5G security is all-important for governments

By Gerald Reddig

17 Mar 2020

The 5G revolution is about to flip us from a society that "uses networks" to one that "runs on networks".

5G will connect everyone to everything. It will combine with other key disruptors - the cloud, robotics, AI and machine learning - to digitally transform even the most physical aspects of our lives. I can hardly think of a single industrial segment, public service or critical infrastructure that won't be running on 5G.

Image supplied

Anyone working in the security field, as I do, can't help but get a nervous flutter in their stomach when they read these words. If the security of our 5G networks is compromised, the consequences will be vast. And, as we all know, the more indispensable 5G networks become, the bigger the prize they will be for hackers and hostile domestic and foreign agents. This is why governments are being extremely careful about how they implement 5G.

Every aspect of government operations, from essential services to national defence, are potentially vulnerable if 5G security fails.

The network as sensor

Although at first glance, putting all our eggs in the 5G basket may seem imprudent, ubiquity is one its advantages over previous networks. Since everything will be on 5G, nothing will escape notice. Current IP networks, for instance, are not architected to know much beyond the next router or peering point and hackers have opportunities to marshal captured botnets unobserved and undetected, leaving security systems in reaction mode and, often, overwhelmed when attacks hit.

5G networks are architected around and include technologies like IoT, big data, artificial intelligence and machine learning. 5G will potentially be, among other things, a vast planetary sensor that can instantly spot anomalies and identify even multi-dimensional attack vectors.

This kind of intelligence and analytics will be necessary for 5G networks to be able to accommodate the multiple use cases and performance parameters that they will have to meet. It also equips them with the intelligence and resources to be able to sense attacks and defend themselves when required.

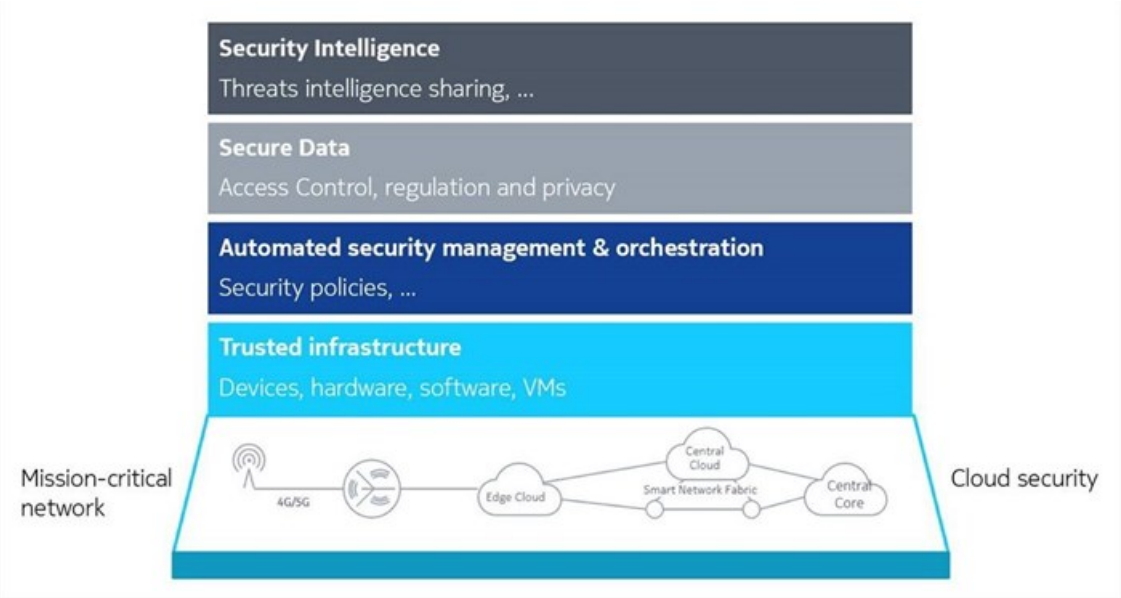

Image supplied

The security architecture for 5G has four layers.

At its base level, security must be in place for both the service network and the cloud infrastructure. Multi-layer, defence-in-depth security with robust encryption and protection mechanisms must be present.

Moving up the stack, the entire infrastructure - spanning software, virtual machines, hardware and devices - also needs to be "trusted". Automated security management and orchestration must provide frictionless security across all these dynamically changing elements.

At the third level, all sensitive data must be secure, providing access control, privacy and compliance.

Finally, security-related intelligence has to be shared across all the parts of the network, to help identify abnormal behaviour and traffic, and address it proactively.

Building integrated end-to-end security for 5G government and defence networks must include the full set of these layers and capabilities. Security labs that can apply the most advanced security testing and verification will also play a necessary role in rigorously and continuously testing whether critical security needs are met. At Nokia, we are committed to this kind of rigorous testing in our labs, for instance.

Armed with the intelligence and sensing capabilities of 5G, the job of security teams in the 5G era will be to limit how and where hackers can attack networks and services. They will need to be more accurate in determining which threats are real and which can be ignored. Fortunately, they will have tools like AI and machine learning to both identify and speed up

mitigation when a defensive response is needed.

As a provider of 5G services for government networks, we at Nokia are committed to offering these tools and sharing the advanced methodologies that we have developed working with mobile operators and industry standards bodies that will allow governments to secure their vital 5G-enabled national infrastructure and services.

ABOUT THE AUTHOR

Gerald Reddig, Director Product Marketing - Security and Network Management at Nokia