print | close

Securing the 5G Network

Electronic Design

Andrei Enescu

Thu, 2016-01-14 16:20

From an extremely low-latency communication network for the self-driving car to high latency designed to support the long battery life of devices associated with the Internet of Things (IoT), everyone wants a piece of the 5G network and is eagerly awaiting its arrival. However, each of these applications and many others being considered for 5G bring with them a variety of challenges that must be addressed before the 5G network can be fully utilized.

While everyone awaits 5G coming into its own as the standard wireless network, we need to take a step back and look at the issue of security, which is looming large. Security is rarely a consideration in the design and development of IoT devices, largely due to cost and time concerns, and we've seen in recent months the potentially devastating consequences of an unsecured self-driving car. No matter what it becomes, large amounts of information will be sent over the 5G network and that data must be secured and protected both in transit and at its destination.

Related

SDN 101: Defining Software-Defined Networking

What's the Difference Between Secure Comms and Secure Systems?

10 Things You Should Know About NFV

As 5G standards have not been set, we now have the opportunity to build security directly into the 5G network. Patches will always be needed, but a network with security built in will be more secure than one where security is a patched-on afterthought.

To accomplish this secure 5G network, it's important to consider three key factors: users' data, authentication and software-defined networking (SDN) and network function virtualization (NFV).

Focus on Users' Data

While the focus of network security has historically been on authentication and preventing billing fraud, the focus has recently shifted to concern over users' data. This shift is due in large part to the influx of data and users as the IoT continues to add millions of devices to the network. Because IoT devices, particularly those associated with smart cities, are often in public spaces and can therefore be tampered with very easily to either extract or alter the data they contain, this needs to be the chief focus regarding 5G-network security.

In addition, sandboxing must be leveraged to ensure that if one device gets hacked, not all connected devices are compromised. These widely available and quickly proliferating IoT devices are often designed without security in mind and lack an easy way to push out security patches. Thus, once a vulnerability for a device is uncovered,

h or without malicious intent, it's very difficult for a company to flip a switch and update the potentially lions of devices it sold around the world.

On top of that, malicious actors can use one insecure device to leapfrog their way into the broader connected networks. For instance, a smart coffee maker could serve as a backdoor into other devices with potentially more sensitive data on the same network. Sandboxing separates those devices, ensuring user data is more secure.

Authentication

A proliferation of wireless and wireless infrastructure driven by 5G will provide users with the bandwidth they need. Wi-Fi will be aggregated with the cellular network to provide data offload. This means that additional small cells will be distributed closer to the users, i.e. not physically secured. This increases the potential for physical attacks on the infrastructure. Authenticating the software loads on the infrastructure will help ensure that they have not been tampered with, and that the data or device is reporting true data.

SDN/NFV at the Core

It will be essential to have SDN and NFV remain at the core of the 5G network in order to accomplish these security goals. Due to its open, flexible, programmable nature, they may sound insecure. Nonetheless, beneath that façade is the ability to find and close security vulnerabilities quickly and easily, especially in comparison to traditional, static networks. SDN offers the ability to identify an issue rapidly and then isolate and apply patches to address it. In an environment that's constantly changing with new threats, the ability to evolve as fixes are made and stay ahead of future threats is critical. SDN also has the flexibility to accommodate new users and devices, while making it easier for 5G to adapt to the changing security needs that come with new users and devices.

Security is a key concern for networks as more devices and users continue to infiltrate the network. However, the industry is presented with a unique opportunity to future-proof the network as 5G standards have yet to be set. With the industry still in the preliminary stages of 5G, there's no better time than the present to build the network with security built in—not bolted on.

Source URL: http://electronicdesign.com/communications/securing-5g-network