www.pipelinepub.com
Volume 17, Issue 4

5G: The Next-Gen Threat to Security

By: Jimmy Jones

5G promises to provide ubiquitous connectivity: wherever we are and however we live, at some point almost every facet of our lives will in some way rely on this hyper-connected new world. And that's also the best way to understand the scale of the security threat 5G brings with it.

Right now, that scale is hard to fully absorb—but the level of impact is clear, and it's why governments everywhere are trying to secure the technology.

The European Union's EU Toolkit (supported by ENISA, the European Union's cybersecurity advisers), the Cybersecurity and Infrastructure Security Agency (CISA) strategy document and the US administration's Clean Network initiative all point to dramatic increases in regulatory involvement and authority. We also see the much-publicized restrictions on high-risk vendors, particularly Huawei, and numerous other steps. All these moves show that administrations understand how 5G completely changes the playing field.

Understanding the security threat

Today, when attackers intercept an SMS containing a two-factor authentication message, they can commit serious fraud. If they hack the network to affect a service element, then they can possibly interrupt coverage and hamper the ability to contact emergency services.

Similar types of attacks on 5G infrastructure would be much worse. Instead of only hampering emergency services, they could halt them altogether. Such attacks go beyond personal financial fraud to directly affect your property or even personal safety. The effects could touch all sectors of society, including healthcare, transportation, utilities and more. This escalation skews the risk-reward equation and will inevitably intensify hackers' efforts.

5G also accelerates the move to virtualization. Network function virtualization (NFV) has been with us for nearly a decade but has never gained the expected traction, thanks mainly to the accompanying complexity. However, 5G cannot realistically be delivered *without* virtualization, so the move to NFV and its successor, cloud native infrastructure, has to happen now. This is true not only of data centers but also of the satellite infrastructure forming at the virtualized network edge.

5G ushers in a service-based architecture to maximize virtualization and deliver the new services and benefits promised by IoT. The network currently supports one solution tailored to subscribers' use of their devices, but moving forward, every IoT solution will need its own environment—that's how each IoT service can have the latency, throughput and other features needed for success. Slicing the network like this creates multiple diverse networks, increasing the complexity exponentially. Now imagine this complexity multiplied again, simply due to the massive increase in numbers of connected devices.

5G also brings new technologies and protocols to what was previously a closed network. APIs become central to delivering 5G services, both at the core and the virtualized edge via multi-access edge computing (MEC) and radio access network (RAN). And remember, as Gartner forecasts, APIs will be the most attacked threat vector by 2022.

Security improvements

Universally understood protocols such as HTTP/2 offer a welcome security improvement, such as for international roaming interfaces. Here it replaces the much-maligned SS7, created 40 years ago and not designed to run on IP at all, let alone securely. However, using such a well-known protocol does remove the 'security through obscurity' practice. Early research in 5G standalone labs has already shown that HTTP/2 and Packet Forwarding Control Protocol (PFCP) are vulnerable—bad actors could steal subscriber data, intercept communication and cause significant network denials of service.

The same research does make a point that a majority of the vulnerabilities found rely on access to the protocols when being used within what should be internal areas of the operator network, isolated from the outside world, so if deployed correctly should not be possible. However, even with less complex networks, operators make mistakes in configuration and allow internal interfaces to become accessible through the global network. The same researchers highlight that if internal interface security is similar to today's GTP protocol implementations, then half of all operator networks will be exposed.

5G further brings a broader vendor pool to deliver new services and applications. We've seen the Open RAN initiative already get a boost from operators forced to replace Huawei: more choice eliminates vendor lock-in, which is good for operators and removes the security threat posed by monoculture networks. However, it also introduces a larger supply chain threat than ever before. Moving forward, operators need to adopt a zero-trust policy: the recent events involving SolarWinds prove this necessity. But this is far more difficult to achieve if instead of testing a full end-to-end solution from one vendor, you have to vet and test the five or ten vendors each responsible for a portion of the delivery.

These risks are all associated with 5G, but those linked to previous generations can't be neglected either. 5G will have to support legacy devices even in the most forward-thinking markets, and beyond the local market backward compatibility will be needed for many years. Connectivity to other regions for roaming is probably the most enduring: vacationing in small exotic locales usually requires us to use earlier mobile technologies, as the local economies may not be able to support the expense of upgrading, and that opens both us and our home network to the threats they contain.

Wrapping up: 5G and threats

To be clear, telecom networks are still the most secure way to connect devices; the same authorization and encryption you receive on a cellular device via SIM/eSIM/UICC technology underpins all connectivity, and this applies to IoT as well. 5G also benefits from security being a primary concern from the time these standards were initiated, marking a significant improvement from previous generations. In short, while all of the technical threats outlined previously are real, 5G also represents the best security choice for any connected device.

Not all threats are technical, however. Another factor in this perfect storm of security has to do with the integration of other industries' processes, workflows and expectations. Telecom has been a beacon of reliability for the last 140 years, achieved through design, testing, massive investments and cooperation between operators. However, all this takes time, and history tells us that time is not always available.

Some operators will recall the time and effort that went into the Rich Communication Suite (RCS) 15 or so years ago. Ironically, the technology is now being revived, but back then a host of competitors—Skype, WhatsApp, Telegram, and others—moved faster and captured the market. This is because telecom operators were held to a higher standard, both by regulation and to retain their premium reputation.

Telephone as lifeline

The telephone has always been our lifeline in times of emergency; 911 has been drilled into our psyche since we were children. If you ever have to call that number, you will use your mobile operator's direct service. This level of trust results from absolute diligence in service delivery and testing, which can take time.

So how does this work when 5G provides ubiquitous connectivity and new IoT apps appear every day? As some industry verticals move very quickly, how do we ensure security before integrating them to 5G? And remember, rolling out the service is just the very start: long-term security must encompass maintenance and management, including regular patching, upgrades, configuration, and more.

We can see clear signs of an acceleration in the industry already. After updating the 5G advice, ENISA noted that due to the "dynamic nature of 5G technology and the related threat landscape" they "may consider using an alternative electronic format ... to better support regular updates."

This is surely wise—and it shows how forward-thinking organizations understand the unparalleled threat to security. But it also indicates that ENISA understands that 5G is going to be far more dynamic and require a whole new way of working to keep pace with the changes and innovation we will experience.

In summary, we need to work together. Operators must be supported by all their vendors cooperating, with security specialists advising network equipment providers to secure as efficiently as possible. Providers of connected services and devices must share needs with their telcos to allow them to best understand them and support them. Finally, as consumers, we must be mature enough to grasp that security is an imperative. Our buying decisions have enormous power.

5G will soon touch every aspect of our lives. When it's truly secure, it can be hugely beneficial. When it's not, it can bring disaster. We have to do it right.