www.pipelinepub.com
Volume 16, Issue 10

IoT Security:
Is the Real Test for Telcos Still to Come?

By: Stephen Buck

As we hit the mid-year mark, most communications service providers (CSPs) may have exhaled a sigh of relief to have withstood the coronavirus pandemic relatively unscathed. Even under enormous strain, such as when European operators experienced a 70 percent spike in traffic demand during the European pandemic peak, CSPs were able to maintain network connectivity. According to a member survey by the International Financial Group, part of the World Bank Group, operational performance was normal during the first half of the year, with service levels exceeding 99.95 percent. But a second, more sinister wave of risks may be just around the corner for CSPs.

In the rush to respond to stay-at-home orders, enterprises and consumers have quickly adopted the use of IoT devices to support remote working, learning, and caring. In healthcare, IoT devices are being used for remote patient monitoring, telemedicine and to support digital diagnostics. For example, the US saw a spike in the use of smart thermometers, which can help epidemiologists predict where an outbreak may soon occur. In retail, autonomous robots are being seen as a solution to maintain clean floors and deliver goods in grocery stores, big-box retailers, malls, and airports—showing how the digital transformation of some industries has accelerated more in the past six months than it has in a decade. As IoT adoption increases, now is the time for service providers to critically assess the security implications of IoT devices connected to their network.

In fact, the risks to network security are already abundant. A Mobileum poll of 90 global communications service providers found that 61 percent said network security threats have increased, and 75 percent experienced new or emerging incidences of fraud since the beginning of the COVID-19 outbreak.

More devices, but less secure

According to Gartner, the worldwide number of IoT-connected devices is projected to increase to 43 billion by 2023, an almost threefold increase from 2018. In five years, the attack plane of a CSP's network has grown exponentially, as billions of IoT devices flood the market. However, in IoT's case, millions of these devices will be connected to the network with limited or outdated security firmware. For example, it has been three years since a security vulnerability was first identified in the Zigbee low-power IoT protocol that is used in many smart lights and other IoT products, and it is still yet to be fully rectified. This shows the pervasiveness of unsecured IoT devices being connected to a CSP's network, and with the firepower to launch a DDoS attack by a simple flick of the light switch. As we see IoT devices become more mobile and autonomous, they will also need to roam between networks and be powered by network slices, each with their own security requirements. This new risk profile of IoT devices shows that the old approaches to network security are no longer adequate.

Multi-networks, multiple security vulnerabilities

Not only does IoT security involve managing diverse hardware, firmware, and operating systems, it may also require managing 2G, 3G, 4G/LTE and 5G communications protocols. Today's multi-generational networks are based on different signaling protocols that create different security risks. For instance, 2G and 3G networks run on the SS7 protocol, while 4G relies on Diameter, both of which lack built-in security features such as encryption and sender authentication and are more prone to spoofing.

5G networks have taken positive steps by building upon proven 4G security mechanisms, with enhancements for encryption, mutual authentication, integrity projection, and privacy. However, 5G's built-in cybersecurity features cannot roll back the clock and plug the existing vulnerabilities found in the other networks. This is particularly pertinent as 5G coverage remains dispersed, and traffic will continue to traverse between 2G, 3G and 4G/LTE networks for the foreseeable

future. While 5G may prove more secure, the same trust cannot be given when traffic crosses different networks.

IoT device security will become even more complex

The introduction of 5G network slicing will support a wide range of new use cases and revenue opportunities. However, the rise of network slices will also expand the attack surface available to hackers by exposing more entry points that need protection: user devices, radio access and core networks, the mobile edge, Internet, roaming and air interfaces. All of these must be protected.

The addition of APIs to these slices will mean more types of enterprises will be communicating, and they will all have different security requirements. Greater flexibility in managing who can send what will be required, meaning security considerations will need to be addressed at an individual level. For example, even though both 4G and 5G applications support video services, there are vastly different security requirements for mission critical video applications like remote surgery, as opposed to what would be required for a simple video conference.

To protect IoT devices going forward, it is paramount for CSPs to understand what the device is and the context of its communications. By doing so, you can understand if a device is changing its behavior, or if the eSIM/SIM card has changed. For example, changes in behavior, such as sudden spikes in traffic, can indicate that the device has been taken over by a botnet. By detecting changes in behavior, you can identify the signature of a rogue device and use this to find more devices with the same fingerprint and potentially block them. In addition, by analyzing the data that devices are sending with their mobile connectivity information, you will be able to identify if the rogue device is a lone actor or part of a wider, coordinated attack. To make matters even more confusing, COVID-19 has created a fundamental shift to what is deemed ‘normal’ behavior and traffic. Operators are now seeing significant volume increases both in data and voice, with domestic usage patterns shifting toward the day, away from the evening, and business traffic abating due to remote working.

According to a GSMA report, typical usage, such as call duration, is also changing. Traditional rules-based fraud and detection tools will not understand this shift, which could result in a spike in false positives alarms or worse, with fraud and security threats going unabated. This underscores the need for AI and machine learning-assisted fraud and security threat detection tools to recognize new patterns so that network security teams are equipped with the best protections.

In addition, CSPs will need to have the same understanding of how their IoT devices and subscribers are protected on-net as well as when they are roaming. In the case of your subscribers, if someone is driving their autonomous car on your network, you want to ensure that it is not vulnerable to attacks. Similarly, when your subscribers' devices are roaming on another network, you want to make sure they are being protected. Juniper Research projects that by 2022, IoT roaming revenues will increase by 20 to 30 percent. Therefore, multi-protocol signaling firewalls are required to ensure that traffic that traverses between your 3G, 4G, and 5G networks has the proper security protections in place, and that your roaming devices are steered to preferred partner networks.

Recent research sponsored by Mobileum found consumers and enterprises alike want CSPs to take a leadership role in the protection of their data and devices—and they want reassurance from their CSPs about the detailed steps they are taking. In fact, subscribers will stake their customer loyalty on it. The same research found that 58 percent of enterprises and 52 percent of consumers said that they would leave their operator in the event of a security breach.

IoT network security is complex, but not impossible. Developments in multi-signaling firewalls and AI and machine learning capabilities mean that network security teams no longer need to feel ill-prepared when it comes to IoT device security. Instead, they have the tools to detect current and emerging threats and protections that ensure that IoT-based messages are verified and allowed to be sent by that operator, to that user, in that context, from that location.