Deep Science Publishing
https://doi.org/10.70593/978-93-49307-75-9_7

DeepScience
Open Access Books

Chapter 7: Addressing evolving cybersecurity threats within virtualized and software-defined telecom infrastructures

7.1. Introduction

Many of the traditional approaches to security in telecommunications networks assume that the network is 'confined' within certain boundaries, and measures like defining the perimeter of security defenses, privileging certain traffic types, and adding extra layers of security—like deep packet inspection, traffic anomaly analysis, and sophisticated intrusion prevention systems—have been developed to deal with external threats. However, in a virtualized and software-defined infrastructure, these traditional approaches become less effective, as these measures have been designed to operate at the macro level of communication, while a large amount of security risks involve threats arising from resource sharing at the hardware level. In such a context, various resources, which traditionally operate as physically separated and truly secure, are instead replaced by software that operates over standard hardware based on standard protocols. This increases the risk of various types of snooping, data leaks, identity masquerades, information tampering, and denial-of-service attacks.

This paper, which focuses on how a virtualized and software-defined infrastructure can be attacked and the consequences of these attacks for critical communications pointing to the lack of a significant security approach for facing this scenario, shows that many of the threats come from the limited use of cryptographic security mechanisms. The full deployment of built-in security, which can be made much more manageable and less expensive than the sheer volume of attempts—through the integration of carrier-grade

encryption and grouping services and inter-service isolation, traffic separation, and centralized control based on the specific management plane, which should include not only capabilities to manage security elements but also policies and processes specific to security.

7.1.1. Overview of the Report's Focus and Purpose

This report begins with a brief overview of the advances that have been made in network architectures to allow greater automation and facilitate cost-effective benefits from cloud data centers. Smarter, software-definable, and more responsive telecom infrastructures are not only integral to the 5G vision but are also key to sustaining market innovation and competition. However, these changes expose telecom networks to a wider array of cybersecurity threats and incident damage. The benefits they offer are real, and exploiting virtualization capabilities promises a return to the historical reduction in operational costs proportional to capital costs to fuel the 5G innovation cycles. This suggests that network services cannot and should not be limited to the traditional ecosystem but instead be created from shared resources in a decentralized way, with cloud-enabled services able to access many complementary assets held in many different kinds of entities.

Yet, SDN and NFV architectures are still surprisingly immature. Evolving towards these ever more dynamic configurations will require changes to the traditional way in which network services are secured. Resellers and new entrants will need access to an appropriate level of cyber resilience, allowing the creation, management, and responsive protection of services at vastly shorter timescales. Requirements for network immunity from infection will extend to an increasing proportion of devices that have hitherto enjoyed the 'security by obscurity' bonanza. At the same time, the cost of maintaining 'infection-free' status is unlikely to be feasible on all device types, and even the newest types are likely to have lifecycle security models that depreciate over periods less than the decade timescales expected for 5G networks. The threats to which such networks must remain immune are also rapidly evolving, with ever more sophisticated attackers leveraging widespread understanding of devices and vulnerabilities in future deployments.

7.2. Understanding Cybersecurity in Telecom

Although some aspects of cybersecurity are unique to telecommunications—the uncertainty between the intention of a packet and actions in the physical layer, the high

importance of confidentiality, authentication, authorization, availability, and integrity, the scarcity of information about the physical and logical structure of multi-layer networks, the existence of a myriad of legacy systems, and the increased importance of attacks triggering national security concerns—most of the security issues affecting telecommunications are due to the implementation of security policies, which are usually common to those of other verticals. Such policies involve the hardening of telecom network functions and resources, regular network audits, creating and maintaining a security perimeter, data encryption, both in transit and at rest, and monitoring the traffic with specific security tools, among other measures (Lal et al., 2017; Conti et al., 2018; Gonçalves et al., 2021). The intense adoption of NFV and SDN brings new challenges to telecommunications in terms of security. Some issues are related to the loss of control of the physical layer, which makes some attacks more feasible. Because cybersecurity in most of the current NFV and SDN implementations is an application of traditional IT security technologies for telecom network functions and resources, all the detailed security measures traditionally adopted in telecommunications are still valid. In NFV environments, however, security efforts should be increased at the virtualization and orchestration platforms of network home servers and the management orchestration platform for NFV. Moreover, operators may require that VNFs are overprovisioned by the VNFM, imposing load balancing choices that affect security based on the overutilization levels, which in practice favors some categories of customers with particularly low service level agreements.

7.2.1. Historical Context of Cybersecurity

The requirement for cybersecurity is deeply rooted in the design of telecommunication infrastructure. As far back as the early years of the telegraph, communications were encrypted, and secure procedures were essential. When telephones were first run over copper wire, interconnections between operators were manual and physical, creating inherently physical security. Increases in interconnection led to electronic switching, and new security mechanisms were developed, enabled by cryptography. Early work on computer-based data traffic networks included enciphering methods, known at the time as unclassified protections, followed by early use of bifactor systems for data privacy. Such work laid the foundation for modern cybersecurity concerns. From the start, the design of computer communications networks took as a fundamental assumption the need to protect the exchanged information from those who were not entitled to it. In telecommunication infrastructure design, while the use of classic firewalls is justified and efficient for providing basic system protection in most cases today, the level of security provided by the telecommunication infrastructure directly affects how an adversary might use it to attempt exploitation. From the early days of encrypted

communications, what has changed is the landscape of actual and potential adversaries and the specific threats and technologies that are associated with those adversaries. The history of cybersecurity in telecommunications is a continuing story of maintaining security over a changing problem scope as these adversaries acquire new means of attack.

Fig 7 . 1 : Counterattacking Cyber Threats

Attack types and motives have evolved through several generations, each associated with the use of a new technology and the establishment of a new economic model for its use (Scott-Hayward et al., 2016; Sharma et al., 2018). Each defense was a reaction to the existing or predictable capabilities of adversaries that made the new technology exploitable. For example, many telecommunication networks have had strict admittance control since their inception to protect against adversaries from the general public. The broad use of crypto—the defense approach to keep adversaries from abusing the new transmission technology—represents in each case major changes in the basic economic and business models of communications, not technology advancement and expense. The steady cost and performance advantages of digital computers and digital communications technology have led to cyber-subversion, which is the economic driver for the development, protection, deployment, and use of crypto. Also apparent is that preventive crypto is far less expensive than many of the increasingly widespread and expensive post-facto response options available—in loss of finance, reputation, opportunity, and critical infrastructure. The relationship between crypto and the post-

facto effects of failure is a balance of losses and gains, rights and privileges, in which placing blame can distract from the search for technical or administrative solutions.

7.2.2. Current Threat Landscape

The development of infrastructures based on virtualized network functions (VNFs) has led to an expansion of the threats that have always accompanied the use of previous infrastructures, such as hyper-converged infrastructure and the most recent concepts of cloud computing, with infrastructures based on virtual machines (VMs), containers, storage management, and control units like orchestration and management systems. It has also led to the creation of new ways of exploiting the vulnerabilities typically associated with such infrastructures. The evolution of the different types of attacks goes in parallel with the development of the characteristics related to the VNFs and the possibilities of usage concerning the installation and interconnection of the same with each other. It should be noted that we are only referring to the main threats and not to all possible threats. This is because it is difficult to try to make a classification from the beginning given the continuously evolving situation. Furthermore, the classification could change depending on the sector in which the virtualized infrastructures are used, such as telecommunications, industrial, and consumer, and on the scale of the use to which they are placed.

This being a particular type of infrastructural technology, the characteristics of the attacks mainly concern the manipulation of the hypervisor, the exploitation of connection vulnerabilities, the use of VNF unsecured installation and operations, and the unauthorized interaction between the various VNFs. The back-and-forth communication that takes place in a virtualized infrastructure is more vulnerable than what could normally happen in infrastructures not based on virtualization. Any service or application is routed through the hypervisor, which receives packets from one client, then processes those packets and forwards them, since the guest operating system is not involved in the packet movement. Furthermore, in the most recent virtualized application infrastructures, considering for example the applications that exploit live migration, the packets do not remain in the logical path (which has the function of managing the flow of packets to pass). This means that the controller is not aware of the packets, which could lead to additional security complications. The identity of an attacker can be verified through an IP address, which is the identifier used by other telecommunication infrastructures. However, in the virtualized infrastructure, the IP address would link the traffic to the computer rather than to the client machine. Furthermore, in a virtualized

infrastructure in a data center environment, the majority of the critical services are not isolated inside an end-to-end network that is entirely managed by the same service provider. However, critical services can be implemented by a separate organization from the one that normally manages the data center. The threat of service clouds is therefore comparatively more interchangeable with traditional communication threats both due to the presence of professional carriers that provide security services and because the enterprise does not expect the cloud service provider to operate the services of the contracting enterprise together with the services of others. This aspect differs fundamentally from the mechanisms put in place for the besieged WAN.

The threat landscape for virtualized infrastructures refers to the following activities or operations:

"A" Attack to hypervisor/SDN operation.

"B" Hypervisor discovery mechanism vulnerability.

"C" Malware execution on host OS.

"D" Unauthorized interactions between VNFs.

"E" Flow misdirection.

"F" HLI leakage.

"G" Grouping concept threats.

"H" SSDC attacks.

"I" Network procurement threats.

7.3. Virtualization in Telecom

Telecommunication infrastructures are currently undergoing a radical shift in the form of cloud-based architectures. Cloud-based racks are controlled by virtualized networked technologies and have both access/edge as well as deep brain applications. This convergence of both applications and services in virtual infrastructures and the use of cloud-computing technologies push Telco traffic kilometers from the core to the edge of the core network to provide the connectivity needed for user applications. These trends imply that two infrastructures will be built to accommodate the very different requirements and workloads associated with Telco, edge, and cloud technologies. Telco-specific virtualized infrastructure differs from enterprise servers and services-based virtualized technologies and has security, workload, performance, and mobility issues as well as limited server-to-server communications and a high throughput requirement for user VPN aggregation between applications.

Secure SDN approaches are evolving that associate SDN, NFV, and storage resources and can enforce specific network arrangements that represent services and transport across infrastructure. Secure SDN, NFV, and storage infrastructure help reconstruct all the possible behaviors of cloud computing and fix security performance problems related to both speed and volume of control flow changes and malware. This will be achieved with SDN controllers being aligned to fiber orchestration controllers, underlay or overlay SDN functionalities, key chains and counters for DNS, and a secure control loop and micro-segmentation, and assistance in maintaining virtual optical bypasses for sensitive processing while improving security, monitoring, ops support systems, orchestration, system operations, service management, cost, and energy savings. Firewall interventions—established by secure in-band routing concepts that are automatically created and removed on demand—based on unique login IDs—cannot adapt to today's complex networking service demands and are challenged by incessantly occurring network, service, and application changes away from endpoint-based protection with proximate, online, highly efficient, and real-time communication between telemetry data, security compliance, and SDN-based model-driven policy updates.

7.3.1. Overview of Virtualized Infrastructures

To be specific about particular security concerns, it is important to define the virtualized infrastructures on which those services are now running. Virtualized infrastructure is the term used to describe the network and cloud infrastructures (together with the management and orchestration functions) that are being used to deliver Network Functions Virtualization and Software-Defined Networking to network operators. That is, it is the environments in which virtualized networking appliances are running. The scenarios in which generic Information Technology appliances (such as web servers), rather than specific virtualized network appliances, are being used, are also considered in this area.

Telecom operators have historically created complex infrastructures based on custom appliances and commonly involving proprietary hardware, applications, and tightly coupled orchestration and Management and Orchestration. The network functions that the service providers deliver are specialized in the sense that they can implement the detailed Quality of Experience requirements for media transport – sensitive to delay, jitter, and bandwidth. The introduction of virtualized infrastructures brings opportunities in terms of flexibility and reduced complexity but also creates additional threats, substantially elevated in many cases by the particular service provider requirements. In particular, the pervasive use of large numbers of virtual machines to create the Network Functions Virtualization infrastructure, along with the use of general-purpose computing

platforms to deliver the virtualized infrastructure, creates increased vulnerabilities against which more effective mechanisms must be applied.

7.3.2. Benefits and Challenges of Virtualization

Virtual network functions (VNFs) offer numerous benefits, including cost reduction, flexibility gain, and rapid VNF deployment, migration, and scaling. Specifically, cost reductions occur through the sharing of hardware resources in modern high-performance servers, promotion of server hardware competition resulting from open VNF interfaces, quality of experience improvements from the sharing of high-speed hardware such as GPUs, and capital expense benefits from software licenses relative to dedicated hardware. VNF deployment, migration, and scaling flexibility come from inter-VN communication that enables direct VNF communication and configuration capabilities that enable VNF specialization, network access, and hardware use optimization. These benefits allow service providers and network operators to reduce VNF activation times and the costs of accelerating network infrastructure responses to advances, needs, external threats, and cyberattacks. Cost-effective VNFs are capable of cost-effective network accelerations infrastructure optimizations and data-sharing paradigm shifts that use impact analysis to quickly assess emerging cyber threats and vulnerabilities.

Telecom networks consist of issues similar to data center networks, including many security problems associated with generic hypervisors, rendezvous virtual machines and containers, and operating systems. However, the VNFs deployed on telecom networks are subject to distinct telecom performance and data integrity constraints, often requiring more stringent performance and quality of service guarantees in new 5G virtual radio access networks and ubiquitous 4G/5G coverage radio networks. VNFs located closer to the edges of these networks face greater performance degradation due to backhaul bandwidth constraints, RF path diversity and redundancy constraints, and time-critical revisited constraints. Furthermore, because many telecom services are customer-facing, the telecom network must continue to provide the requested bandwidth, despite attacks that can affect the performance, availability, and integrity of the infrastructure network. These slow recovery advantages are noteworthy for virtualized telecom networks after denial of service arrests instead of architectural flexibility.

7.4. Software-Defined Networking (SDN)

Software-defined Networking (SDN) architecture is designed to address the network administration and traffic delivery challenges facing modern network operators. It

allows network operators the ability to control network traffic from a centralized server. By doing so, SDN abstracts the networking infrastructure from design, operation, and business models. SDN promotes the simplification of network nodes' forwarding rules, with a central controller taking forwarding decisions based on its global network monitoring view. This leads to improved network performance and enhanced security services. SDN deployment is largely based on the Software Defined Networking Controller. SDN is already widely adopted in different sectors of commercial networking as well as in key research fields. The benefits of adopting SDN principles in these environments encouraged telecom architectures to adapt to the same approach with the implementation of small cells and Virtual Base Band Units.

Despite this clear trend towards SDN integration, there is no clear agreement on what the architecture of an SDN controller should look like to effectively support the future needs of operators. On the one hand, we can today find a minutia of small business or research SDN controllers, some of which are open source, whereas others are closed. Although selecting a tool from the shelf and customizing it to a particular requirement is appealing, this approach often results in the controller being unsuitable for more complex scenarios or unable to bleed the full benefit from the particular system conditions. On the other hand, we find most large telecom vendors developing their own SDN controllers or at least amending the open source offerings to try and best leverage their technological capabilities. These controllers are enterprise-class or professionally engineered. This approach requires a significant amount of financial overhead that may not be rational to engage in, considering that several vendors share very similar requirements.

7.4.1. Principles of SDN

Context and History. SDN decouples the network control layer from the forwarding layer and provides a central point of control for the network. The programmable network components delegate the low-level details of the packet terminal to the network through an abstraction of the network state and allow a network operator to control network flow. The SDN architecture does not depend on the internal technology used by the network, such as optical circuits, wireless links, or Internet Protocols. NFV success and the need to maintain and manage their state created a need for the networks to be more flexible, automated, and transparent than traditional networks to achieve NFV success and reduce operation, maintenance, and deployment expenses and time. This shift occurred concurrently with the development and maturity of SDNs, making them ideal and complementary responses to the network requirements. SDN is used as a control interface between the network and the infrastructure, and together they are managed to

provide a flexible and dynamically configurable communication infrastructure that is transparent to the different autonomous systems and their hierarchical differences. SDN is based on three practical principles: logically centralized control, network programmability, and abstraction of the network resource.

While network application innovation can be accelerated using self-modifying on-demand control programs developed and hosted on logically centralized control computers, costly and complex network equipment can be simplified in terms of functions for forwarding. An increase in equipment and maintenance risks is also expected. The networks, however, abstract the equipment into a simpler and more manageable form, making them seem less complex for network clients. These principles are made possible because of the following: separation of control and data planes, data planes as simple forwarding engines, and centralized control. Internet services and deployments are collected on a set of physical cables, routers, switches, load balancers, WAN optimizers, firewalls, and the like. They extend their reach using VPNs, VPLS, VLAN, VxLANs, and MPLS and participate in routing, load balancing, decision information, and look changing. They face challenges to keep up with the requirements that come from different sources, which have scopes, reach, and business logic that evolve. They are difficult to adapt and reconfigure due to the scarcity of robust network operators and a lack of programmability and accounting for the equipment and services from which they are made.

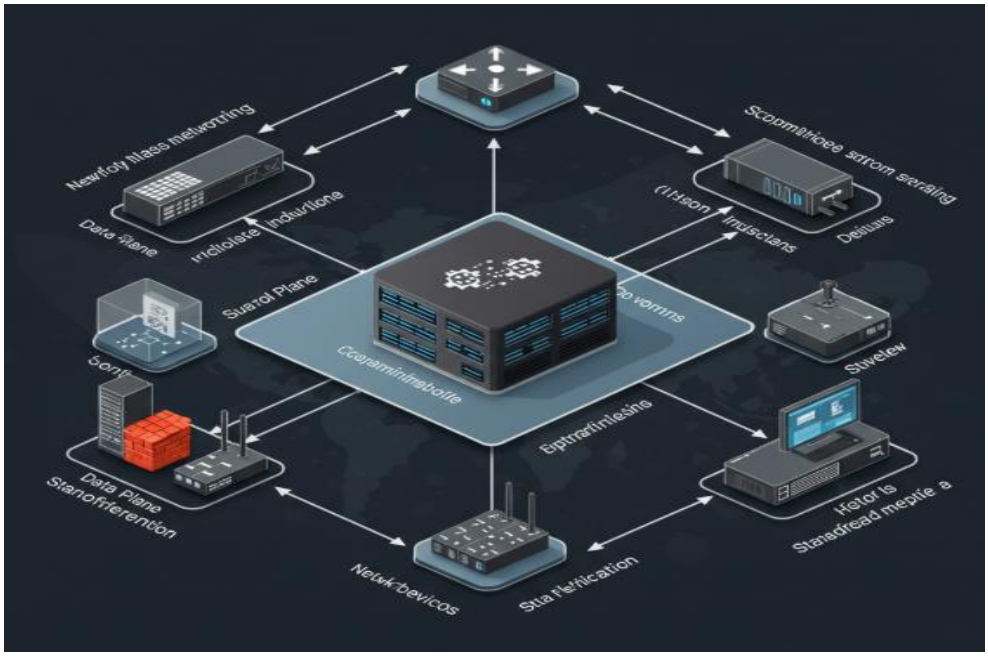

Fig 7 . 2 : Software Defined Networking (SDN)

7.4.2. SDN Security Implications

Software-defined networking (SDN) shifts the intelligence in the network from distributed routing and switching elements like routers or switches to a logically centralized control point, while the complexity of the network control and policy provisioning is abstracted from the underlying network. As with many other technologies, SDN has disintegrated the logical components, including data and control planes, from networking devices such as routers and switches. For instance, SDN-compliant switches are merely data plane units that execute commands received from the software controller. Similarly, virtualized network control brings forth the capability to centralize network security policy enforcement. The underlying network switches are relegated to simplistic hardware serving only as the data plane, which the controllers configure. Although SDN architecture does not necessarily hinder cybersecurity, this composability shift certainly adds more security concerns to programmable networking technologies than traditional networks.

The implications of SDN on cybersecurity are, however, two-sided because SDN can offer enhanced capabilities for securing and managing a network. An SDN controller maintains a detailed overview of the entire network fabric. This centralized knowledge is paramount when detecting or handling network security threats. Centralized management of security configurations and policies renders networks more resilient against human error. Most important tasks can be efficiently outsourced to a single security appliance such as deep packet inspection engines or firewalls deployed with improved capabilities. Such an approach offers a cost-effective alternative to currently widely deployed hierarchical network security architectures. However, in return, the single point of failure of the software control plane has the potential to be an even bigger target for attackers. If the control plane malfunctions, the forwarding state is lost, and all packets are dropped.

7.5. Cybersecurity Threats in Virtualized Environments

The merging of telecommunications and virtualized network services architecture through the adoption of virtualized and software-driven network protocols, traffic exchange and routing protocols, management functions, and applications leads to potential openings to new types of cyberattacks. Telecom services depend on the integrity and security of management and applications, as well as the security of routing their traffic, and those requirements are slowly spreading to core and edge services. The malicious aspect of running the virtual network functions in a cloud environment, with shared resources and access to the underlying hardware, is called the VNF poisoning

concept. The concept of using the orchestration function to find critical paths of the VNFs running on the same physical infrastructure, to disrupt the underlying cloud environment, is also present.

The use of the cloud environment for the virtualized infrastructure causes additional aspects to the threats on the virtualized environment due to network separation functions and their policies. The virtual network functions can access online sources that deploy DNS functions, decrease the TTL for the DNS queries, create online resources, exfiltrate traffic through the web proxy resources, or send specific instructions. DNS access can be used for information redirection and decrementing of queries. The virtualized environment traffic separation concerns can be mitigated by applying countermeasure functions and segregation on traffic sources.

7.5.1. Common Vulnerabilities

Some of the vulnerabilities in the VNFs are due to the static hard-coded points in the source code. When errors or new bugs are found post-release, patches are not often issued, and fixing these hard-coded points presents additional challenges when done manually. Some technologies, like containers and VMs with an ARM64 architecture, make the exploitation effort more involved, but the level of effort required is not adequate to support the business-critical functions in the telecommunications industry. If hackers gain control of these virtual network functions (VNFs), they will be able to steer traffic and pilfer sensitive data or provision cloud resources to direct the digital exhaust from the malicious server into the billing system to inject fraudulent data. Device configuration management is a less tracked issue in today's networks. Control planes of network devices, such as various orchestrators or orchestration managers, are state-heavy in their behavior and their data modeling, while southbound protocols between management and control planes of mobile and fixed-line networks, as well as transport and data center networks, are vulnerable to certain types of traffic steering attacks. Control plane protocols and southbound protocols can deliver performance but do not provide adequate security against the active adversary.

NFVI security combines security principles and processes in trusted network data centers dedicated to telecommunications and new open-source platforms introduced or managed using various development technologies. This includes the general-purpose cloud infrastructure resources of computing, storage, and network. Different control mechanisms are used in these subsystems, each with a different impact on end-to-end service security. From a cloud perspective, the introduction of the control plane introduces a fine-grained access control challenge. The ability to manage the security

posture of each VM from a common cloud platform complicates the existing cloud security model. Accidentally misconfigured VMs lead to denial of service. When misconfigured data networks are introduced, availability attacks prevent control exchange, preventing genuine endpoint-based data reporting actions by both the mobile and fixed-line elements.

7.5.2. Case Studies of Attacks

Two different types of attacks showed interesting evolutions in the mobile network domain due to virtualized and software-defined characteristics. The first case study treats a significant class of multi-cascading attacks targeting both core and RAN in classical LTE networks. Some specific attack patterns were observed in a more recent virtualized LTE setting. Machine learning-based detection can be deployed in the MDV-GW for the newly identified attacks. Detecting DoS attacks by monitoring the number of failed registration attempts is useful in protecting virtualized telecom infrastructures. A more scalable and generalized defense mechanism by learning from algorithm attack patterns is an interesting research direction.

Protocol downgrade attacks lead to security vulnerabilities in software-defined systems. Network management interfaces should implement the message format upgrading functions. Protocol downgrade attacks on architectural control interfaces can greatly weaken software-defined networks. The inter-component communication in SDN monitoring can be used to detect attacks, reduce the introduced overhead by adopting an ML-based detector, and gradually migrate to a protection algorithm with high accuracy. The relatively small volume of blackhole attack detection training data for ML detectors can be solved by semi-supervised learning algorithms. Software-defined mobile backhaul networks that perform both signaling and user data plane flow management can also be used in other types of networks.

7.6. Threat Mitigation Strategies

This section analyzes and proposes mitigation strategies to combat the threats that we discussed in earlier sections. In this context, we use the term mitigation to refer to any listed defense mechanisms such as detection, identification, recovery, and prevention among others at various scopes, namely network, virtualized infrastructure, and network services. The mitigation strategies are developed while considering the overall trust computing models that we proposed at a network level as well as the specific trust computing models for a NUV, SDN controller, and an SD-WAN service. The proposed

trust models are used to identify the hiding and the trickle effects in networking for the network and the VNFs corresponding to an SD-WAN overlay service and provide the required security complement for managing the network virtualizations of an SDN-enabled environment. These root cause trust vulnerabilities exposed through the proposed trust models would be difficult to identify or may have different manifestations in traditional control systems.

The mitigation strategies will mainly identify solutions to the causes of the root trust vulnerabilities and can be used to design trustworthy telecom infrastructures. With the proposed trust models, we aim to develop solutions that apply at a service provider level due to the trust vulnerabilities unique to these entities. We adapt the proposed solutions at a high level to address the same vulnerabilities at the enterprise level. We focus on the SD-WAN solution, and some of the mitigation strategies may require detailed tailoring for corresponding network and overlay service designs used as specific business implementations. For every case considered, the proposed solutions do not require hardware modifications, even with the use of advanced security capabilities that are available with many popular hardware options. In particular, our solutions are deployable in conventional data centers, and the proposed mitigation strategies remain applicable when emerging programmable switches go beyond the scope of verification and off-the-shelf data routing, utilizing standalone guidance on when and how to propose these into commercial designs. We provide the rationale and the utility of the mitigation strategies.

7.6.1. Best Practices for Security

Selecting wisely and adhering to "best practices" in designing, coding, testing, and deploying telecom applications is the lowest "cost of security." Formal software development quality assurance, such as covering most capabilities with automated tests, using peer reviews, and preventing basic vulnerabilities such as defective access control and lack of boundary protection, enables standard, overt, plaintext protocols to be used for communications between building blocks.

Encryption is critical to protect confidential information or when building elements cross untrusted parts of the infrastructure. For wireless signals and coordinated timing signals in mobile networks, the "in-band" nature of encryption could be a significant burden to both performance and security efficiency. If an attacker can cause reliability problems, it can amplify and magnify those attacks. Confidential information must be kept secret not just from adversaries external to the infrastructure, but also from the malfunctioning parts of the infrastructure. Consequently, end-to-end encryption is often advisable,

particularly for control information. Standard encryption, using a mix of symmetric and asymmetric encryption, should be used for in-band end-to-end protection. Since the control signals used for communications between elements are cleartext, and describing or monitoring encrypted signals onsite may be illegal, the intrinsic, overt cyberattack vulnerability cannot be mitigated through encryption unless it is "out-of-band."

7.6.2. Technological Solutions

At a high level, security solutions that were recently deemed effective in securing physical infrastructure can be applied to secure the VNFs within VST. However, these solutions may need to be adapted to secure VST of CNF-X and CNF-Y. In addition, some of these solutions are not well-suited for protecting virtualized workloads as they lack a distributed security mechanism and may pose performance overheads due to certain devices. In what follows, we discuss several high-level security solutions that can be used to secure VNFs within VST, then focus on state-of-the-art approaches that can be used to secure CNF-X and CNF-Y. Finally, we provide a discussion of CNF security from a performance perspective.

One of the simplifying assumptions that were made at the beginning of overseeing the VST security discussion is that the security within the VST involves the security of the CNF-X and CNF-Y. As outlined in the previous major section, plugins can be used to secure CNFs. Building on security implementations within CNFs is particularly interesting in the context of technologies like virtual tapping, where security implementations within tapping instances can be used to increase the overall security of VST.

7.7. Regulatory and Compliance Considerations

To clearly understand the frameworks established by various regulatory entities concerning cybersecurity, especially as they might pertain to ICT, including telecommunication network infrastructures, it is important to first understand these frameworks. Consequently, the goal of this section is to provide an overview of the established regulatory frameworks for risk management, privacy, data protection, and cybersecurity used by organizations globally to address the governance of ICT and security matters, including compliance aspects and government law enforcement procedures. In short, this material is relevant to all telecommunications carriers. Its purpose is to create a high-level, easy-to-read review of the most important telecommunications-related aspects of the regulations.

Regulations around the world, and especially in the United States, require public companies to file specific documents regularly. Congress created the federal securities laws and the regulatory agencies that enforce them. The following is a high-level view of the regulatory environment under which telecommunications carriers operate in the United States. The Securities and Exchange Commission requires U.S. publicly traded companies to adhere to a set of rules that help ensure that investors can depend on the accuracy of the information disseminated by the companies. Each year, the telecommunications carriers publish comprehensive reports and also make available an overview.

a) The Federal Communications Commission processes different types of forms with the U.S. Office of Management and Budget. The two forms that are specific to telecommunications carriers are Form 477 and Form 477-D. The impetus behind the Telecommunications Act of 1996 was to open any telecommunications market to competition. The Act addressed economic regulatory issues such as price and market entry control, industry structure, and choice of service delivery technology. The 1996 Act also expanded the FCC's responsibility for universal service. The funds are distributed through a system of regulated inter-company payments. In the United States, both regulators and industry have roles to play in ensuring the reliability of the telecommunication network. The telecommunications carrier is responsible for maintaining the network, and the regulatory entity is responsible for assuring itself of the carrier's compliance with its network maintenance responsibility. The FCC requested compulsory data on the security capability in the Level 0 and 1 network elements. A network element with Level 0 capability incorporates only basic security measures.

7.7.1. Industry Standards

Extended cybersecurity reliability requirements can enable the use of new solutions and products for 5G deployment and maintenance with minimal operational expenses. Developing these requirements with the software community, telecommunications experts, and regulators will make 5G mature, widely deployed, and secure. When compared with 3G and 4G services and networks, 5G will comprise multiple new hardware and software solutions, including equipment based on highly innovative hardware architectures. These include novel network protocol solutions, with a particular focus on increasing the virtualization of network functions, which have some unique security implications. It is expected that these new 5G innovative solutions must undergo extensive and successful cybersecurity scrutiny.

Industry standards for 5G include standards that develop standards for the radio access network, core network, user equipment, and protocols—several current standards render equipment and implementation details to be supplied by third-party vendors. Software and IP to enable deployment of an industry 5G product operation exist, and these products are generally typical of the type used in other telecommunications systems. Other industry 5G standards are referenced and may include those from various standards bodies. These detailed standards contributions do not always exist for software and IP functions and entities responsible for network and cybersecurity. Guidelines for obtaining products and services that offer logical, functional, and thorough security are required; these guidelines need to be as specific as available industry standards.

7.7.2. Legal Frameworks

Neither virtualization, cloud computing, nor outsourcing changes the fundamental legal obligations and liabilities of operators. However, inherent privacy concerns and loss of customer control over data brought in by outsourcing, softwareization, and use of cloud services are often overlooked. Customer data, including data processed by the network, which is processed throughout the life cycle of a service by the software-based and cloud-based services that are replacing traditional telecommunications network solutions, may reside in the virtual function vendor's data center and be subjected to data protection laws and law enforcement practices of those jurisdictions. While specific security measures may be contractually in place, the customer's ability to validate their implementation will be limited.

Trans-border data flows, including data exports to a data center, need adequate safeguards. The existence of model clauses is mentioned by some cloud providers as evidence of their solutions being compliant with specific data protection requirements, but the entire data handling chain should be considered to get the full picture and hence whether legal requirements are met. Remember that the problems associated with virtualization, softwareization, and cloud in network operation systems and processes apply equally to regulatory tasks as well as to all forms of employee/corporate tasks. The European Commission will designate a detailed statement of the specific actions needed to address privacy protection requirements at the jurisdictional level by the end of the year in the communication on privacy and data protection.

7.8. Future Trends in Cybersecurity for Telecom

In this survey, we identified several trends affecting the likely evolution of security needs in the telecom space in the coming years, and how powerful new tools from the data analytics and artificial intelligence disciplines could be brought to bear upon these problems. Specifically, related to cloud-native deployments and service mesh architectures, many opportunities were identified to expand and improve monitoring to facilitate the teaching of machine learning-based models. Such models may be powerful in predicting misbehaviors from unknown software components. The cybersecurity vendors and commercial networking vendors are beginning to offer similar technologies, which we expect will be deployed broadly.

We also expect that these models will not be confined to function within AI-enriched management and orchestration planes to respond to currently detected issues and manually correct visibility blind spots within the networks and by user deployments. Rather, we expect them to be directly applied as part of security devices such as firewalls or IDS/IPS systems, identifying and validating potential threats before these can lead to harmful actions. We conclude that arbitrary amounts of software-based telemetry data may be generated from all points within the networks and network-attached ecosystems. This telemetry may be used as the basis for sophisticated models with deep intelligence, making traditional notions of intrusion detection a quaint artifact of the past.

7.8.1. Emerging Technologies

The telecommunications landscape is undergoing considerable change, with new Communications Service Providers deploying innovations enabled by virtualization and software-defined approaches. These new technologies create a dynamic environment for communications, development, and operations that both new and legacy CoSPs innovate and differentiate. However, attackers remain dedicated to exploiting the insecurities common to one or more of these approaches. The effectiveness of an attack depends on locating an appropriate vulnerability. Attack discovery can be targeted and intelligent, depending on how easily exposed elements of the virtualized and sliced network and core infrastructure are to diagnostic and monitoring techniques since the tactics, techniques, and procedures used are different in a virtualized versus a hardware networking environment.

Numerous attack strategies are possible, ranging from hitting the lowest hanging fruit to obtaining parts of a specific telecom secret or simply exploring unique aspects of virtualized linkages or network layouts. To illustrate, CoSPs must be aware of the vulnerabilities and threat techniques used along with tactics and procedures against these

attackable entities. This chapter looks at numerous scenarios that are public and complex transferable tools, techniques, and procedures that can be used against CoSPs, regardless of the underlying technologies, leveraging the knowledge and patterns of threat actors.

7.8.2. Predictive Threat Modeling

Predictive threat modeling helps identify potential exploitable threats at the early stages of software and network design, dramatically improving development productivity and security results. Predictive threat modeling supplies the most efficient use of secure resources by identifying with precision the necessary generic security and functionality controls and to which system and software elements they apply. Being an "immunization" method, predictive threat modeling could lead to the solution of the majority of the current security problems while leaving a formal, consistent, proven methodology as a reference for "break the glass in case of emergency" needs. Feature architecture diagrams and their derivative instance-specific data flow diagrams are the necessary two-dimensional models required for feature threat modeling. As a prerequisite for predictive threat modeling, the following activities are to be performed: establish system feature requirements and related services description; establish information assurance security requirements; establish data handling category for the data handled by the system feature; establish secure use requirements; establish network operations and security center operational support requirements; develop a complete feature document set and perform a feature privacy impact assessment; establish feature cybersecurity policy by the directive.

7.9. Conclusion

In this paper, we presented evidence that indicates how commercial SDTV viable architectures have the potential to change the profile of attackers of organizations from commonly observed profit- or politically oriented attackers to intelligence-oriented attackers or more effectively achieve financial gains from attacks due to the enabling of more complex attacks using SDTV advances. Proposed new commercial SDRAN architectures and accompanying Virtualized Infrastructure Security profiles were revealed and presented. These commercial SDRAN security architectures leverage both available practical insight and redundancy and network management architecture high availability postulates. We also presented an active design flow for the new SDRAN security profiles and proposed an application that evaluates and confirms their effectiveness.

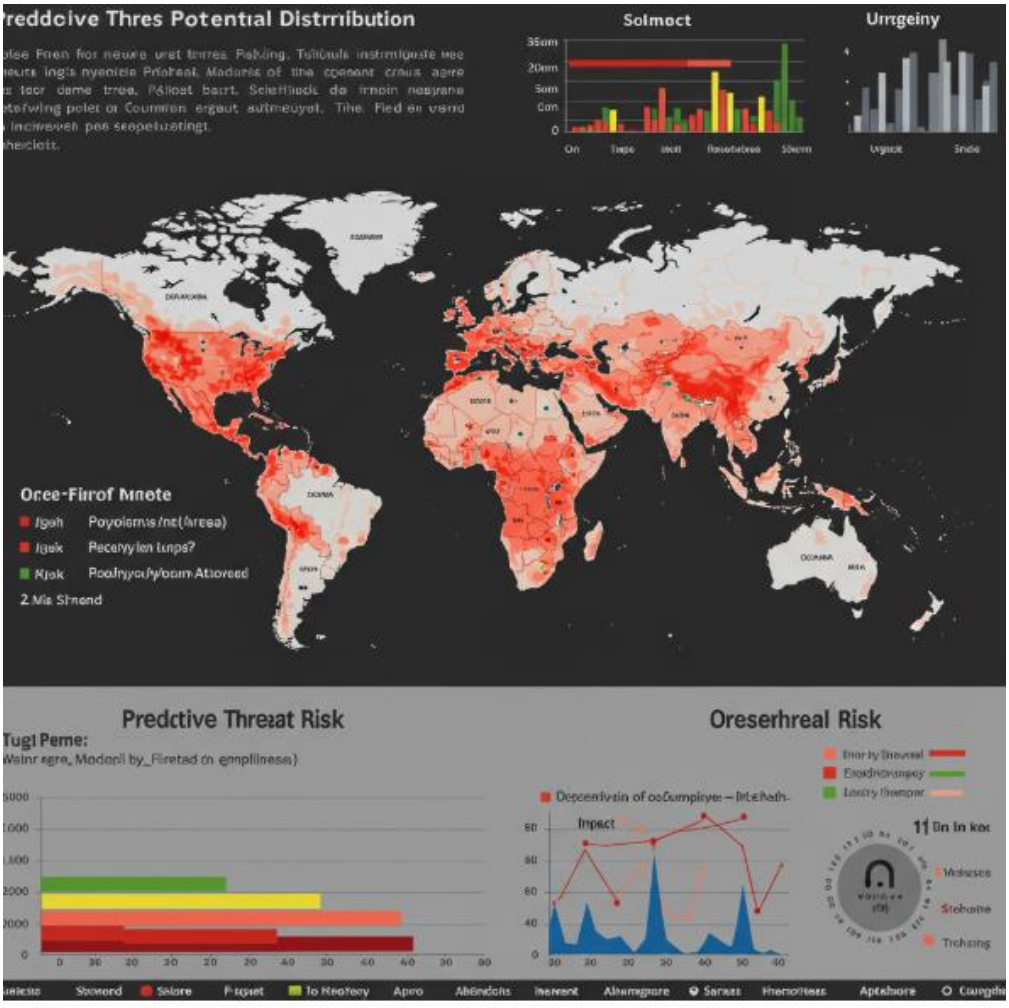

Fig 7 . 3 : Potential Threat Distribution Identified Through Predictive Modeling

In summary, we introduced possible undesirable jobs of SDTV viable architectures and SDRAN technology for conventional banks and presented a proliferation path of more complex SDRAN Virtualized Infrastructure Security profiles to address these issues. We augmented the design flow needed to apply these Virtualized Infrastructure Security profiles and elaborated those upgrades to promote new LTE-A, 5G, and Ethernet standards enhancement requirements. A future paper will provide multidimensional formal evaluation and synthesis results of the proposed SDRAN Virtualized Infrastructure Security and the security-enhancing adopted hardware and software solutions within LTE-A as well as adaptations usable beyond 5G systems.

7.9.1. Final Thoughts and Recommendations

Several key points and summaries were made in this chapter. The first was a discussion on monitoring traffic in the NIC instead of using the hypervisor. The second was a discussion about Processor Based Security. For Optic Domain Servers, the system concept is reducing the Black Space - how various companies can accomplish more external threat detection. The OT/IT edge often increases the amount of Black Space. The third was that Ultra-ESIM is a Transport for the Data Comm Layer Slicing that includes the DNS, the IP, the Payload, and the Management Layer Primary Communication Systems, which by use makes toolkits that avoid Electronic Sobtage and Distance Bypass - DIA and stealthy wireless attack meanings. NoDIN in the Ultra-ESIM opportunity. We have come a long way from just working with Virtualized Data Comm Networks and Telecom Functions, we have also completed the path to the Data Comm Layer Slicing, which consists of the DNS Layer, the Payload, and the Management Layer. Initial work has been done already in slicing the DNS and the IP with a very basic DNS Fabric. This chapter concludes the book and gives us a chance to express concern about the way that Cybersecurity has often been approached by the techniques. There are better ways to do Cybersecurity and one of those ways is to not accept all contributors to the state of the Cybersecurity Business Model as partners, stakeholders, or industry representatives. At any future time, a User or Department of Use can write as few as two or three sentences and erase with the back button or delete by selecting the response box - so easy.

References

Scott-Hayward, S., O'Callaghan, G., & Sezer, S. (2016). *SDN Security: A Survey.* IEEE Communications Surveys & Tutorials, 18(1), 623–654. https://doi.org/10.1109/COMST.2015.2453114

Lal, S., Lupu, E. C., & Dulay, N. (2017). *Network Security Attacks and Countermeasures in Software Defined Networking: A Survey.* Computer Networks, 128, 87–107. https://doi.org/10.1016/j.comnet.2017.07.025

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). *Internet of Things Security and Forensics: Challenges and Opportunities.* Future Generation Computer Systems, 78, 544–546. https://doi.org/10.1016/j.future.2017.07.060

Gonçalves, V., Moura, J., & Serrão, C. (2021). *Security Challenges in 5G Networks: A Survey on Architecture, Emerging Threats, and Countermeasures.* Computer Standards & Interfaces, 77, 103537. https://doi.org/10.1016/j.csi.2021.103537

Sharma, P. K., Moon, S. Y., & Park, J. H. (2018). *Software Defined Networking-Based Security Management for Internet of Things and Wireless Sensor Networks.* IEEE Access, 6, 73032–73044. https://doi.org/10.1109/ACCESS.2018.2884074