. The issue, however, is that the tower doesn't have to authenticate back, making it extremely easy and effective.

With the sheer variety of possible attacks 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.

Accelerating IoT adoption

Many enterprises lack a user-friendly, efficient, and cost-effective connectivity solution that supports IoT devices and their use cases. Companies often must deal with system overload or network incapacity due to the sheer network traffic of deployed cellular IoT devices.

Finally, enterprises do not always have a single view of all their connected devices for visualization and operational control purposes. In some cases, their connected devices are spread across multiple platforms provided by the operator, making it hard to control all the connected devices in one place versus one central management platform that allows them to manage them all as if they were "one" device.

In a time of hyperconnectivity and record levels of cellular hacking, IoT security threats are hindering business operations for many enterprises that depend on their IoT cellular-connected devices.

Critical infrastructure—from power grids to financial services to telco operations—increasingly implement IoT to streamline operations and reduce costs. Yet, as security is often not embedded in the design of these IoT devices, it opens them up to cyber risks, such as threat actors interfering with services and even putting lives at risk.

Many mobile healthcare organizations that deploy cellular-connected IoT technology face threats that interrupt operations, resulting in risks to health and life, especially if the simplicity of the devices prevents built-in solid security.

Effective IoT fleet management maximizes utilization, minimizes costs, and ensures safe operations. However, insufficient IoT security for the devices tracking and managing cargo can encourage threat actors to attack and compromise the cargo.

Moving forward to connectivity success

Enterprises require solutions that will help them achieve their business objectives, from cost efficiency to easy-to-use interfaces, and security to customizability. Enterprises need complete network control to achieve easy, reliable connectivity and streamline security and operations. They need flexible configurations for fast deployments. They need simple and self-explanatory GUIs and easy-to-enforce business rules and security policies. Ideally, they'll be able to use a network-based, secure platform to assure protection against a whole host of security risks from network-based attacks. They should be able to isolate network services to ensure the security of enterprise data, provide low latency, and enable companies to self-control the network. Operator lock-in can also be an issue if the operator doesn't supply the appropriate connectivity or service. Therefore, having contracts with several operators gives an enterprise more control over the management of its IoT cellular devices.

With complete control of their connected devices, enterprises can have the peace of mind to focus on meeting their business goals. Optimum cellular-IoT connectivity management and security streamline IoT device operations—helping the enterprise make things run more smoothly.