www.pipelinepub.com
Volume 17, Issue 9

Baking Security into Cellular IoT Deployments

By: Adam Weinberg

The Internet of Things (IoT) is bringing some of the most change-resistant businesses into the vanguard of the digital age. Utilities, healthcare, manufacturing, agriculture, and a wide range of other industries are revolutionizing their operations with smart, interconnected devices and sensors. For many of these enterprises, private cellular networks are the obvious solution for getting these devices to talk to each other in the field. The pace of cellular IoT adoption is picking up, driven by cellular standards designed to fit the low-power, low-cost requirements common to large-scale IoT implementations.

The number of narrow-band IoT connections has quadrupled over the past two years, and is projected to reach 1.2 billion by 2025. Cellular networks are an affordable, scalable solution for organizations that need to build and maintain robust IoT systems for modern applications.

But the benefits of cellular IoT come with challenges that need to be taken into consideration early in the process of blueprinting your IoT deployment—challenges like mitigating the risks associated with cellular networks and remote device installations. One frequently neglected risk is actually an old threat that is rapidly becoming relevant once again: signaling attacks.

Consider the case of an agricultural operation that uses IoT devices to monitor greenhouses for temperature, humidity, and other conditions. A malicious competitor could connect to the network and use their own device to send signaling commands that allow them to gain unauthorized access to the network and execute attacks to stop watering, turn off the grow lamps, and send false data back to whoever is monitoring things.

This may seem like a lot of intrigue over some plants but concerns like this are very real for high-stakes growers. Take medicinal cannabis farms as an example. In addition to utilizing IoT sensors, valves, and other growing equipment, installations like these frequently protect themselves from theft through the use of extensive physical security devices such as motion detectors, video cameras, and smart fences. These devices could be disabled through attacks carried out over the cellular network. Sophisticated hackers could even use a man-in-the-middle attack to override a live video feed, just like in the movies.

The particulars for businesses in other industries may differ, but the threat remains the same: cybercriminals accessing IoT devices through cellular connections for the purpose of causing harm.

Signaling attacks & cellular IoT: old problems, new risks

Generally speaking, IoT networks give hackers plenty of opportunities to refine their craft and test many of the assumptions that these technologies were built upon. Unfortunately, IoT developers have been slow to make built-in device or network security a priority.

Software tools and encryption methods that provide security at the IP layer and device level offer important protections against certain types of threats. However, they provide no defense at all against threats like signaling attacks—a key vulnerability unique to cellular networks.

Signaling attacks can be used to intercept protected data, track the physical location and status of connected devices, send falsified communications, or disconnect devices from their network. The cellular networks in use today rely on signaling protocols that have been around for many years, such as SS7, GTP, SIP, and Diameter. The newer protocols were released to keep pace with advancements in cellular technology, but they're all designed to be backward-compatible and communicate with each other. This means that some of the vulnerabilities present in SS7, the oldest protocol, remain present in newer ones like Diameter, or even 5G.

Signaling attacks that exploit vulnerabilities in SS7 and Diameter have been known for a long time, but the unique properties of IoT deployments make them especially vulnerable to these types of attacks. Take, for example, battery drain attacks. With this type of attack, the hackers send signaling messages to a networked device that causes it to perform a function that increases battery usage. By sending the same message repeatedly, the hacker can effectively perform a denial-of-service attack by rapidly causing the targeted device's battery to drain completely.

A battery drain attack on a mobile network user's smartphone is a nuisance. A battery drain attack on a remote IoT device that performs a critical function in a high-stakes industrial setting is a different matter entirely. Let's return to the example of the IoT cannabis farm. If thieves wanted to sneak into the facility undetected, one way they could do it is by draining the batteries on the security cameras, which would allow them to gain physical access to valuable assets without leaving any digital evidence in the surveillance system.

Unarmed mobile network operators

What are mobile network operators doing to protect themselves and their clients from potentially devastating signaling attacks carried out over cellular IoT networks? The answer, unfortunately, is not much.

According to one study, three-quarters of all mobile operators would be considered vulnerable, with insufficient defenses in place to deal with all of the potential attack vectors into cellular networks. And nearly four out of ten operators don't know how often they're being attacked or how much it might be costing their organization.

One problem common to many organizations is a lack of institutional knowledge around cellular networks and their security vulnerabilities. Over the past few decades, cybersecurity has focused primarily on accounts carried out over Internet protocols. Security experts may have gaps in their knowledge where cellular defenses are concerned, and the relative newness of narrow-band IoT and its applications means that both the methods of attack and the most effective ways to prevent them are evolving fields of study.

As attacks on IoT deployments continue to ramp up, the decision to put cellular security on the back burner in favor of defenses that are easier to explain and quantify may come back to haunt some network operators.

Equip before you ship

With cellular IoT networks having inherited so many vulnerabilities from legacy signaling protocols, leaving tremendous potential for harm and abuse, it is critical for mobile network operators or private network owners to bake cellular security into the design of their networks as early on as possible.

Institutional expertise in this area is lacking. Not enough is currently being done to provide proactive forms of defense. Solutions based on VPN or encryption are simply not sufficient to prevent signaling attacks. It's up to IoT device management service providers and cybersecurity experts to make sure that their IoT deployments come online with strong supplemental security measures already in place, not added as an afterthought once devices are already in the field.

Once they're deployed, it can get very costly and complicated to reach IoT devices for the purpose of installing new security measures. This is especially true for the SIM-based security solutions that can actually provide protection against signaling attacks. You can imagine scenarios in which thousands of SIMs out in the field need to be recalled and replaced or picture the logistical challenges (and expenses) involved in retrieving a single SIM card in a mining rig located in the distant Alaskan wilderness.

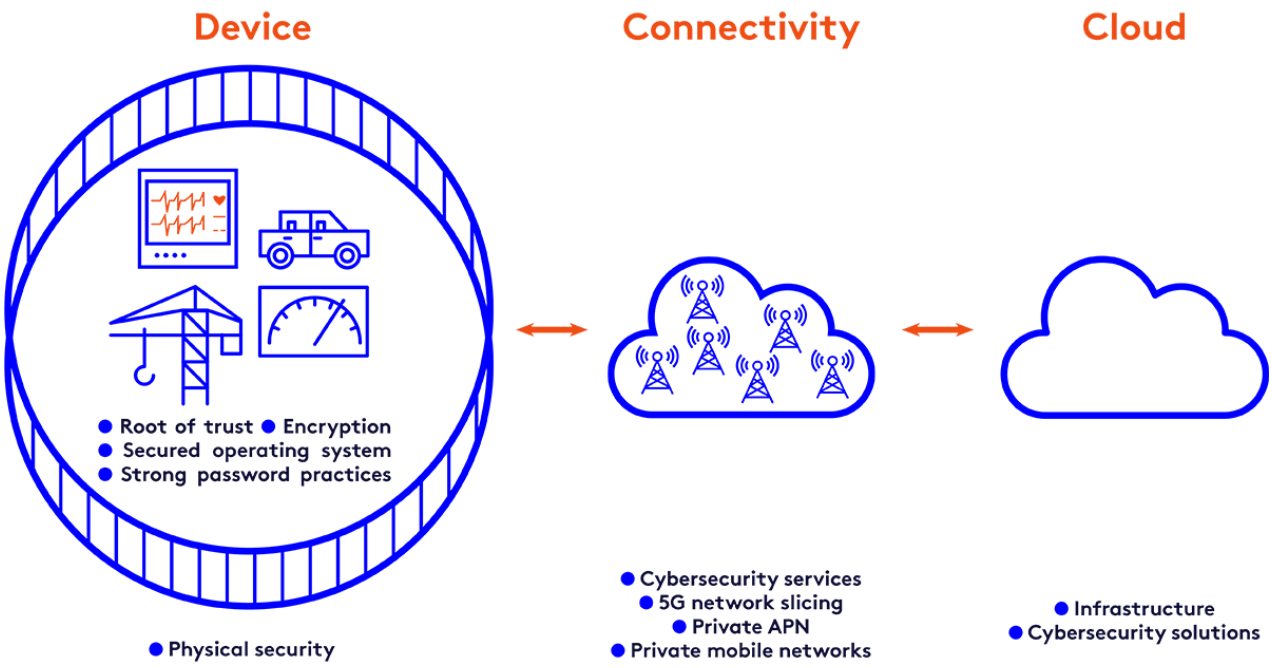

Figure 1: Cellular security overview
click to enlarge

The threat of signaling attacks tends to get neglected when blueprinting cellular IoT deployments. One way to tackle them is with device-agnostic security that works at the SIM card level. This can help detect and block signaling attacks to ensure that the devices remain safely online, carrying out their essential functions with minimal downtime.

Keeping your IoT devices powered up, online, and functioning as intended is important not just for preventing malicious attacks and revenue loss, but also for maintaining safety standards and regulatory compliance. The right security solution can give you greater visibility into the status of deployed devices and shorten the time it takes to diagnose problems that cause devices to go offline.

Maintaining a large-scale IoT installation is a massive undertaking that will present expected challenges as well as surprises. By incorporating security into your plans at the very earliest stages, you can make sure that your devices are protected from bad actors from the moment they're switched on.