The Deep Blue Sea of 5G

Craig Gibson, Vladimir Kropotov, Philippe Lin,
Rainer Vosseler, and Fyodor Yarochkin

TREND MICRO™ | research

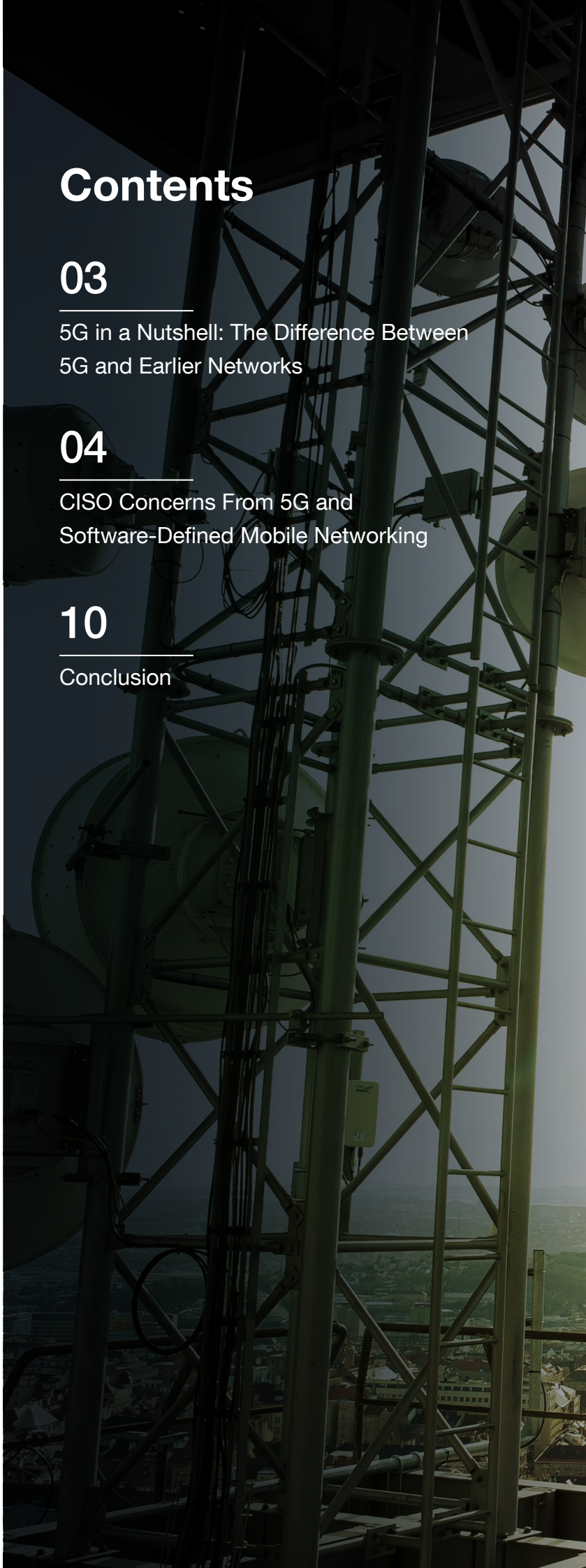
Published by:
Trend Micro Research

Written by:
Craig Gibson, Vladimir Kropotov, Philippe Lin, Rainer Vosseler, and Fyodor Yarochkin

Stock image used under license from Shutterstock.com

For Raimund Genes (1963-2017)

Contents



5G in a Nutshell: The Difference Between 5G and Earlier Networks

The management of a telecom carrier network is very expensive, and the network passes the added cost to the customer. As technology improves, the performance increases and the billing for the improvements increases. Unlike traditional hardware-defined networks (IT, 1G, 2G, 3G, 4G), the 5G network is software-defined, which means that it can be reprogrammed to suit customer requirements that change quickly and quite often. Unfortunately, this data volatility can affect security network statistics, and correcting this presents a complex identity and access management (IAM) and attribution problem, especially for ecosystems connected to the internet of things (IoT). This wasn't an issue prior to the emergence of the IoT because telecom companies had to deal with only one subscriber type: humans. The addition of thousands of additional subscriber types means that networks have to go from one complexity to multiple ones that interact.

For clever customers and enterprises, the cost of doing business is set to decrease substantially. For most customers, the speed and network scalability of 5G is not as important as the opportunity to get improved value at a reduced cost. The customer-specific experience that 5G "programmatic" networks offer allows 5G users to gain some of the power normally reserved for telecommunications carriers themselves.

A specific phone technology has never had such a central place — even world leaders recognize the competitive power of 5G in nation-state issues such as the loss of industrial and commercial competitive advantage.

CISO Concerns From 5G and Software-Defined Mobile Networking

Overview

The dynamic and volatile data-driven nature of 5G involves many fundamental changes. Many of these relate to identity and attribution, specifically after the introduction of a second subscriber type: the "machine subscriber," made up of IoT devices.

While security statistics were thoroughly designed to monitor only one known subscriber type (humans), IoT machine subscribers have hundreds of thousands of different subscriber types with their own network behaviors, most of which are new and unknown. What is acceptable for one kind of machine subscriber might be indications of botnet infection for a second similar IoT device using the same hardware; these two will look identical on carrier network logs, creating confusion.

Since the carrier is the most important part of a 5G network's data supply chain, the inability to profile a variety of IoT devices is a critical issue. Most carrier ISP-dependent security applications, threat models, security vendors, and machine learning rule sets cannot tell the difference, corrupting the behavior models they would be trying to apply. They cannot take a security action without affecting — causing denial of service on, or DOSing — the operational technology (OT). Without the ability to take definitive action, the affected business units will typically disable the noisy security function, effectively sabotaging their own network.

Decreased Detection Rates

The security platforms that a chief information security officer (CISO) and their staff rely on use very common, industrially accepted security rules typically obtained from third parties. These rules rely on industry-common filter statistics called "blacklisting," "signatures,""network behaviors," and the like. All rely on the "if it's on the list, don't let it perform X" concept.

These data-level access controls do not understand the subtleties of very legitimate — but very customized — traffic. This previously unknown customer software-defined network activity will look like a statistical anomaly: It will appear as a false positive, and become whitelisted as a business response. Whitelisted items are invisible to security processes, and when enough of these occur, the value of the security

platform will decrease to less than its cost, that is, decreasing return on investment (ROI). This will cause decreased output quality in many blacklist-enforcing hardware-based security platforms as they struggle to cope with an increasing body of whitelisted traffic and the volatile nature of software-defined networking (SDN) and 5G. The evolution from old hardware-defined networks to software-defined networks will create a perception of failure for the affected CISO as the performance of previously trusted security architectures decreases toward zero.

Business-oriented machine learning rules that handle security and privacy risks as a function of revenue and operating expense (opex) present one way of addressing this. This system is called a security orchestrator.

IoT Attribution

As we move toward 5G now (and later to 6G), all customers become subscribers with common traits, and a CISO is compelled to manage the risk of the subscriber base. IoT devices, or machine subscribers, have a variety of valid identities and behaviors, and network statistics may not be able to identify what is valid and what is not. A CISO will then have to prevent issues that could affect a machine subscriber base they have no familiarity with, and no means of acquiring that familiarity except through very painful experience.

5G machine learning (5GML) is the real-time use of machine learning rules to govern a live 5G production telecommunications carrier network and all its customers. Using 5GML to establish a baseline of acceptable network traffic presents a way to address this.

Enterprise Data Architecture as Security Architecture

When security is deployed without being first planned by an enterprise security architect, it is unnecessarily bureaucratic, significantly affects customers, and is expensive. It will also have unnecessary duplication of infrastructure and functions, and a proliferation of vendors that undermines capital expense (capex) reductions like bulk purchase discounts. The lack of enterprise security architecture leads to escalating complexity and management overhead. It also stifles innovation by adding obstacles to deployment timelines, costs, and approvals. When compounded, these inefficiencies require highly qualified and nimble bureaucrats to manage. The larger and older the company, the more it becomes difficult to manage.

Creating a mature enterprise architecture practice using a methodology such as The Open Group Architecture Framework (TOGAF) can address this.

Human Resourcing Bottleneck Toward Single Points of Failure

Human resourcing is another CISO-level issue. Most cybersecurity roles are difficult to fill given the millions of unfilled security jobs globally. The resourcing impact of this shift from hardware-defined networks to software-defined networks will amplify this issue.

The very rare advanced security professionals who can identify the pain points for the software-defined network (or application, or data) are usually the same subject matter experts for the enterprise's advanced incident response. A mature, motivated, well-funded organization may have one or two of these apex responders. One likely hired or trained the other directly, and most companies will have never met or even heard of them. They typically are not hired using traditional human resources practices. (They are so sought after that they tend to block or unfriend recruiters as spam.) The issue is that apex responders' skill set is the rare combination of the following:

- underground hacker contacts
- advanced technical skills
- law enforcement or intelligence contacts
- "hacker mindset" needed for analysis and incident response
- membership in at least five trust groups
- a reputation of being at the top of their field
- being highly paid and sought after with as much as 40-percent annual wage increases across the industry
- being approached for new employment opportunities weekly

They also typically have these characteristics:

- limited to the working week
- loyal until overworked
- intolerant of bureaucracy and office politics

The advanced criminal insight and technical knowledge of *how to block* these attacks are present in the same person *actually blocking them*. Here is a typical scenario in an organization: A new network is launched, it is attacked, the apex responder stops the attack, and the network's architects ask for the apex responder's help in designing the fix. If the apex responder helps fix the *last* attack, the apex responder is unlikely to be available to fix the *current* or *next* attack.

The most common approach involves unintentionally overworking the apex responder until the incident is over. Unfortunately, security incidents never end. If an approach overworks or burns out the apex responder, the CISO is then in for an even bigger surprise: Apex responders can be hired only by other apex responders, as they are so rare that only their peers can find or hire them. If the previous apex responder left because of too much workload, the next one (who personally knows the last one) will be unlikely to accept a job offer.

Using a 5GML security orchestrator can address this. The 5GML security orchestrator will "learn" from the apex responders to commoditize their skills, reducing dependence on these rare specialists.

New Skills Needed by Security Staff

A software-defined network is a collection of software applications sitting on generic computer hardware. As software, it is managed at the data level (data plane). Most security practitioners have never worked directly with operational technology data plane production data before. They may have used specific applications and existing reports for the detection and prevention of security events, but this is not "raw." The traffic of a software-defined network is likely invisible to pre-SDN era appliances and applications.

Security staff will suddenly need to add software coding skills to their other skills (like fraud investigation or network security strategy) to interpret this data, since other products and appliances are unavailable due to the obsolescence of their statistics that support attack identification and attribution. Many organizations may lack the apex responders necessary to teach other staff members, leaving the staff to "train the trainer" from scratch (see section on human resourcing above).

Many organizations that rely on software developers for their product development needs may find that this transition requires "reskilling" developers into data scientists.

Using Data Metamodeling to Create an Inventory of Data Assets

The development supporting automated 5GML security business logic (security orchestration) requires the organization to know, at the levels of both detailed business and detailed application logic, how it makes money.

At the enterprise architecture level, most organizations do not know this and handle the gap by involving human business analysts. To perform the level of automation needed for full automation and scalability of 5G, the many separate models must be linked to become one. The level of automation needed disallows reliance on human business analysts.

Without this common inventory of data, the enterprise will have no way to tell when an inventory "item" of data has been stolen, moved, or replaced. Since all but the largest and most mature organizations do not have enterprise data security architecture functions performed by a mature enterprise architecture office, most organizations will see a negative impact on their project's critical path project launch timeline, causing them to lag behind their competitors in time-to-market.

Alternatively (but not ideally), they may go to market without this inventory, and have no way to know if their operational revenue-generating datasets have been modified by criminals or competitors.

Supply Chain as Data Provenance

In a software-defined network, all service providers are part of the supply chain. The organization (and its customers) inherits the vulnerability and risk of all the elements above it. Legal requirements such as contracted data privacy clauses and the European Union's General Data Protection Regulation (GDPR) enforce a regime of fines, ensuring that entities push their privacy and data security requirements back through the supply chain.

The volatile nature of 5G and SDN makes it difficult to ensure that all the dynamically allocated links in the service chain satisfy supply chain requirements.

One way to ensure this is by including privacy as a data security feature of the SDN security orchestrator, and auditing these privacy features at the time of service chain design (in the SDN's design studio). This makes sure that supply chain issues such as privacy can be built in. CISOs can opt for this capability, using their procurement (buying) power to alter the market to match their appetite for risk.

Similarly, other standards, audit requirements, and detailed controls can be added to the upstream software defined network to reduce risk as well as minimize legal and audit impact.

Products as Datasets and Intelligence Subscriptions

CISOs are also required to reduce both cost and risk. One source of risk is "vendor sprawl." In this expensive situation, vendor sprawl becomes a persistent and escalating interoperability problem that introduces further risks because of increasing complexity and vendor lock-in. One approach to resolving this is to remove all vendors through abstraction. The effect of this enterprise architecture technique is to take the common denominator of vendors (intelligence and insights) and ingest these directly into the 5GML network.

Choosing vendors that provide their services as 5GML-visible data feeds makes the entire network both scalable and interoperable. In addition, the value of separate feeds can be easily reported, and the value of various feeds can be directly seen down to the ROI level.

This replaces "by-download licensing" with ongoing subscription licensing models based on traffic volume analyzed. Hardware appliance-based licensing becomes obsolete, since it introduces the inefficiencies that 5G SDN was designed to prevent.

Hyper-Accurate, High-Integrity Security Telemetry for 5GML

What was once a hardware appliance containing proprietary apps with proprietary intelligence will then become virtualized repeatedly into a simple intelligence feed. The resulting intelligence feed can come from the same place the vendor got it from (if available) or another more credible source. Procurement can become very simple when this is performed across multiple supply chains.

CISO Opportunity – Simulations and Vendor Value Comparisons

At the beginning of a transition period from a hardware-defined state to a software-defined state, there will be opportunities that can be identified to reduce costs and increase risk management efficiency. In a software-defined network, there will be different vendors with service offerings that overlap. Through the use of the data architecture work described above, the empirical ROI of each can be assessed against one another with or without their knowledge. This comparison will then be used to determine the short list of highest-value competitors providing a given security feature.

This process can be done with all the competing vendor services already in the network. It can also be used to simulate the effect of launching a proposed new service, and to create new "optimized" proposals that may not include vendors at all (and may remove the need for existing vendors). These optimized proposals may then rely on internally generated reports rather than vendor products.

Conclusion

Moving to a dynamic and scalable data network leaves the inefficiency and complexity of previous generations behind. This is both promising and challenging, as it requires staff to have a level of competence they have not previously needed. Many 5G-era companies rely on Ph.D.-level staff led by senior Ph.D.-level staff to operate in this powerful, high-leverage environment. When every model is a data model, the reliance on networking staff decreases and the reliance on data scientists and mathematicians increases.

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

TREND MICRO™ research