Security Technologies and Research Challenges on Microservice-Based NFV

Xiaochun Wu, Yuling Shen*, Junnan Zhang
Zhejiang Gongshang University, Hangzhou, China.

* Corresponding author: email: xylinglalala@163.com
Manuscript submitted April 6, 2020; accepted June 15, 2020.
doi: 10.17706/jsw.15.5.138-146

Abstract: In recent years, Network Function Virtualization (NFV) is an emerging key technology that has enabled network operators to change the way they build networks. The application of NFV improves the flexibility of the network and services, improves the operating efficiency, and reduces the operating costs. NFV reconstruction based on microservice architecture can speed up the software development cycle as well as decoupling software. This article first introduces the development process of NF from the physical equipment to the microservice based VNF. Then, we discuss the establishment of a trusted environment and the monitoring of the environment based on microservices which are the key security issues of NFV. Finally, we put forward some research challenges and future directions of NFV security based on microservices.

Key words: Microservice, network function virtualization, service chain, virtualized network function.

1. Introduction

Network function virtualization (NFV) offers a new way to replace expensive dedicated hardware appliances with generic servers that use software to design, deploy, and manage networking services. NFV enables operators, carriers and ISPs (Internet Service Providers), to quickly deploy new applications for customers by quickly provisioning supporting services compared with the three-to-six-month provisioning time for services. Nowadays, we are aware of the essence of NFV which a separation of functionality from capacity should be rather than an abstract of software function from hardware. Different services depended on deploying service chains can be easily chosen by the customers. An email application, for example, could require a service chain of the varying anti-virus, anti-malware, and anti-spam services; a VoIP application could add a traffic-shaping service to the mix while removing anti-spam services. What the service agility NFV technologies offered is the ability to launch and decommission services more rapidly and efficiently than before, with which a customer can turn it on or off much like a utility.

Despite the above advantages, there are still significant challenges and hurdles to the smooth using of an NFV-based solution especially in terms of a secure network service. Providing a secure network service is relying on a security control platform that not only needs to ensure the security of the physical and virtual operating environments but also prevents the illegal injection by sharing resources and unauthorized access. Meanwhile, the security of the service deployment transmission channel should be ensured, for fare of the information being stolen and tampered during the transmission. Therefore, a security control platform is the key part in security architecture, which has the same effect as the controller in Software Defined Networking (SDN) architecture. Security control platform usually performs all the security core functions (e.g., resource management, log analysis, network control and service orchestration).

From the view of telecommunications, Interaction between the Service Life Cycle Manager (SLM) in MANO frameworks and others (e.g., monitoring and resource Manager, resource Manager) in control platform is complex which is suitable for distributed systems implemented as microservices. Microservice is gaining increased adoption in the Telco NFV world. The project of SONATA is an example which implements the ETSI MANO architecture as microservices. The microservice-based architecture allows multiple organisations to work together autonomously to realize MANO framework functionalities. In [1], it proposes scalable mechanisms for fault recovery and high availability adding to a both centralised and distributed microservice-based implementation of the MANO framework architecture. However, as the core of the implementation of secure NFV, the direction of VNF deployment and security difficulty in the management and control platform need rethinking and analyzing. Unfortunately, there is still a lack of systematic summary of the security technologies of such management and control platform. Meanwhile, we found there are few papers focus on implementing the ETSI MANO architecture with microservices after reviewed the development trend, which motivates us to survey and summarize the current development of those solutions.

Accordingly, our main contributions in this work are summarized as follows:

- This article, for the first time, proposes secure risks related to Microservice-based NFV. Its latest development and challenges are discussed in detail.
- A summary of trust concerns and solutions in the literature is presented, enabling researchers to have decent knowledge about how to establish trust for microservice-based NFV service.
- In order to come up with an accurate strategy, we present various difficult issues for abnormal monitoring and enforcing correct behavior of microservices in VNF-based environments.
- Finally, we discuss security issue related to SFC creation and deployment.

2. Background

2.1. Overview of NFV Infrastructure

Nowadays, all organizations and researches are rethinking how to enhance the security management requirements in ETSI NFV, as the ETSI-NFV MANO working group has defined its Reference Architecture. One solution is to enhance or integrate security features into the framework of ETSI-NFV, and the other is to independently develop a secure application deployment system.

As is shown in Figure1, from architectural concept to deployment, such kind of Closed-loop lifecycle of NFV management and control is provided by all kinds of components such as Policy-driven Microservices orchestration, deployment and management of VNF, Monitor, Security analytics and events, trust access management and so on. Closed Loop Automation includes the service instantiation and delivery process. The orchestration management and control framework provide the automation of the configuration necessary for the resources at the appropriate locations in the network to ensure smooth operation of the service.

2.2. Overview of Microservice-Based NFV

The NF has experienced three historical stages, from the physical device to the virtual device, and then to the microservice based VNF. While early VNF deployments focus on how to implement the NFV correctly such as realizing a single VNF through monolithic VNFs. In recent years, some software development teams try to decompose a VNF into smaller functional blocks for the reusability and faster response time with no downtime or interruption to operational processes. as early as [2] FRESCO experimented with modular security and equipment reorganization, encapsulated the security functions of different vendors into a basic Security module, which utilizes scripting languages to combine simple and basic security actions,

providing sophisticated security functions. Therefore, it has validated the feasibility and benefits of security functionality decomposition and reorganization. The microservices architecture is a viable framework to segment NFVs with different particle sizes. [3] takes firewall as example, it is decomposed into multiple elements, which are classified and merged.

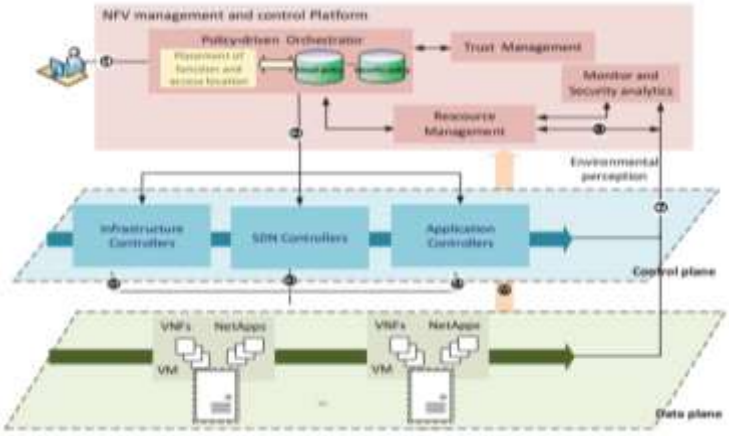

Fig. 1. Closed-loop lifecycle of NFV management and control.

These more flexible and lightweight architecture named microservices applied in NFV which means the traditional monolithic function can be broken into blocks of microservices. Although the architecture of microservices can solve the above problems faced by monolithic VNFs. The major drawback of microservices based NFV is same as the VNF deployment which is an important part of the complexity of a distributed system suffers from security vulnerabilities. For example, there are three problems as follows: 1) Microservices usually use REST mechanism as main data interchange formats, attention should be paid to providing security of the data transmission. 2)An additional challenge is to provide authentication mechanisms with third-party services and ensure that the sent data is securely stored. 3) Deploying microservices may also be complex as we need coordination among multiple services. Therefore, the microservices architecture pattern is implementing changes that span multiple services. Successfully deploying a microservice in VNFs requires greater control of deployment methods by developers, and a high level of automation. And maybe testing a microservice in VNFs is also unprecedented complex than before. It needs mechanisms to monitor and enforce the connections among microservices to confine the trust placed on individual microservices, limiting the potential damage if any microservice gets compromised. During the evolution from the monolithic architecture to the microservices architecture, the biggest problem is how to separate the microservices. The size of functional decomposition should be one of the key factors for better service delivery in the future.

3. Trust Concerns and Solutions

3.1. Establishing NFVI Platform Trust

The NFVI consists of hardware, operating systems, and virtualization layer. Infrastructure providers should keep confidentiality and auditability so that service providers can ensure secure data transmission and integrity [4]. Trust, meaning a known configuration, of the underlying NFV platforms, should begin with the trusted platform module (TPM), which is used as hardware root of trust. Boot integrity measurement to establish a set of common NFV attestation technologies as [5] shows. [6] develop a security extension for NFV orchestrator which are based on TOSCA data model. It implemented the security

extension based on Moon framework, which is an available platform for dynamic access control to cloud resources, the high level access policies can be automatically enforced to protect underlying NFV infrastructure.

In NFV infrastructure, VNFs can be deployed over a single VM or multiple VMs. In microservice-based NFV, microservice blocks are usually deployed on a single or multiple container. When service providers and developers deploy and execute microservices on infrastructure, it means that memory or CPU have to share resources, especially if microservices are not properly isolated from other microservices, which will inevitably cause security problems. Therefore, it is not only different NFS that needs memory isolation, but also different microservices need stronger memory isolation mechanism [7] to increase the security of NFV.

3.2. Establishing VNF Trust

Automated trust establishment among multi-VNFs when it is facing the situation of mutually non-trusting party and securely convey trust from platform to end users/subscribers in a virtualized environment is the basic security guarantee from trust management point of view. And establishing trust for microservice-based NFV service are far more complicated than before. After VNF is decomposed into smaller microservices, the communication between each microservice will become complex, and there will cause security problems such as bypass monitoring or malicious tampering. These security challenges are exacerbated by the extensive use of various communication channels between all VNFCs, creating more channels for data hijacks and interception while in transit [8]. Therefore, it is very necessary to establish mutual trust between microservices and encrypt all traffic in and out of microservices in a service function chain. In [9], the author believe that a secure communication tunnel can be built to protect the communication between each other, and an end-to-end encrypted tunnel can be set up to control the communication traffic.

3.3. Establishing Trust between VNF and NFVI

These operations include system attestation, verification of VNF image integrity before launch, as well as providing orchestration policies for binding VNFs to given NFVI elements. Such as [10] built an external trusted security orchestrator (TSecO) to perform VNF related security operations.

NFV supports multiple tenants , and VNFs is likely to be provided by different vendors, which may cause interoperability problems [11] and lead to infrastructure security vulnerabilities. For NFV security, ETSI introduces trusted computing. An important principle of trusted computing is identity authentication. Authentication data can consist of passwords, private keys, cryptographic certificates, tokens and other secrets. Software validation is a useful alternative. This verification includes checking the digital signatures of VNF modules from different vendors. To address privacy issues in authentication, authentication tokens need to be generated and authenticated in a multi-layered multi-tenant environment, as well as mechanisms for the exchange of identity attributes [12].

3.4. Solution

As we know, trust can be classified into identity-based trust and behavior-based trust from the access control perspective. Next, we will analyse the trust establishment methods for some identity-based trust and the behavior process in microservice-based NFV services.

1) Authentication and authorization: Underlying areas of concern in microservice-based NFV, new security issues when it comes to AAA platform certification, is that the current identity and accounting are not unique and spreading across more layers, such as the network infrastructure (identifying tenants) and network capabilities (identifying actual users). In end-to-end virtual network architectures (such as VNFaaS, VNPaaS, etc.), identity stacking can occur at multiple tiers,

any type of horizontal and vertical integration pattern needs to address identity-related issues. Microservice validation, which could be conducted both in isolation and in composition with other microservices, allows us to identify and mitigate potential vulnerabilities in the software, implementation, or interaction between microservices. Therefore, AAA mechanisms among vNFs, between vNFs and application layer and between vNFs and management stations should also be enforced to prevent threat injecting as insufficient vertical and horizontal VM AAA mechanism.

2) Bootstrapping a security trust model: There are some solutions show how to manage the trust chain and evaluate the trustworthiness of chain to minimize security risk of the network. A zero trust approach which is compatible with automated network service chaining microservice based ,would include authentication of not just users or applications, but would extend down to the level of authenticating individual packets. According to this way, network segmentation can be realized. Not only will an unauthorized request for access to the network be denied, but also any information about the nature of resources which are connected to the network will be denied.
3) Credibility model evaluation: As is mentioned above, many trust researches are based on a trusted third party (e.g., Certificate Authority) or out of band channel (e.g., add public keys in known hosts file). However, these kinds of methods are not fit for solving the problem of trust fundamentally in the NFV multi-party dynamic environment. There are still some challenges as follows: 1) Automate trust establishment among multi-party (e.g., VNFs), especially those are mutually non-trusting parties 2) Securely convey trust from platform to end users throughout its virtualized environment life cycle 3) Trust decision for an identity by any party is not publicly verifiable, hidden under one or more layers 4) Lack of tamper-proof evidence for any trust decision. A trust evaluation. criteria for microservice-based NFV should be proposed that a multiparty and dynamic trust environment for different kinds of actors such as virtual network function (VNF) provider, Infra-provider, Telecommunication Service provider and End users/subscribers who dynamically provide or consume services.

4. Monitor and Detect in Microservice Based NFV

4.1. Monitoring in Virtual Environments

To catch up dynamic traffic changes rapidly and adaptively, any security attacks such as malicious traffic require quick detection and effective measure to keep the managed network securely and safety.

In order to reduce the security threats in NFV, we usually choose to add security monitoring and detection mechanism into the framework. For example, the NFV Security Module (NSM) [13] is proposed in the literature to provide anomaly detection mechanism for NFV Orchestrator. The security monitoring service technology for NFV security architecture is provided in the literature [14]. The NFV security service controller transmits a security monitoring policy to the NFV security service agent and implements the security policy. Flowtap is proposed in the literature [15], which describes the monitoring function of each VM, and monitors and enforces all external and internal security sensitive network events.

In microservice-based NFV, IP addresses or NFs chain may frequently dynamic changes due to increasing security network features or adjusting VNF's optimized deployment. The method of creating a hard copy listing, as is the practice with static networks, may no longer be feasible. The deployment environments of NFV require a completely new methodology to gather telemetry for security monitoring. New resources and their associated security threat must be discovered by the monitor in order to generate appropriate security analytic trails.

4.2. Anomaly Detection Techniques for SFC

SFCs are vulnerable to many types of attack, such as unauthorized reconfiguration of VNFs (for denial of service or unauthorized privilege for specific users), flow redirection, and duplication. Deploying anomaly detection techniques for keeping the integrity of SFC becomes necessary to resilient to well-known and zero-day threats [16]. An additional SFC Integrity Module (SIM) for the standard NFV architecture is proposed which enables NFV orchestrators to analyze NFV elements and perform suggested actions with the goal of keeping service integrity in the network. Or to identify anomalies in the service chain by proposing anomaly detection methods, such as using Markov chains [17] to ensure that the VNF sequence is correct. Then observe the behavior of the entire VNF service chain through K-means classification.

5. Orchestration of Microservice-Based Security Service Chain Strategy

5.1. The Construction of SFC

Service chains are built by orchestrator, which deploy VNFs in a shared hosting infrastructure to generate complex network services [18]. This is a challenge for orchestrator.In the microservice-based NFV platform, the orchestrator can generate a security strategy according to the current requirement and construct the microservice module into a corresponding service graph.

Since the delay of the service chain may increase linearly with the length of the chain, when VNF is decoupled into multiple microservices, the length of the service chain will also increase, so the delay will become greater. Therefore, some researches focus on the processing of microservices. The common way is to improve the performance by merging or parallel microservice blocks. In OpenBox [19], the author chooses to merge multiple NFs into the same processing graph while preserving the correct processing order and results, and would like to reduce latency by reducing the number of blocks each packet traverses. NFP [20] attempts to construct high performance service graphs with parallel NFs, which requires the orchestrator to identify NF dependencies and automatically compile the NFP policy into high performance service graphs.

Since NFV supports multiple tenants, as the service chain grows linearly, multiple tenants are affected by each other and under greater risk of attack. When a microservice is attacked, in order to ensure that users' use is not influenced and the risk is reduced, the attacked microservice is usually replaced and restored in time, or the backup mechanism is adopted to switch links after the failure occurs quickly[21].

5.2. The Deployment of SFC

The service chain must be deployed in a trusted environment. In a virtual environment, multi-tenants share cloud infrastructure, which increases the possibility of attacks inside the cloud and expands the scope of danger. In this multi-tenant and multi-domain scenario, it is important to accurately define and locate failures to identify malicious agents that can damage the good behavior and quality of service of thousands of users at the same time. BSec-NFVO [22] provides secure services by ensuring the auditability of all operations in the service function chain. The literature [23] adopts an identity-based ordered multisignature scheme. Each VNF involved in the service chain needs to verify its signature on the received packet, and then the verifier can verify the signature and determine whether the security properties of concern for a particular service chain is well preserved.

Microservices run in containers, such as kubernetes, which is a very popular container orchestration tool. It can automatically complete container’s deployment, update, and monitoring tasks, using three steps of authentication, authorization and admission control to ensure security. Combining Kubernetes and the service mesh can compensate for the shortage of Kubernetes in microservice communication and help to restrict access to the application layer. For example, Istio is an open source application, it meets the diverse needs of microservices applications by providing behavioral insight and operational control for the entire

service mesh. In addition, it provides key functions such as traffic management, policy enforcement, service identity and security in the service network.

6. Conclusions and hints for Future Developments

In this article, we have discussed the security challenges of management and controls in microservice-based NFV environments. Although some research results have been proposed to overcome the security challenges in NFV, many potential security risks are still exist. In this section, we discuss some research challenges and future directions of microservice-based NFV security.

Secure data transmission: As a distributed system, microservices suffer from security vulnerabilities such as SOA. Microservices use REST mechanism and XML with JSON as main data-interchange formats, particular attention should be paid to providing security of the data being transferred.

Authentication mechanisms: An additional challenge is to provide authentication mechanisms with third-party services and ensure that the sent data is stored securely. Deploying microservices may be complex as we need coordination among multiple services, which may not be as straightforward as deploying in a container. Therefore, the granularity of microservices should be considered in future research. When the microservices orchestration is deployed, it also needs mechanisms to monitor and enforce the connections among microservices to confine the trust placed on individual microservices, and limit the potential damage if any microservice gets compromised.

Multi-management strategy: The coordination of microservices security strategies will be complicated by the multiple management. For example, who will be responsible for configuring and maintaining security credentials such as public and private keys? In addition, should the private key be allowed to be copied or redundant in the microservices-based NFV? Which kinds of security coordination mechanism can make the system more secure and reliable?

In this work, we investigate a comprehensive overview based on microservice-based NFV security architecture. We studied the art of state-of-the-art in development of NFV, presenting how NFV orchestration implement strategy based microservice to optimize virtual network functions service chain. We also analyse the risk of microservice-based VNF deployment and management environments. Furthermore, abnormal service chain detection, credible trust mechanism and Monitoring building in microservice-based NFV management and control are presented. Finally, promising research areas are illustrated, and future directions are presented.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This work is supported by the National Key Research and Development Program of China (2016YFB08001022017YFB0803205); Zhejiang Provincial Key Laboratory of New Network Standards and Technologies (NNST)(No.2013E10012); Zhejiang's Key Project of Research and Development Plan (No.2017C03058); the Key Research and Development Program of Zhejiang Province(2017C01064); the Fundamental Research Funds for the Central Universities2016XZZX001-04; the Natural Science Foundation of Zhejiang Province under grant number Y19F020021; the Natural Science Foundation of Zhejiang Province under grant number Y19F020031.

Reference

[1] Soenen, T., Tavernier, W., Colle, D., & Pickavet, M. (2017). Optimising microservice-based reliable NFV

management and orchestration architectures. *Proceedings of the 2017 9th International Workshop on Resilient Networks Design and Modeling* (pp. 1-7).

[2] Shin, S. *et al.* (2013). FRESCO: Modular composable security services for software-defined networks. *Internet Society NDSS*.

[3] Meng, Z., Bi, J., Wang, H., Sun, C., & Hu, H. (2019). MicroNF: An efficient framework for enabling modularized service chains in NFV. *IEEE Journal on Selected Areas in Communications*, *37(8)*, 1851-1865.

[4] Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: State-of-the-art and research challenges. *J. Internet Services Appl.*, *1(1)*, 7–18.

[5] Lal, S., Taleb, T., & Dutta, A. (2017). NFV: Security threats and best practices. *Proceedings of the IEEE Communications Magazine*, *55(8)*, 211-217.

[6] Montida, P., *et al.* (2017). A first step towards security extension for NFV orchestrator. *Proceedings of the ACM International Workshop on Security in Software Defined Networks and Network Function Virtualization* (pp. 25–30).

[7] Ni, Z., & Wood, T. (2018). Measuring performance and isolation tradeoffs for NFV. *Proceedings of the 2018 IEEE International Symposium on Local and Metropolitan Area Networks* (pp. 114-115).

[8] Hassan, H., Jammal, M., & Shami, A. (2019). Exploring microservices as the architecture of choice for network function virtualization platforms. *Proceedings of the IEEE Network*, *33(2)*, 202-210.

[9] Lal, S., Kalliola, A., Oliver, I., Ahola, K., & Taleb, T. (2017). Securing VNF communication in NFVI. *Proceedings of the 2017 IEEE Conference on Standards for Communications and Networking* (pp. 187-192).

[10] Ravidas, S., Lal, S., Oliver, I., & Hippelainen, L. (2017). Incorporating trust in NFV: Addressing the challenges. *Proceedings of the 2017 20th Conference on Innovations in Clouds, Internet and Networks* (pp. 87-91).

[11] Yang, W., & Fung, C. (2016). A survey on security in network functions virtualization. *Proceedings of the 2016 IEEE NetSoft Conference and Workshops* (pp. 15-19).

[12] Briscoe, B., *et al*. (2014). Network functions virtualisation (NFV) - NFV security: Problem statement. *White Paper*.

[13] Bondan, L., (2019). NFV environments security through anomaly detection. Ph.D. dissertation, Dept. Computadores. Eng., UFRGS Univ., Porto Alegre, Brazil.

[14] Sood, K., *et al*. (2017). Technologies for scalable security architecture of virtualized networks. U.S. Patent No. 9,560,078. 31.

[15] Sun, Y., Nanda, S., & Jaeger, T. (2015). Security-as-a-service for microservices-based cloud applications. *Proceedings of the 2015 IEEE 7th International Conference on Cloud Computing Technology and Science* (pp. 50-57).

[16] Bondany, L., Wauters, T., Volckaert, B., Turck, F. D., & Granville, L. Z. (2017). Anomaly detection framework for SFC integrity in NFV environments. *Proceedings of the 2017 IEEE Conference on Network Softwarization (NetSoft)* (pp. 1–5).

[17] Blaise, A., Wong, S., & Aghvami, A. H. (2018). Virtual network function service chaining anomaly detection. *Proceedings of the 2018 25th International Conference on Telecommunications* (pp. 411-415).

[18] Mechtri, M., Ghribi, C., Soualah, O., & Zeghlache, D. (2017). NFV orchestration framework addressing SFC challenges. *IEEE Communications Magazine*, *55(6)*, 16-23.

[19] Bremler-Barr, A., Harchol, Y., & Hay, D. (2016). OpenBox: A software-defined framework for developing, deploying, and managing network functions. *Proceedings of the ACM SIGCOMM Conf. (SIGCOMM)* (pp. 511–524).

[20] Sun, C., Bi, J., Zheng, Z., Yu, H., & Hu, H. (2017). NFP: Enabling network function parallelism in NFV. *Proceedings of the Conference of the ACM Special Interest Group on Data Communication* (pp. 43–56).

[21] Xu, S., Ji, X., & Liu, W. (2019). Enhancing the reliability of NFV with heterogeneous backup. *Proceedings of the 2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (pp. 923-927).

[22] Rebello, G. A. F., Alvarenga, I. D., Sanz, I. J., & Duarte, O. C. M. B. (2019). BSec-NFVO: A blockchain-based security for network function virtualization orchestration. *Proceedings of the IEEE International Conference on Communications*.

[23] Pattaranantakul, M., *et al*. (2019). Footprints: Ensuring trusted service function chaining in the world of SDN and NFV. *Proceedings of the International Conference on Security and Privacy in Communication Systems* (pp. 287-301).

Xiaochun Wu received the Ph.D. degree in computer science and technology from Zhejiang University, China in 2013. She had one year's visiting experience at the Department of Computer Science, Northwestern University, Evanston, IL, USA from 2017 to 2018. She is currently an associate professor with the School of Information and Electronic Engineering, Zhejiang Gongshang University, China. Her research interests include are forwarding and control element separation (ForCES), software-defined networking (SDN), network function virtualization (NFV), and network security.

Yuling Shen was born in 1996, she received the B.E. degree from Taizhou University, Taizhou, China, in 2018. She is currently pursuing the M.E. degree with Zhejiang Gongshang University. Her primary research interests are in the areas of network function virtualization and service chain.

Junnan Zhang was born in 1997, he received the B.E. degree from Zhejiang Shuren University, Hangzhou, China, in 2019. He is currently pursuing the M.E. degree with Zhejiang Gongshang University. He is current research interests include software defined network and internet security.