www.pipelinepub.com
Volume 17, Issue 9

The Private 5G IoT Security Imperative

By: Jimmy Jones

Just 10 years ago, cellphones had a single camera on the back, Jeff Bezos' billions of dollars was only in the tens, and mobile networks were just evolving from 3G to 4G. A lot has happened since then, but just how far telecom networks have come during this time is often lost in the blasé way we talk about MHz and GBs.

Think of it this way. Back then, the first Tesla, the Roadster, was the only model available and had a top speed of 125 mph. If Mr. Musk had kept pace with the evolution of telecom networks, his "5G Roadster" would clock 29,761 mph, meaning you could drive Route 66 in under five minutes. In fact, if the Tesla Roadster sent into space in February 2018 had been the 5G edition, not only would Elon's dream of getting to Mars have been achieved, but he could also be safely parked on Jupiter by now!

This sort of progress, while impressive, will completely pale in comparison to what we're about to experience as 5G finds its stride.

Security in the 5G era

5G is not just the next mobile generation, delivering more speed and flexibility. With 5G, telecoms are opening up and embracing a plethora of technologies to deliver more service than ever before. 5G will consolidate the most successful, innovative and widely operated applications. It will allow them to communicate and interact between each other, and more importantly, communicate with an ecosystem of billions of IoT devices globally.

However, all these individual applications and devices will have security vulnerabilities, with the potential consequences of an attack as varied and damaging as the infinite IoT solutions we can conceive. This magnifies the rewards for a hacker, increasing the temptation, likelihood and diligence of an attack.

Interestingly, 2011 was also the first time the white Guy Fawkes mask was adopted, now a globally accepted symbol of protest and cyber threat. Over this same period, telecom networks have experienced an explosion in cyber risk that was previously never considered. Vulnerabilities have been exposed, exploited and regularly reported in the media. But just as the last 10 years represents the "warm up" in technology terms, it is also just the prelude for security.

We are about to start the main event.

While 5G IoT autonomous cars and remote surgery are still a way off, areas such as agriculture and industry 4.0 are pushing forward, driven by the significant financial incentives 5G and IoT can bring to those businesses.

Imagine the impact for a manufacturer if they could monitor and evaluate environmental conditions, machinery performance, supply chain logistics, and even product quality in real time via sensors. This huge volume of data could provide invaluable insight and also power AI or ML algorithms, potentially allowing efficiencies to be pushed back via 5G to maximize the performance of smart factory equipment, or any other assets, optimizing productivity.

Again, network security is key, not only to protect the sensitive business information as we are familiar with in today's IT corporate networks, but also the operational technology (OT) elements of the business, the manufacturing line integrity, logistics chain, and even to employ safety. There is an important distinction. IT security tends to be better protected and have more monitoring for better visibility. It often also has well-rehearsed recovery strategies—networks can be restored from backups or use disaster recovery options to be restored in a matter of hours. Operational technologies are much more diverse and less protected and monitored, though the impacts of an attack can be far more serious. Simply affecting the logistics management, causing a factory to run out of a key component, could stop manufacturing for weeks. Turning off refrigeration of a vaccine in storage could result in the loss of lives. Almost all consequences will take longer than a reboot to resolve and will have massive knock-on effects.

To protect businesses, we need to consider how to secure the IoT, and how to secure the network that supports it.

Security in a connected world

Looking at the network, the enterprise has two principal deployment options. The first is to use a public mobile network operator, which may additionally be able to partition or slice the network to provide more privacy. The second is to opt for complete isolation and control, as enterprises have in their existing LAN environments, by building a private 5G network.

Public or private, one thing remains the same for early adopters: they're deploying network elements early in their security development cycle. These network elements are delivering state-of-the-art technology and innovative use cases, which will inevitably evolve very quickly as lessons are learned.

Mobile operators are working tirelessly to build out their 5G offerings, but at this early stage, the focus is almost exclusively on the core business. If an enterprise requires a more bespoke solution, what do they need to consider for private 5G?

Principally, it requires a 5G radio access network (NR-RAN) and core network functions for 5G based on service-based architecture (SBA), both delivered on virtual infrastructure, either NFVi or cloud-native. However, our factory example may blur the lines with some of the services described needing extremely low latency, meaning resources need to be as local as possible. This requires a technology called multi-access edge computing (MEC) to also be included into infrastructure design.

Moreover, these four primary elements require management and orchestration, radio-frequency (RF) planning, IT and public cloud integration and a comprehensive suite of support and maintenance services. This sounds complex and it is, requiring multiple varied skillsets from legal to negotiate for radio bandwidth licenses, public and private cloud expertise and a full composite of telecom skills—many of which need to be continued for the lifetime of the network in order to keep it running and secure.

Realistically, the only option for the enterprise is to employ a specialist system integrator who would deliver the private 5G via an ecosystem of vendors. Use of diverse vendors and a move away from monolithic vendor architecture is a key element to all of 5G, not only private networks. It promotes commercial competition but also innovation as more varied and niche core and radio access vendors come to market. But in security terms, it increases the supply chain risks, and creates opportunities for malefactors to use vendor interactions or functional differences caused by separate design streams to negatively impact the network.

All the effort in building the network is to enable IoT, so all security built in serves to protect the foundations the services rely on. However, the network is only one element of an IoT solution and in order to protect it, you need to look at it end to end.

Security challenges

IoT can be considered the "device," the "network" and the "application;" this is its DNA. Mobile IoT (MIoT) benefits from licensed bandwidth and SIM-based security in the same way your expensive smartphone does, so is inherently less vulnerable. However, the devices can be anything, some so small and limited in hardware resources they simply cannot support cybersecurity. Many will be sensors or other inaccessible nodes, meaning they are "set it and forget it," generating limited maintenance and long lifecycles—both adversaries of security.

Speed to market and cost is key for IoT vendors, and to support this, most will reuse components and software to reduce overhead cost. This compromises the continuity and security of design and allows cyber techniques to be reused on multiple, possibly very diverse and not obviously related IoT solutions. Regulations and legislation could combat this issue but currently they appear to focus on particular segments of IoT such as government applications. This will eventually trickle down over time, but the exposure will be there, and success depends on how well-harmonized the guidelines are globally.

Some assets are too expensive to replace, so instead will require retrofitting of connectivity. This again represents a compromise in design, and potentially security. We must also remember that security, or even connectivity, may not be a core competence of the manufacturers upgrading, or building IoT—meaning processes and testing for security must be an integral part of rollout.

We've seen that MIoT and 5G will be large and consist of exponentially more vendors and suppliers than ever before and the skill needed to secure them will be equally more diverse. To be effective, security needs to be considered for the end-to-end solution, from the device through the network to the applications that run them. This is true in not only recognizing threats but addressing them. To tweak a problem with a network setting or in the application code is more effective than a visit to the hardware.

Cooperation between network operators, network vendors, IoT manufacturers, system integrators, security professionals and 5G consumers is the only way protection can scale to secure 5G. Enabling this collaboration is just as important as any technology.

What will we be contemplating in 2031?

5G will move the primary use of telecoms from individual humans communicating to something far more encompassing: any IoT device communicating with the network. Historically, this could be compared to the invention of the printing press. Instead of limited person-to-person communication by letter, newspapers and books allowed delivery of information much more widely. This sharing of data created a consciousness that drove a speed of social and political change never seen before. This was unprecedented and unpredictable, and it brought about huge global change, bringing down governments and monarchies.

2031 will see 6G designed to allow every device to communicate with every other. This could represent IoT's arrival as true social media, with billions of interconnected devices communicating with each other at a global scale.