GCCM MAGAZINE

Carrier Community
Global Telecom Club

ISSUE 15, NOVEMBER 2019

Google invests in Clean Data Centers

WOMEN in tech

Huda al Habsi, Omantel

How Does Facial Recognition Technology Work?

– 5 Real World Use Cases

SOHAIL QADIR

OMANTEL

CREATING A GLOBAL HUB

READ MORE...

The need for state-of-the-art security with next-generation networks

5G technology is more advanced than its predecessors, but you cannot state the same thing when it comes to security.

Hackers will continue to take advantage of critical vulnerabilities in signalling protocols like Diameter and SS7 to perform criminal actions including tracking subscribers' locations, committing fraud, stealing personal data and executing denial of service attacks. Even during operators' transition from 4G to 5G networks.

Operators must minimise the impact of such attacks on their reputation and at the same time safeguard their bottom lines. But eager signalling security professionals are hard to come by. Advanced security solutions are therefore required, such as big data-driven portals with rich analytics, signalling firewalls, and monitoring capabilities for real-time detection of anomalous activities.

Sparkle

Sparkle is a leading global operator, with direct presence in 33 countries and an unparalleled experience and know-how in a multiplicity of diverse markets. With its IP&Data, Cloud & Data Center, Corporate, Mobile and Voice Platforms, Sparkle actively takes part in the development of worldwide communications, providing a global connectivity solution to Fixed and Mobile Carriers, ISPs, OTTs, Media & Content Players, Application Service Providers and Multinational Corporations.

Sparkle exploited the opportunity to integrate specific security VAS in connectivity services for Mobile Operators who can benefit from next generation security in terms of maintaining customer trust, ensuring regulatory compliance, and delivering time and cost savings.

Sparkle partnered with Positive Technologies, who have pioneered research into telecom security. They were the first to discover the security issues associated with SS7 back in 2014, showing how such flaws could be exploited for everything from remotely intercepting phone calls to bypassing two-factor authentication (2FA) for access to social media profiles. Positive Technologies continues to lead research and development in the field, with papers dedicated to network security for Smart City technology, as well as development of a dedicated 4G and 5G assessment service.

Sparkle launched the Signalling Protection Suite; by combining Sparkle's innovative connectivity and roaming services, with Positive Technologies' next-generation intrusion detection system for Telecom operators, it protects operators against revenue loss, enabling them to concentrate on their core business, and provide their customers with a fully secure service. On top of that, professional services as Vulnerability assessments can be performed. Sparkle's embedded Signalling Firewall, for both SS7 & Diameter, completes the picture with a state-of-the-art platform that enables blocking of suspicious traffic. This way an operator can establish a proper security lifecycle iteration process.

A story

Signalling protocol SS7 saw its birth around the seventies, when we could still speak of a closed trusted ecosystem of limited parties. At that time security was not

an issue at all. Things started to change with the rise of the multiple interconnections between operators, with the objective of guaranteeing roaming functionality to its end-users. By 2000 also the CAMEL protocol came in sight (mostly for handling prepaid roaming), and some later IP-related SIGTRAN as well, which is used to encapsulate SS7 over IPX access ports. And not only mobile operators are mutually connected, but also e.g. VAS providers or aggregators in the messaging business.

Diameter, the Signalling protocol for 4G mobile networks (LTE), was developed as an evolution of the authentication protocol RADIUS. This is not the ideal way of handling mobility either, given that RADIUS bears its origin in fixed telco networks. The upshot is that Diameter can be even more vulnerable than SS7. And let's not forget that Diameter signalling messages are often converted to SS7 in order to enable interworking between different networks standards.

Hackers

So what can hackers do? First of all, it is easy to find numerous manuals on the darkweb, where they observe sets of instructions on how to perform attacks on, for instance, SS7 networks. Malefactors can point at stealing operators' data, tracking subscribers' locations, committing fraud, and executing denial of service attacks.

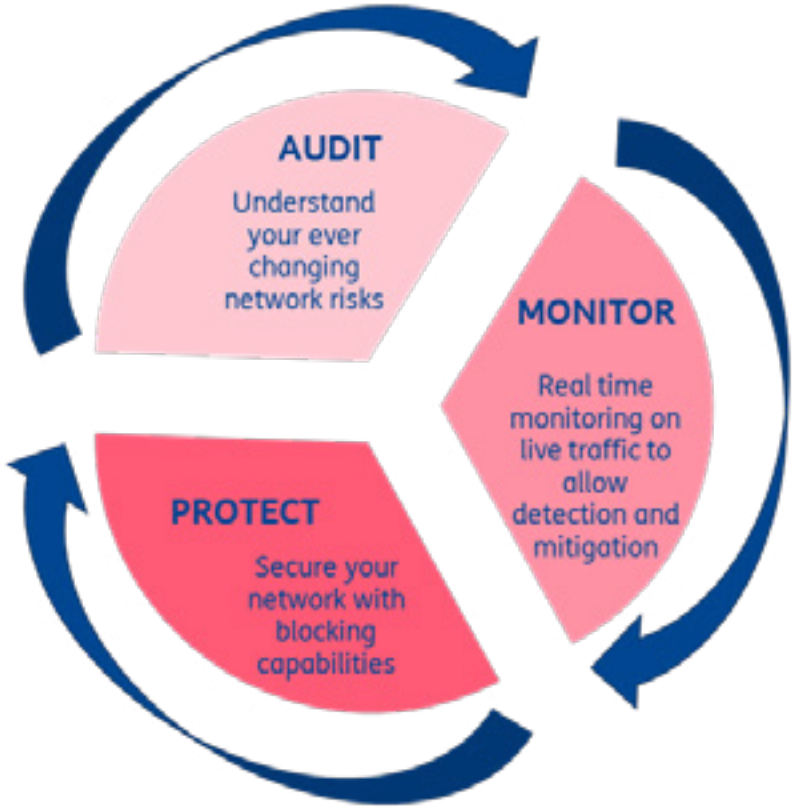
Needless to say that attacks have become more sophisticated over time, as the risk awareness of the industry is gradually increasing. Nonetheless, there are a number of recent cases where operators suffered the significant consequences of one or more attacks. An outage of only three hours which happened to a Norwegian network in 2017 caused serious financial loss.

And not only operators are at risk, but any company in the value chain of a service can be affected. Many banks are making use of two-factor authentication processes with One Time Passwords (OTP) by SMS. In Germany an operator that was struck by personal data theft for banking purposes saw a 7% decrease on the stock exchange market in just one day.

5G

And what about 5G networks? The market expects networks to become increasingly more secure over time. On the one hand, industry organs as the GSMA have put lots of attention on the operators over the last years, providing binding security requirements in some cases and non-binding guidelines in others. On the other hand though, the fact that 5G networks have a different nature than its 'elder brothers' will make other kind of challenges come around and, therefore, attention to network security will progressively increase once 5G networks will become more popular and capillary.

5G networks are all-IP, virtualized and software defined, and not the typical networks we were used to



in the past. They are merely forming a pure IT cloud infrastructure. The Signalling protocols that will be used in 5G networks (HTTPs/TLS based) are those commonly used in Internet technologies and web applications. Hence we are shifting from network security towards IT-cybersecurity, with new related threats.

IoT

With 5G networks the Internet of Things (IoT) will see its real take-up in the coming years. All kinds of devices will be connected to 5G networks, and often those devices will be part of an industry or an organization that is critical for a country. Devices that may even be residing in other networks, acting as (nearly) permanent roamers. Not human this time, but in a M2M (machine to machine) logic. Hence the increasing importance of taking care of security.

Generally speaking, preventing a network completely from intrusion will be hardly possible. You can easily define this as an illusion. It's all about (early) detection, and prompt mitigation afterwards through tuning and blocking suspicious traffic. Thus, detection of proper attacks in your network in real time is key. At the same time, regular vulnerability assessments are important to remain constantly aware of potential vulnerabilities. Operators should refrain from "only acting when it's too late".

During last years, Sparkle has been constantly increasing the focus on security aspects in its platform and offer. For more information on the Signalling Protection Suite for mobile connectivity, please visit https://www.tisparkle.com/our-platform/mobile-platform/sparkle-signalling-protection-suite#catalogue

Biography:

Melvin de Jonge is senior product manager in the Marketing division, dealing with the development and go-to-market of wholesale services for Mobile Operators worldwide, that vary from pure connectivity to disruptive solutions as Big Data reporting tools and security/protection services.

Prior to joining Sparkle, he worked for TIM Group from 1998 to 2009 gaining a deep experience in mobile value added services for retail markets in Italy and abroad. He was appointed in several marketing roles as innovation specialist, product manager and customer base analyst.

He started his career as an ICT consultant at KPN in The Netherlands.

Melvin de Jonge holds an MSc in Econometrics & Operations Research from the University of Groningen (The Netherlands).

SPARKLE