Intrinsic Security: A Robust Framework for Cloud-Native Network Slicing via a Proactive Defense Paradigm

Qiang Wu, Ran Wang, Xincheng Yan, Chunming Wu and Rongxing Lu

Abstract

Opening-up sharing has prompted the multi-tenancy architecture, whereby different vendors (including outsourcees) work together with network operators to form a vibrant service ecosystem, resulting in several advantages as well as risks. In particular, the static nature of existing architectures in network functions virtualization-based (NFV-based) clouds facilitate hacking. Thus, much attention has been focused on determining how to avoid the uncontrollable cloud security induced by complex production relations and non-trustworthy software/hardware sources when the two sets of security risks intersect. In this article, we investigate latent persistent threats against cloud environments and determine a high degree of complementarity and consistency between the NFV-based cloud environment and the dynamic defense concept. More specifically, new NFV-based cloud features provide an effective implementation for dynamic defense, while the generalized robustness of dynamic defense theory allows for high security gains. Intrinsic cloud security (iCS) is then proposed to align NFV-based clouds, mimicking defense and the moving target defense (MTD) paradigm to implement a seamless integration and symbiosis evolution between security and NFV-based clouds. We quantify the impact on system overhead to account for efficiency and cost issues. The simulation analysis demonstrates that the enhanced mode is able to consistently obtain a more beneficial and stable defense compared with the counterparts.

Introduction

Traditional networks are customized based on basic telecommunication services and can be characterized as static and closed systems. Under diversified service scenarios and business models, the static network model is unable to effectively deal with the uncertain factors and differences in the development of massive mobile Internet services. In terms of evolution, networks prior to 5G can be compared to a track athlete, while the 5G network is an all-round gymnast, with a more favorable openness and stronger innovation capabilities. Facing more complex and volatile requirements in the vertical industry, network functions virtualization (NFV)-based clouds overcome the network static model problem to undoubtedly provide significant benefits for the implementation of network slices due to their cost efficiency and dynamic service deployability. This can result in a comprehensive cost reduction and an open and shared-service ecosystem at the network architecture level [1], enabling 5G networks to truly have outstanding capabilities.

NFV-based clouds are associated with numerous benefits and several new features that enhance the construction of the service ecosystem, such as multi-tenancy, openness capabilities, automated deployment of third-party applications, and multiple-vendor virtual network function (VNF) provision [2]. These features come at the cost of numerous security flaws, whereby the 5G network slice becomes vulnerable to security threats. Despite the challenges to the existing security protection system, the breakthrough of NFV-based clouds in the static network model also provides technical support for the implementation of dynamic proactive defense theories, such as moving target defense (MTD) [3] and mimic defense [4].

Intrinsic security, an innate type of security framework, is an integral component and indivisible part of a service system, providing a universal surface defense rather than a point defense. Key security risks associated with NFV Infrastructure (NFVI) and security practices are considered as important concerns [5], yet intrinsic security issues are ignored in the NFVI reference architecture defined by the European telecommunications standards institute (ETSI) [6]. Moreover, the traditional "plug-in" and "enhanced" defense concept is a fixed passive response mechanism based on prior knowledge, viruses, and malicious behaviors. As communication systems tend to be enormous and open, malicious behavior and virus features including unknown threats are difficult or even infeasible to be enumerated comprehensively. Thus, such passive response mechanisms based on prior knowledge have been proved to be inadequate in keeping up with the development of attacks. Therefore, the judgment criteria for security threats have attracted much attention. When considering the defense mechanism of NFV-based clouds, security technologies must adopt a seamless inte-

This work is supported by the National Key R&D Program of China (2020YFB1804705); National Natural Science Foundation of China under grant No. 62171218, No. 61801215; special project of Mobile Internet System and Application Security National Engineering Laboratory under grant M-2021-03; the Key R&D Program of Zhejiang Province (2021C01036 2020C01077); and the Fundamental Research Funds for the Central Universities (Zhejiang University NGICS Platform: ZJUNGICS2021021).

Digital Object Identifier: 10.1109/MWC.001.2100251

Qiang Wu is with Nanjing University of Aeronautics and Astronautics, and State Key Laboratory of Mobile Networks and Mobile Multimedia Technology; Ran Wang (corresponding author) is with Nanjing University of Aeronautics and Astronautics, and Collaborative Innovation Center of Novel Software Technology and Industrialization; Xincheng Yan is with the State Key Laboratory of Mobile Networks and Mobile Multimedia Technology; Chunming Wu is with Zhejiang University; Rongxing Lu is with the University of New Brunswick.

1536-1284/21/$25.00 © 2021 IEEE

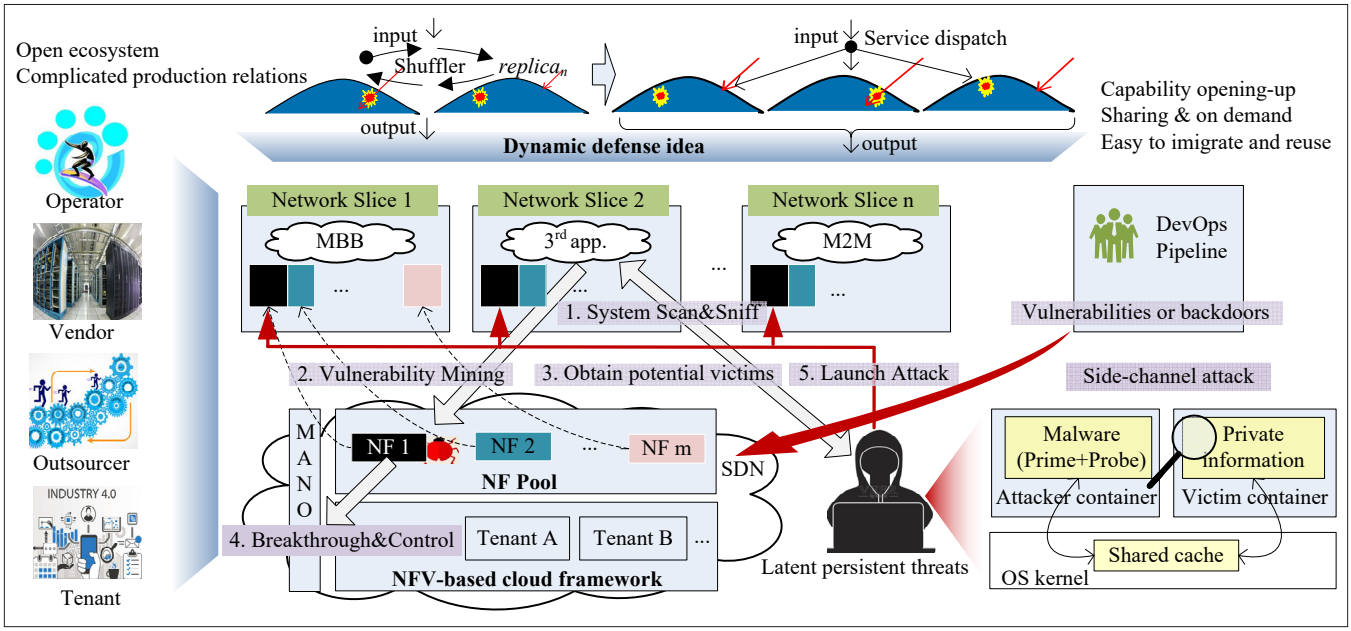

FIGURE 1. NFV-based cloud structure and corresponding attack-defense profile.

gration and symbiosis evolution with the service system, and evolve away from traditional defense concepts to achieve intrinsic proactive protection.

Based on the NFV-based cloud framework, we propose a security defense method based on intrinsic cloud security (iCS), a dynamic and heterogeneous attack surface model. The proposed method can adaptively achieve seamless integration and the symbiosis evolution between cyber security mechanisms and network slice services. The key contributions of this article are as follows:

- We systematically classify and review the security challenges that pose threats to NFVI, and the pivotal characteristics, fitness, and coherence of both the Dynamic Heterogeneous Redundancy (DHR) system and NFV-based cloud are thoroughly analyzed.
- We propose the iCS framework to align the NFV-based cloud with the paradigm of mimic defense and MTD under the cost and efficiency constraints.
- In response to the lack of security mechanisms in the ETSI NFVI reference architecture, the intrinsic security features are expanded at the architecture level (e.g., the heterogeneous dynamic redundancy of the attack surface and the automated deployment of key security components).

The rest of this article is organized as follows. In the following section, we discuss the principle security risks associated with NFVI and highlight the potential intrinsic security themes. The iCS framework is then proposed. The experimental results are then described. The final section concludes the article.

Dynamic Proactive Defense: Threat Analysis, Emerging Requirements, and Coherence Analysis

Opening-up sharing, a key feature of the NFV-based cloud system, is cost-effective, agile, enhances productivity, and does not require complicated management. Moreover, opening-up sharing has lowered the threshold for service developers, thus more and more different vendors (including outsourcees) are collaborating with network operators to form a vibrant service ecosystem [7]. In terms of cyber security, a lower threshold can be both a convenience and a risk, which consequently increases the vulnerability of cyber security. Attackers have an asymmetric advantage due to the static nature of traditional cyber systems, whereby they are able to sniff a system, study its vulnerabilities, and select the most appropriate opportunity to maximize the attack benefits. Determining how to avoid the uncontrollability of cloud security caused by Devops, COTS and non-trustworthy software/hardware sources proves to be a complicated task when the two sets of security risks (i.e., opening-up sharing and the static cyber nature) intersect. Fig. 1 describes the potential security risks associated with NFV-based clouds based on several potential attack scenarios. These are discussed in more detail in the following.

Cache Side-Channel Attacks Cross VM or Container

The enclave and non-enclave share numerous system resources, resulting in a very large attack surface for side-channel attacks. Malicious tenants or insiders can easily employ the underlying shared resources to bypass the logical isolation and stealthily steal the private information of other co-resident virtual machines.

Efficiencies of Scale from Code Reuse Attacks

The majority of NF components are homogeneous in the NF pool with shared properties. NF1 in Fig. 1 introduces shared vulnerabilities or backdoors, whereby different network slices are vulnerable to code reuse attacks, acting as economies-of-scale incentives to attackers.

Latent Persistent Threats against Cloud Environments

In an open and shared environment, the production relations evolve toward diversification and

NFV-based cloud	DHR System
Challenge	Security Gain
Blurred boundary, invalid boundary isolation	Intrinsic security, increase uncertainty
Open source and 3rd software, internal threats	Component-level, architecture-level security
Infrastructure homogenization, broader spread of vulnerabilities	Component diversity, smaller attack surface
Multi-tenancies, outsourcers, DevOps	Generalized robustness, dynamic empowerment
Feature	Benefit for implementation
Automatic deployment	Flexible and diverse changes
Resilient scalability	Dynamic, random, no software update blackout
Componentization, microservice	Normalized input/output interface, dynamic
Service chaining, orchestration	Dynamic, random, improved interface compatibility
CTOS-based	Diverseness, lower cost
Heterogeneous resource pools	Heterogeneous redundancy
Centralized control, global view	Dynamic, random

TABLE 1. Fitness and coherence analysis of DHR systems and NFV-based cloud environments.

complexity. The addition of multi-tenancies and outsourcers induces the relationship between network operators and vendors to diverge from the "one-to-one" fixed relationship, and the fluid and overlapping outsourcing relationship established by the network platform is continuously expanding its scale. This results in the imbalance and mismatch of the security capabilities of the service providers. Furthermore, the outsourcee and the outsourcer may in fact be competitors in certain market segments [8]. Attackers can take advantage of the more convenient conditions to implement advanced, persistent and effective threats and attacks with various methods (e.g., infected medium, supply chain, and social engineering). In terms of the defender, the defense effectiveness often depends on the scale of the prior knowledge on malicious behavior features, and so on. Determining the malicious behavior and its occurrence in real-time can be a theoretical challenge, particularly with the endless emergence of new types of attacks and zero-day vulnerabilities [9].

Dynamic defense frameworks have been proposed to provide intelligent countermeasures by the implementation of a dynamic cyber nature. MTD attempts to build self-defending systems via dynamic systems that are harder to sniff and predict [10]. Mimic defense theory provides a new perspective for solving component-level security issues, without reliance on prior knowledge and post-maintenance [4]. More specifically, the system itself has the capability of proactive defense using the DHR model, while multiple replicas of the heterogeneous functionally equivalent executor are deployed to produce multiple outputs. Selection judgments are then made on the output results (typically the majority judgment). The dynamic nature creates uncertainty on the resources to be potentially exploited by the attacker in the spatio-temporal dimension, and the attack surface moves irregularly on the macro level. According to the attack surface theory, the attack accessibility of the victim cannot be guaranteed, and thus the attacker's workload and difficulty are increased [11].

Previous studies have presented an extensive range of MTD and mimic defense models, yet their implementation is highly coupled with the corresponding service system, and thus a dedicated solution is required for each specific service system. The security scheme and service system are nested together, and coupling and interface compatibility issues limit the scope and effectiveness of the solution. Moreover, embedding these dedicated security solutions into the entire service design, network topology and network element dynamic deployment proves to be difficult. The opening-up of network capabilities and the improvement of the ecological chain [12] require that X complies with the diversification and complexity trends of the production relations. Thus new theories and methods must be determined to effectively relieve the contradiction between security and opening-up, with advanced progressiveness and controllability characteristics.

New NFV-based cloud features, such as dynamic resource scheduling, microservice, and centralized control [6], provide guidance for the MTD and mimic the defense unified paradigm. Recent advances allow for cost efficiency and the effective deployment of the implementations, as well as the seamless integration and symbiosis evolution between intrinsic security and the NFV-based cloud to achieve proactive defense and high security gains. Table 1 reports the fitness and coherence analysis of the DHR systems and NFV-based cloud environments. The genes of NFV-based clouds are highly complementary to the DHR model.

Methodology: Intrinsic Security for NFV-Based Clouds

Figure 2 presents the iCS system architecture. Virtualization is applied to realize the decoupling of the underlying physical device and software. The lightweight VNF design results in executors of smaller granularity, and thus the normalization requirements of the executor input and output interfaces in the mimic defense are more easily satisfied. These existing features provide a solid basis for the dynamic and random DHR system, which is typically a source of uncertainty. Based on the NFV architecture in the ETSI, the iCS foundation maximizes the use of the existing mechanisms, such as dynamic scheduling and orchestration management, to maximize the dynamicity and randomness. This can effectively reduce the increased costs induced by the DHR security gain. Moreover, due to the improved interface compatibility, the iCS can be applied to a wider range of fields rather than a specific dedicated system, and exhibits a high development and runtime efficiency. The security controller is primarily responsible for the creation, management, and distribution of the unified security policies. The mutations of attack surface, showing its changes in network environment, topology, NFVI, and so on, are achieved through enhancing the use of the dynamic and redundant characteristics in the NFV-based cloud.

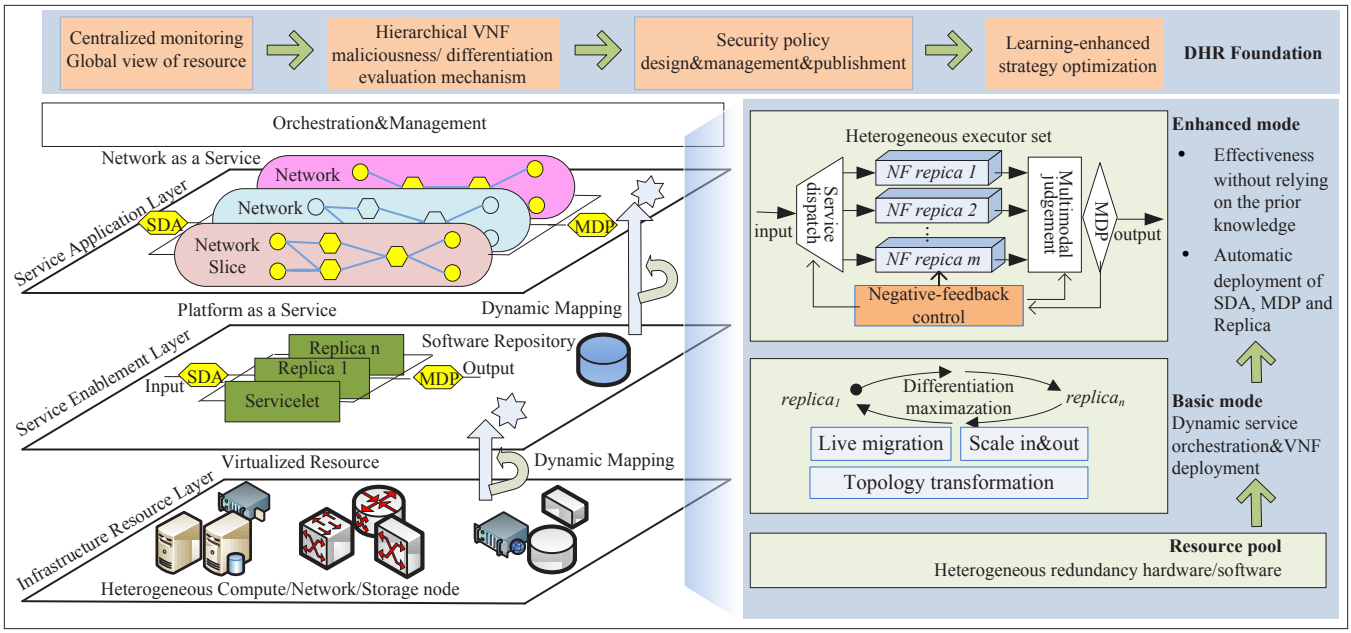

FIGURE 2. iCS system architecture: intrinsic security for NFV-based clouds.

Construction, Evaluation, and Deployment of Heterogeneous Replicas

Software diversification can effectively break the attack chain dependence pattern and is able to deal with common attacks and cracks. The iCS framework is compatible with numerous diversification techniques. As the preferred building tool for executor variants in the iCS basic mode, the compiler has the advantages of convenient deployment, low cost, and universality. It can effectively generate redundant versions and diverse executor variants, and the resulting uncertainty import factors are inherited by different components.

The evaluation mechanism is performed based on maliciousness and differentiation. The differentiation evaluation involves the weighting of the heterogeneity degree between replicas by the entropy value method. Heterogeneous deployment is then adopted as a minimax problem, whereby the optimization goal is to maximize the degree of heterogeneity between replicas. This is followed by the implementation of an immune algorithm to quickly solve the optimal deployment solution. For the maliciousness evaluation, in the mimic decision point (MDP) multimodal judgment link, the dysfunctional replicas with output results distinct to the majority of replicas are shuffled and transferred out of the executor set to be cleaned. The malicious behavior of replicas is collected and compared with the malicious score information in the knowledge graph database, and the normalized score result will be assigned to the maliciousness attribute of a replica. A replica with a maliciousness attribute score exceeding an arbitrary empirical threshold will be shuffled and subsequently cleaned.

When the system is initialized, the set of the redundant replica is pre-installed in the software warehouse. These replicas are used to meet the requirements of the heterogeneity characteristics in the DHR system. With the orchestration and management mechanism defined in ETSI, the heterogeneous versions are selected randomly or according to a preset policy, and are then instantiated and deployed on the infrastructure. The redundancy is induced by three factors:

- The 1+1 or N+M backup mechanism of the service system for high reliability
- The number of heterogeneous versions of the same component
- The resource number of the virtualized infrastructures.

Through the heterogeneous resource pool management of the iCS system, the redundancy rate can be flexibly set according to security level and cost constraints.

Dynamic Scheduling and Orchestration Management

If the attack surfaces of a target system exhibit random changes, maintaining the effectiveness of an attack chain (e.g., information acquired by the attacker, the resources controlled by the attacker, and previously effective attack schemes) following the next scheduling can be difficult. Enhancing the use of the dynamic and redundant characteristics in the NFV-based cloud can obtain the same effect of the DHR atypical construction. This can consequently increase the attacker's cognitive difficulty on the target object. Irregular VNF scheduling and task migration will disrupt the reachability of an attack chain, while virtualized and dynamic resource allocation mechanisms can disrupt the stability of an attack chain. This can be effective, both economically and technically, in alleviating the current and future cloud trends and security credibility contradictions. The intrinsic uncertainty factor is reflected in the following four aspects:

NFV Service Chaining Orchestration and Management: The service chain is an ordered set of VNFs. Tenant traffic passes through multiple VNF components in turn according to a specified policy. When a service chain model is established by NFV orchestration (NVFO), the VNFs that are able to be flexibly scheduled are marked in the security policy template, which includes several threshold parameters and corresponding security policy control actions (e.g., schedule opportunities,

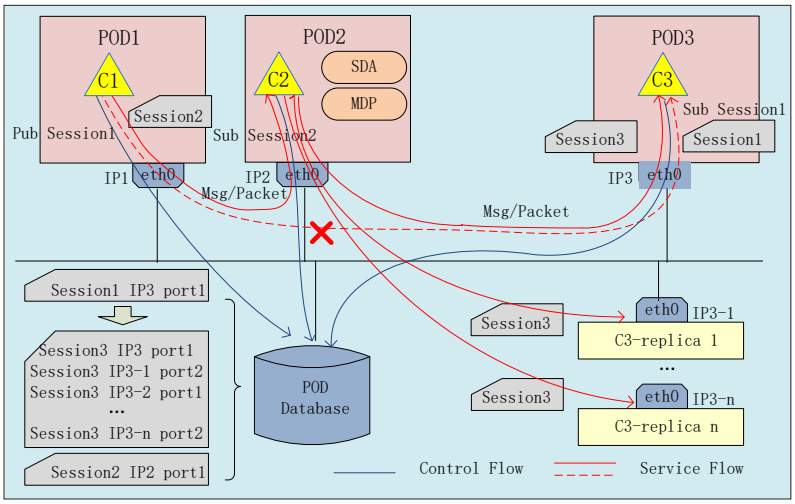

FIGURE 3. Subscription and publication mechanisms of the SDA/MDPs and replicas.

reconfiguration timing, and the algorithm selected for the heterogeneous executors). The threshold parameters are measured and analyzed via the big data analysis module. The high scalability ensures the capability of the VNFs flexible deployment and rapid adjustment, with the ability to economically schedule heterogeneous executors. The service chaining running mechanism can constitute a considerable dynamic space to reduce the reliability of exploiting vulnerabilities and backdoor attacks.

Dynamic Management of the Cloud Resource Pool: NFVI achieves the unified management and global monitoring of computing, storage, and network resources. Physically distributed resources are constructed into a logically unified cloud resource pool. The resource orchestration allocates resources for the tenants or the application on demand according to a certain orchestration algorithm, and aggregates the resources to form a certain network topology relationship. This allows for the purpose of automatic deployment to be achieved. The resource orchestration not only serves the service function requirements, but also acts as the execution unit that implements dynamic requirements in DHR.

Resilient Scaling and Service Migration: In the NFV-based cloud framework, the service processing unit can flexibly scale in and out, and the traffic is automatically migrated at the minute level. Therefore, the dynamic matching of resources and service load is realized. This not only improves the resource utilization efficiency, but also ensures the response speed required by the DHR system. The service processing units built on the basis of equivalence heterogeneity (i.e., the NFVI and VNF components) constitute the multiple heterogeneous elements in the spatial dimension. Furthermore, each processing flow of the resilient scaling and the service migration constitutes dynamical elements in the time dimension. This results in an irregular system's attack surface. The interface between the DHR Foundation and the management and orchestration (MANO) unit is used to deploy the security policy, while the resilient scaling and service migration are performed according to the security policy. Note that the security policy management within the DHR Foundation is hierarchical. The resilient scaling policy can be at the network element, network service, or network slice levels. This mechanism is also used to clean unhealthy service processing units and deal with the software update "blackout" without service interruption.

Communication Based-Dynamic Translation Mechanism: The Software Defined Network (SDN)-C has a global network topology and a packet forwarding table. The parameter translation unit is superimposed in the SDN-C, and the global dynamic adjustment to the network topology and traffic path can be implemented as required. Under the unified scheduling of SDN-C, the session traffic is sent to an address translation gateway. The machine learning algorithms are trained on historical attack data and implemented to identify the potential malicious connections and potential attack destinations. The network topology is hidden from attackers and is employed to trap them into decoy nodes via strategic and holistic network topology mutations based on the adversary characteristics. This can effectively disrupt the adversarial network reconnaissance [13].

Lifecycle Management and Automatic Deployment of the SDA/MDPs and Replicas

Although the features of component diversification, dynamicity, and randomness in the basic mode increase difficulties in exploiting software vulnerabilities, threats are not completely eliminated. It is thus necessary to introduce multimode judgment to generate a more reliable output compared to a single executor. This is denoted as the enhanced mode. Multimode judgment can partially solve the judging criteria issue for unknown malicious behavior. Thus, the service dispatch agent (SDA) and MDP are implemented in the service processing flow. In addition to meeting the requirements of the service system, the extended functions are implemented with the existing cloud foundation, including the SDA/MDPs and replicas lifecycle management, automated deployment, logic relationship management with components, and resource reservation strategies. A single MDP does not apply to all service components due to the lack of a normalizable input/output interface. Hence, the differences in the component attributes need to be accounted for in the cloud foundation service. They can be deployed incrementally based on the security level needs. The MDP realizes the function abnormality feature through multimode judgment at the bit-, load-, behavior-, or even content-level. It then triggers negative-feedback control and the dysfunctional replica is cleaned. Figure 3 presents the subscription and publication mechanism of the SDA/MDPs and replicas.

iCS System Characteristics

The infrastructure of NFV-based clouds is highly homogenized with abundant redundant resources, which provides a natural material basis for the introduction of dynamic defense genes such as dynamicity, heterogeneity, redundancy, randomness, and diversity. In addition, the general mechanisms, including resilient resource pool and orchestration scheduling, can effectively cope with the system complexity and cost overhead caused by the DHR. The iCS system exhibits the following characteristics:

- In terms of security performance, the attack surface mutations are manageable according to the security policy of the security controller, and service continuity is maintained while performing proactive defense. Thus, the attack surface mutations are sustainable. The structural gains, such as the open and compatible generation method of heterogeneous components, hierarchical VNF maliciousness/differentiation evaluation, and learning-enhanced strategy optimization, enable the heterogeneous characteristics to be continuously optimized according to changes in the attack situation. The attack surface mutations are both rapid and diverse. The mutations in the network topology and service chain can be implemented at the minute level. Furthermore, the mutation diversity not only considers the mutation modes, but also the diversity of the attack surface parameter range.
- The deployment of the basic mode does not significantly increase the system cost of the NFV-based cloud. The enhanced mode obtains an improved security gain, and the cost is positively related to the protection range of the mimic domain and the number of components. In addition, the plug-in incremental deployment can be performed based on the security level.
- In terms of efficiency, intrinsic security fully exploits the potential of existing NFV-based clouds. The attributes are enlarged for the basic mode requirements (e.g., service orchestration automation, network scheduling flexibility, and network resource allocation scalability). These attributes consequently become a part of the typical mimic defense construction to enable the automatic generation, automatic deployment, and dynamic scheduling of key units.

Simulation Analysis

Impact on the System Overhead

In this subsection, we investigate the impact of various iCS mechanisms on the computing resource overhead under specific traffic loads, as it constitutes the most important metric for NFV resource overhead. 5G core (5GC) network, a typical cloud native commercial system, is adopted to implement the experiment. Specifically, five tests are conducted. First, the computation resource overhead of the 5GC network without any iCS scheme is evaluated, which is deemed as the comparison baseline, as illustrated by curve 1 in Fig. 4. Second, we evaluate the system overhead in the iCS basic mode, under which four aforementioned scheduling strategies are adopted and the mutation period is set to 1 hour, as illustrated by curve 2. We can observe that the iCS basic mode induce quite slightly (less than 5 percent) incremental computation resource overhead compared with the 5GC baseline, and such overhead increment is mainly from the foundation and operation of the DHR system and hypervisor. Apparently, the iCS basic mode exerts rather limited impact on the overall cost of the 5GC network, showing its outstanding potential on increasing the security gains while simultaneously satisfying the system cost and implementation efficiency requirements in real-world exploits.

The performance of the iCS enhanced mode under various configurations is illustrated by curve 3, curve 4 and curve 5 in Fig. 4, respectively. Specifically, curve 3 depicts the computation resource overhead under the iCS enhanced mode with one replica, wherein the incremental overhead compared with the baseline is mainly induced by the DHR and SDA/MDP functional entities. Curve 4 and curve 5 illustrate the overhead under iCS enhanced mode with two and three replicas, respectively. From curves 3-5, we can observe that the incremental cost shows a near linear relationship with the number of replicas, since the overhead is mainly generated by a network element on the forwarding plane (e.g., the UPF), whereas the proportion of overhead from the VNF on the control plane is rather limited. Therefore, restrictions of the VNF replicas on the control plane are not that important, but on the forwarding plane, the number of VNF replicas should be designed reasonably according to changes in the attack situation.

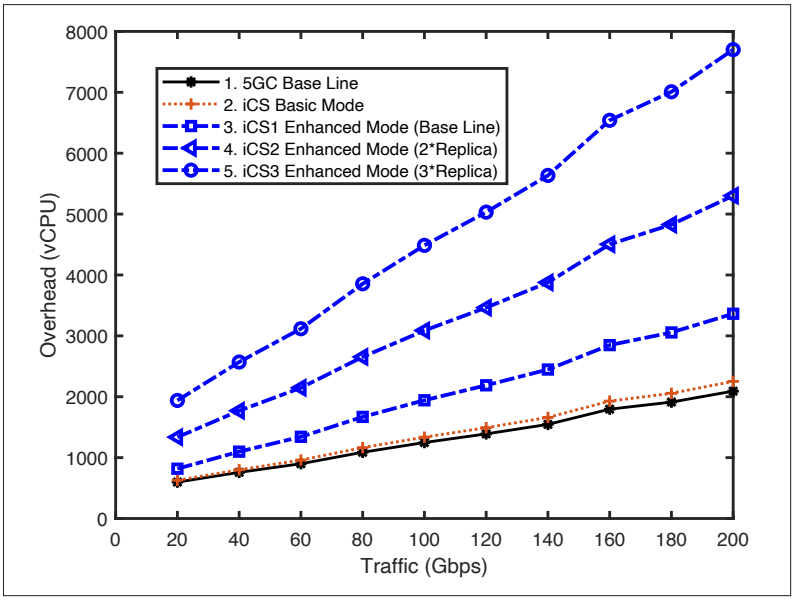

FIGURE 4. System overhead comparison between iCS and 5GC.

Impact on the Probability of Compromise

The testbed adopts a latent serial attack model. Due to the fault tolerance of the cloud system, when an executor is compromised, the attacker does not immediately destroy it but continues to infect and attack other executors one by one, until a complete system breakthrough occurs. Because of the high capability requirements and high resource input of parallel attacks, only latent serial attacks are discussed here. It is assumed that the protected system does adopt other security measures additional to the set defense mechanism, such as intrusion detection, firewall, and so on. The attack process assumes that the attacker masters one or more available vulnerabilities and has experience with one or more threats to take advantage of the known vulnerabilities. Moreover, the meantime-to-compromise and shuffling periods are set to 4 days and 20 days, respectively. Curve 1 in Fig. 5 depicts the average proportion of executors being compromised (i.e., average attack risk) with time. Note that in the experiment settings, the 20 days' period is divided into 80 time slots, and within each time slot, the proba-

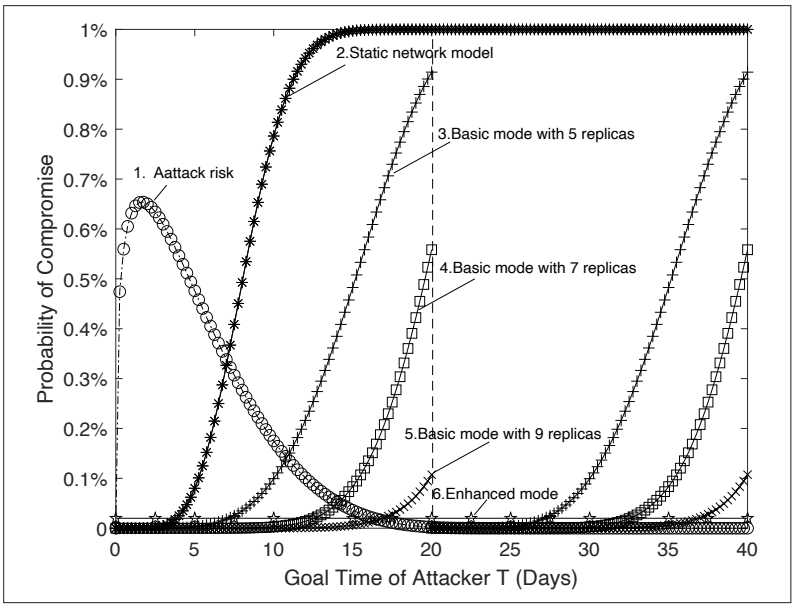

FIGURE 5. Measurement Results of the Impact of iCS on compromise.

bility of compromise (attack risk) follows Beta distribution [14]. For the enhanced mode with 2f+1 heterogeneous executors, the attacker must break f+1 executors during the life cycle of the executor for a successful attack. The service chain consists of five components, simulating a system attack by an expert attacker. Curve 2 demonstrates the probability of compromise in the static network model, which is adopted as a baseline for the security gains comparisons. Curves 3, 4, and 5 compare the probability of compromise in the basic mode with 5, 7, and 9 executors, respectively. The security gains of the system are observed to increase with the number of heterogeneous executors. Hence, managers should select heterogeneous system configurations based on the security level requirements. Curve 6 depicts the probability of compromise in the enhanced mode. The enhanced mode exhibits even higher security gains, with a probability of compromise close to 0, which is consistent with the expectation.

Conclusion

Opening-up and sharing ecological environments can benefit significantly from the incorporation of intrinsic security requirements in the NFVI security mechanism of ETSI [15]. The generalized robustness of dynamic defense theory provides a new strategy for solving component-level and system-level security issues in NFV-based clouds. Following the introduction of the NFV/SDN technology, the communication network with an NFV-based cloud as the core infrastructure realizes service orchestration automation, network scheduling flexibility, and network resource allocation scalability. We determine a high degree of complementarity and consistency, and these new features provide an effective means for implementing these theories.

The iCS framework fuses the MTD concept and mimic defense theory within the NFV-based cloud framework and subsequently implements the seamless integration and symbiosis evolution between security and services to achieve proactive protection against internal and external threats. In the basic mode, an iCS framework obtains the security gain of a typical MTD architecture by default, as well as outstanding cost advantages. However, in the enhanced mode, it exhibits cost rigidity due to the more customized development. The iCS system provides a common support platform for the management and automatic deployment of the replicas and SDA/MDPs. Based on this, the incremental development for each component is performed under the corresponding cost and efficiency constraints to achieve the security gain of typical mimic defense construction. The results reveal the iCS framework to be suitable for high security and cost-insensitive scenarios such as the beyond 5G network, 5G vertical industry, and so on.

References

[1] X. Foukas *et al.*, "Network Slicing in 5G: Survey and Challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, 2017, pp. 94–100.

[2] T. Taleb *et al.*, "On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 3, 2017, pp. 1657–81.

[3] S. Sengupta *et al.*, "A Survey of Moving Target Defenses for Network Security," arXiv: *Cryptography and Security*, 2019.

[4] J. Wu, *Cyberspace Mimic Defense*, Springer, 2019.

[5] S. Lal *et al.*, "NFV: Security Threats and Best Practices," *IEEE Commun. Mag.*, vol. 55, no. 8, 2017, pp. 211–17.

[6] ETSI Group Specifications: Network Functions Virtualization (NFV); Architectural Framework.

[7] E. M. Rudd *et al.*, "A Survey of Stealth Malware Attacks, Mitigation Measures, and Steps Toward Autonomous Open World Solutions," *IEEE Commun. Surv. Tutor.*, vol. 19, no. 2, 2017, pp. 1145–72.

[8] E. Marku *et al.*, "Securing Outsourced VNFs: Challenges, State of the Art, and Future Directions," *IEEE Commun. Mag.*, vol. 58, no. 7, July 2020, pp. 72–77.

[9] M. Zhang *et al.*, "Network Diversity: A Security Metric for Evaluating the Resilience of Networks against Zero-Day Attacks," *IEEE T. Inf. Foren. Sec.*, vol. 11, no. 5, 2016, pp. 1071–86.

[10] R. Kapitza *et al.*, "CheapBFT: Resource Efficient Byzantine Fault Tolerance," *IEEE Trans. Comput.*, vol. 65, no. 9, 2016, pp. 2807–19.

[11] W. Peng *et al.*, "A Moving-Target Defense Strategy for Cloud-Based Services With Heterogeneous and Dynamic Attack Surfaces," *IEEE Int'l. Conf. Commun.*, 2014.

[12] E. Marku, G. Biczok, and C. Boyd, "Towards Protected VNFs for Multioperator Service Delivery," *Proc. IEEE Conf. Network Softwarization (NetSoft)*, 2019.

[13] S. Nanda *et al.*, "Predicting Network Attack Patterns in SDN Using Machine Learning Approach," *Proc. IEEE Conf. Network Function Virtualization and Software Defined Networks (NFV-SDN) 2016*, pp. 167–72.

[14] A. Miles *et al.*, "Time-to-Compromise Model for Cyber Risk Reduction Estimation," *Quality of Protection*, 2006, pp. 49–64.

[15] ETSI TR 103 305-1 V3.1.1, Technical Report, CYBER; Critical Security Controls for Effective Cyber Defenc, 2018.

Biographies

Qiang Wu is a Professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China. Before that, he worked as a chief engineer at the ZTE Central Research Institute, and received his Ph.D. degree from the College of Computer Science and Technology, Zhejiang University, Hangzhou, China. He is a Fellow of the China Institute of Communications, CIC, and a Member of Technical Committee of the National Engineering Laboratory for Mobile Internet System and Application Security. His main research field includes future networks, industrial Internet, cyber security, and Space-Earth Integration Networks. The Chinese government honored him with the Second-Class National Science and Technology Progress Award in 2009 and the Second-Class National Technology Innovation Award in 2014. He has more than 100 authorized patents, of which more than 20 have corresponding relations with international standards.

Ran Wang [M'18] is an associate professor with the College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, and Collaborative Innovation

Center of Novel Software Technology and Industrialization, Nanjing, P.R. China. He received his B.E. in electronic and information engineering from the Honors School, Harbin Institute of Technology, P.R. China in July 2011, and the Ph.D. in computer science and engineering from Nanyang Technological University, Singapore in April 2016. He was a research fellow with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore, from October 2015 to August 2016. He has authored or coauthored over 50 papers in top-tier journals and conferences. He received the Nanyang Engineering Doctoral Scholarship (NEDS) Award, Singapore and the Innovative and Entrepreneurial Ph.D. Award of Jiangsu Province, China in 2011 and 2017, respectively. His current research interests include network performance analysis and Internet of electric vehicles, and so on.

XINCHENG YAN is currently the Chief System Architecture Expert at ZTE Corporation, Deputy Director of the Future Network Research Center of the State Key Laboratory of Mobile Networks and Mobile Multimedia Technology. He is a professorate senior engineer, has 20 years of experience in the telecommunications industry, has more than 40 patents, and has presided over the National Science and Technology Major Project of China in 5G security. He has won several scientific and technological awards and won the title of high-level talent in Jiangsu Province.

CHUNMING WU received the Ph.D. degree in computer science from Zhejiang University in 1995. He is currently a professor with the College of Computer Science and Technology, Zhejiang University. He is also the Associate Director of the Research Institute of Computer System Architecture and Network Security, Zhejiang University, and the Director of the NGNT Laboratory. His research fields include reconfigurable networks, network security, and next-generation network infrastructures. The Chinese government honored him with the First-Class National Scientific and Technological Progress Award in 2004 and the Second-Class National Scientific and Technological Progress Award in 2014.

RONGXING LU [S'09, M'11-SM'15, F'21] is a University Research Scholar, an associate professor at the Faculty of Computer Science (FCS), University of New Brunswick (UNB), Canada. Before that, he worked as an assistant professor at the School of Electrical and Electronic Engineering, Nanyang Technological University (NTU), Singapore from April 2013 to August 2016. He worked as a postdoctoral fellow at the University of Waterloo from May 2012 to April 2013. He was awarded the most prestigious "Governor General's Gold Medal" when he received his Ph.D. degree from the Department of Electrical & Computer Engineering, University of Waterloo, Canada, in 2012; and won the 8th IEEE Communications Society (ComSoc) Asia Pacific (AP) Outstanding Young Researcher Award, in 2013. Also, he received his first Ph.D. degree from Shanghai Jiao Tong University, China, in 2006. He is an IEEE Fellow. His research interests include applied cryptography, privacy enhancing technologies, and IoT-Big Data security and privacy. He has published extensively in his areas of expertise (with an H-index of 74 from Google Scholar as of January 2021), and was the recipient of nine best (student) paper awards from reputable journals and conferences. Currently, he serves as the Vice-Chair (Conferences) of IEEE ComSoc CIS-TC (Communications and Information Security Technical Committee). He is the winner of the 2016–17 Excellence in Teaching Award, FCS, UNB.