Building Trust –
What security means to 5G

Written by:
Gerald Reddig, Head of Security and Network Management Marketing, Nokia
We are about to make the leap from being a planetary civilization that uses networks to one that runs on them in a fundamental and inextricable way.

The more trust customers have in connectivity, the more likely they are to buy it — and to keep buying from its provider. This is true today and will be especially so in the coming years as new 5G services are launched, aimed not only at consumers but also at enterprises that put trust at a premium because their critical business data (and their reputations) are at stake, too.

In a world where building digital trust is an imperative for most companies the current COVID-19 pandemic has wide social and economic implications in countries around the globe. It comes as no surprise that cybercriminals are playing on people’s fears and are seeing this situation as an opportunity to promote their agendas.
Building trust will demand end-to-end optimization of 5G security operations — from devices and access sites to the cloud edge and network core without any compromise.

One thing is clear — 5G is part of future critical infrastructure and as such securing the supply chain is of national importance. The next generation of networks will have to be more secure than any that has come before. Instead of being applied to network services after the fact, security will need to be built in from the start, with the entire network acting as one giant, unified sensor to keep infrastructure and services safe.

The 5G era brings a number of challenges

As more factories and machines come online, Internet of Things (IoT) attacks become a risk factor, from device vulnerability and Botnet DDoS to malware, fraud and even rogue devices. Many Industry 4.0 use cases see devices connected to an edge network that essentially extends the telco or cloud network closer to where devices consume bandwidth.

With 5G, there will be more networks doing more complex things and delivering more kinds of services than we’ve used to. “Slicing” will become the norm: virtualization that allows network resources to be shared with third parties, with guaranteed quality of service (QoS) and isolation. Having end-to-end slices that terminate in private networks will increase the attack surface service providers need to protect beyond securing the network as a whole, they will have to protect every individual slice, each with its own distinct requirements.

Another change that will require providers and enterprises to fundamentally shift how they think about security is the nature of the services themselves. Today’s network services tend not to change once they’ve been designed, and they operate more or less in isolation from each other. They’re static and siloed. But sliced-based 5G network services will be incredibly dynamic, responding to evolving conditions in real time. For example, imagine a remote worksite with autonomous vehicles transporting people or materials from place to place. To keep passengers safe, those vehicles need to be able to respond very quickly to shifting conditions — whether that’s avoiding a herd of animals on the road or adjusting for weather-related hazards like flooding or black ice. Some of this will happen inside the vehicle and some of it will happen in the network. Vehicles’ onboard sensors and processors will combine with the network and control mechanisms in a single, end-to-end ecosystem. Security has to extend across this entire ecosystem and be every bit as flexible and adaptive as the services it’s protecting.

Analytics and automation are vital

What does flexible, adaptive, end-to-end security look like in a 5G scenario — and how can service providers build it in from the start?

The first prerequisite is visibility from the device up through the network and into the cloud. Without the ability to collect, correlate and analyze data from end to end, security threats could easily be missed. In a way, with 5G, the entire network becomes a sensor (or, really, a series of sensors), drawing data from various systems and devices to provide a complete, comprehensive, real-time view for maximum security.

5G security operations also need to be predictive and automated. That means using machine learning, multidimensional analytics and threat intelligence to correlate data from multiple domains and sources, catch anomalies, provide contextual intelligence about threats, weigh business risks and recommend (or enact) mitigation steps.
Analytics are important because many threats are designed to stay undetected for as long as possible, under the radar of the network security operation center or hiding in the information noise of minor, relatively harmless attacks. Machine learning and artificial intelligence (AI) can discover these kinds of “lurking” malicious activities and trigger countermeasures.

**Embedding security in the network**

While firewalls and other defenses will still be important to help stop hackers before they access the network, attacks will inevitably get through. This is especially true in 5G because the network will not have conventional boundaries: it will be an open ecosystem in which all kinds of unmanaged third-party devices are connected.

Strong security should be provided within the network to protect data and infrastructure. Integrated security workflow automation and orchestration are key to this, transitioning from static defenses to agile, adaptive, accurate threat responses.

Ultimately, these security capabilities add up to a set of required applications: active monitoring and workflow orchestration, privileged access management and analytics of user behavior, certification and management of digital identities of network entities, machine learning of traffic patterns for threat detection, automated incident responses, and more.
Key layers for a trusted eco-system

Service providers want to engage the market and monetize the investments they’re making in their networks to deliver on the new 5G use cases. As they do, they will need end-to-end security performance — at scale, from the edge to the core — to defend against advanced, persistent threats. The new 5G security approach integrates and automates 5G network security by treating the entire network as a sensor. Data taken from existing systems is used to give a much greater level of information.

For that, security has to be provided at four key layers:

- **Security intelligence**
  - Threat intelligence sharing
- **Secure data**
  - Access control, regulation and privacy
- **Automated security management and orchestration**
  - Security policies
- **Trusted infrastructure**
  - Devices, hardware, software, VMs

At the base level, security must be in place for both the service network and the cloud infrastructure. Moving up the stack, the entire infrastructure — spanning software, virtual machines, hardware and devices — also needs to be “trustable”. Automated security management and orchestration provide frictionless security across all these dynamically changing elements, and all sensitive data must be secure, providing access control, privacy and regulatory compliance.

Finally, to proactively detect and respond to security threats, security-related intelligence has to be shared across all the parts of the network — among a trusted eco system of suppliers, partners and customers.
Digital trust with a trustworthy partner

No matter how you want to build trust with your customers, Nokia can help. Our team has implemented more than 500 security projects worldwide over the past 15 years, and we play an active role in more than 5 standardization bodies that are shaping the latest in security standards and best practices.

With a long track record of producing secure products for mission-critical networks, the Nokia brand, as one rooted in our Finnish history, has long been a byword for trust with our customers.

We have built over time a catalogue of security requirements, grouped per priority and severity, that are mandatory in every product. This forms the proactive core of our Nokia’s Design for Security (DFSEC) process, which is also informed by our external engagement in industry forums like 3GPP and with customers and regulatory bodies. Taken together, all the various inputs are incorporated into Nokia’s mandatory security requirements. Our products are then assessed to establish a security baseline and to define roadmaps on security, privacy and interoperability; and later subjected to rigorous testing using both internal and commercially available tools. Wherever feasible, we utilize both static and dynamic code analysis as well as strong cryptography to ensure the integrity of our products throughout the development cycle.

We know that even the best software, rigorously tweaked and tested over and over again, could end up being shown later to have an exploitable flaw, and Nokia continuously monitors public and private sources for indications that our own software or 3rd party software embedded in our products could have a security vulnerability.

As we move forward in the 5G era, the systems we have in place through DFSEC give us a very solid center of gravity for effectively optimizing our security checks and delivering the type of reliable and secure products our customers have long come to expect from Nokia.

We’re working with partners and customers to build integrated 5G end-to-end security that applies across all the layers of the network. We also have an advanced security testing and verification laboratory to address the critical security needs of end-to-end networks.

In the 5G era, security cannot be an afterthought. It needs to be put in place right from the start, when new services are first being planned. Otherwise, the trust won’t be there — and the incredible new revenue opportunities that come with 5G could pass you by.

To find out more read our white paper: 5G security – a new approach to build digital trust or visit our Build Trust website.
About Nokia

We create the technology to connect the world. Only Nokia offers a comprehensive portfolio of network equipment, software, services and licensing opportunities across the globe. With our commitment to innovation, driven by the award-winning Nokia Bell Labs, we are a leader in the development and deployment of 5G networks.

Our communications service provider customers support more than 6.4 billion subscriptions with our radio networks, and our enterprise customers have deployed over 1,300 industrial networks worldwide. Adhering to the highest ethical standards, we transform how people live, work and communicate. For our latest updates, please visit us online www.nokia.com and follow us on Twitter @nokia.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2020 Nokia

Nokia Oyj
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: SR2003042480EN (March) CID207306