An Enhanced Security Framework of Software Defined Network Based on Attribute-based Encryption

Yue Shi, Fangfang Dai, Zhiguo Ye
Security Research Department
China Academy of Information and Communications Technology
Beijing, China

Abstract—**With the development of the information and communications technology, new network architecture and applications keep emerging promoted by cloud computing, big data, virtualization technology, etc. As a novel network architecture, Software Defined Network (SDN) realizes separation of the control plane and the data plane, thus controlling hardware by a software platform which is known as the central controller. Through that method SDN realizes the flexible deployment of network resources. In the process of the development and application of SDN, its open architecture has exposed more and more security problem, which triggers a critical focus on how to build a secure SDN. Based on the hierarchical SDN architecture and characteristics, this paper analyzes the security threats that SDN may face in the application layer, the control layer, the resource layer and the interface layer. In order to solve those security threats, the paper presents an SDN security architecture which can provide corresponding defense ability. The paper also puts forward an enhanced access control strategy adopting an attribute-based encryption method in the SDN security architecture.**

Keywords- software defined network; network security; security threats; fine-grained access control

I. INTRODUCTION

SDN has been intensively studied and widely applied in industry in recent years. In order to meet changing demands, SDN enables administrators to configure network resources quickly, and to adjust network-wide traffic flow dynamically [1]. However, with its rapid development, challenges start to emerge in implementing a full-scale carrier SDN. One of the most important challenges is SDN security.

The security problem of SDN has been researched recently. Jiang et al. [2-3] present a secure solution for SDN application based on virtualization technique. Wang et al. [4] analyzed the security model for SDN and summarized typical security issues. Huang et al. [5] analyzed threats of OpenFlow protocol and proposed related solutions. Shi et al. [6-7] analyzed the vulnerabilities and typical attacks of SDN based on its layered architecture.

It can be observed that most of the studies are about solving specific SDN security issues such as network monitoring, spoofing, DDoS attacks, etc. But a complete and unified security architecture of SDN has not been formed yet. This paper analyzes the main factors threatening the security of SDN. Moreover, the paper forms a complete SDN security architecture and adopts an attribute-based access control policy to meet difference security demands in various SDN application scenarios.

II. OVERVIEW OF SDN

A. Background of SDN

SDN originates from the Clean State Project of Stanford university [8-9], which is aimed at proposing new-concept network architectures to exceed the limit of traditional network frame by adopting new technologies, new applications and new services. SDN separates the control plane from the network hardware and runs it as software. A controller in SDN can facilitate automated network management, as well as integration and administration of applications and network services. In conclusion, more possibilities for planning, deploying and operating network are provided by SDN, which promotes the development of next generation network to a great extent [10].

The proposal of SDN has caused great attention of academia and industry. A variety of institutions and organizations join together to research SDN related standards and technology. One extraordinary work among them is present by the Open Networking Foundation (ONF). ONF proposed the OpenFlow protocol to define communication between control plane and data plane [11]. At present, OpenFlow has become the primary SDN communication interface and has been widely used in various network equipment.

This paper is sponsored by National Science Foundation of China No.61471129 and the National High-Tech Research and Development Program of China (863) No.2015AA016106.

978-1-5386-1107-4/17/$31.00 ©2017 IEEE

B. SDN Architecture

The academia and industry have present different architectures to meet all kinds of application scenarios and requirements. Among which, a widely accepted one is proposed by ONF. ONF divided SDN into application layer, control layer and resource layer, as depicted in Figure 1 [12].

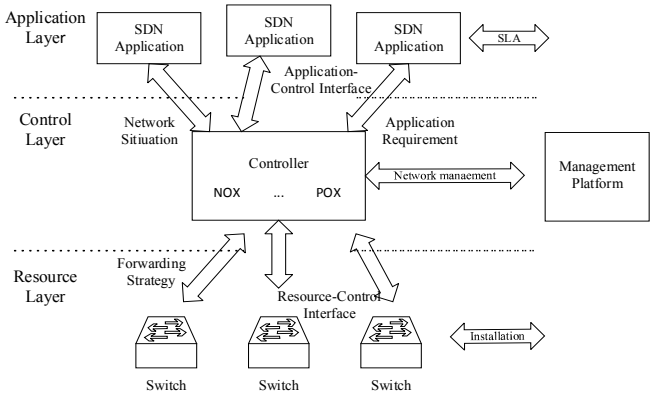

Figure 1. SDN Layered Architecture

- **Application layer:** where SDN applications specify network services or business applications by defining a service-aware behavior of network resources in a programmatic manner. Applications interact with SDN control layer via application-control interfaces to automatically customize the behavior and the properties of network resources [13].
- **Control layer:** provides a means to dynamically and deterministically control the behavior of network resources, as instructed by the application layer. SDN applications specify how network resources should be controlled and allocated, by interacting with the SDN control layer via application-control interfaces. The control signaling from SDN control layer to the network resources is then delivered via resource-control interfaces [13].
- **Resource layer:** where the network elements perform the transport and processing of data packets according to the decisions made by SDN control layer.
- **Application-control interface:** responsible for communication between application layer and control layer.
- **Resource-control interface:** responsible for communication between resource layer and control layer.

III. SDN SECURITY THREATS

Although SDN has developed rapidly, it also brings a series of security issues. Firstly, the net-openness makes SDN more transparent. Attackers would easily get more information about the network, services and policies. Secondly, with a centralized SDN controller, the impact of some attacks such as DoS can be higher than that directed against a single router. Finally, some new functional entities, protocols and interfaces can pose new security threats, such as OpenFlow protocol, application-control interface, resource-control interface, etc. This section analyzes the security threats of application layer, control layer and resource layer.

A. Application Layer Security Threats

Attackers could enforce a malicious network policy by manipulating applications, and that could impact the SDN control layer. The application layer security threats are list in Table I.

TABLE I. SECURITY THREATS OF APPLICATION LAYER

Security Threats	Description
Spoofing	An attacker could get the users' data or service logic and use them for future attack by disguising as a SDN controller
Repudiation	A user may deny the malicious network policy he had enforced, such as copying and forwarding specific traffic flows to a malicious server
Information disclosure	An attacker could disguise as a legitimate user to inject forged flows into network through SDN application
Application vulnerability	SDN application vulnerabilities such as code flaws and insecure code could be exploited by the attacker to access resources

B. Control Layer Security Threats

SDN controller is the core of the whole network and it must achieve the highest level of security, since a compromise of the SDN controller will lead to the disaster of the entire network. The application layer security threats are list in Table II.

TABLE II. SECURITY THREATS OF CONTROL LAYER

Security Threats	Description
Flow rules confliction	Malicious flows could bypass security detection, which conflicts with the preconfigured security policy and will adversely affect the SDN controller
Fake flow rule insertion	An attacker may send some fake flow rules by hijacking a SDN application
Spoofing	An attacker may disguise as an administrator or a SDN application to remove or modify sensitive data from the SDN controller or to obtain network topology information and routing information or even to have complete control of the SDN controller
DoS attack	An attacker could create spoofed traffic to conduct DoS attacks on the SDN controller to cause it to fail
Repudiation	An administrator or a SDN application may deny the malicious flow rules which he had inserted into the flow table
Operating system vulnerability	SDN controllers run on some form of operating systems (OS), then the vulnerabilities of the OS become vulnerabilities for the SDN controller. An attacker may exploit vulnerabilities of the operating system such as default passwords, back-door accounts, which will impact the SDN controller seriously

C. Resource Layer Security Threats

The resource layer security threats are list in Table III.

TABLE III. SECURITY THREATS OF RESOURCE LAYER

Security Threats	Description
Spoofing	An attacker may disguise as an administrator or a SDN controller to remove or modify sensitive data from the SDN switch or to obtain sensitive information such as flow entries in the flow table
Eavesdropping	An attacker may eavesdrop on flows between SDN switches to get the information about related flow, traffic and device
Flow table overflow	The flow table capacity bottleneck leads to potential flow table overflow
Repudiation	An administrator or a SDN controller may deny the incorrect configuration which he had made

IV. SDN SECURITY ARCHITECTURE

In order to deal with several SDN security threats, it is necessary to improve security defense ability of SDN. At present, there are two approaches to solve the issue, one is evolution, which improves the existing controller architecture, develops and deploys security modules to achieve the related security protection capability [14]. The other is revolution, which breaks the framework of existing controller, and develops a brand new SDN controller with internal security capacity [15-16].

A. Security Capacities of SDN

Based on the SDN security threats analyzed above, the security capacities to SDN application layer, control layer and resource layer is obtained, and the SDN security architecture is proposed in Figure 2.

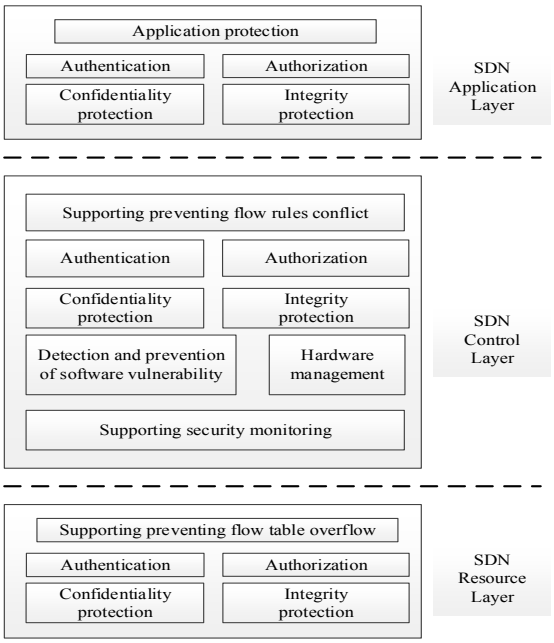

Figure 2. SDN Security Architecture

It can be observed that the security capacities of SDN can be separated into two categories: general capacities and specialized capabilities.

The general capacities are common to other targets and to traditional networking, including confidentiality protection, integrity protection, authentication and authorization.

- **Authentication:** the application layer, control layer and resource layer should authenticate each other to ensure authenticity of identity.
- **Authorization:** authorize user, application and controller to access system information, or manage network policies.
- **Confidentiality protection**: data stored in controller, or transportation over the communication interface should be performed confidentiality protection.
- **Integrity protection**: data stored in controller, or transportation over the communication interface should be performed integrity protection.

The new security threats, which caused by some new functional entities, protocols and interfaces according to the framework of SDN, as listed in Table IV.

TABLE IV. SPECIALIZED CAPACITIES OF SDN

	Security Capacities
Application Layer	Application layer should be able to defend against application vulnerabilities
Control Layer	a) Control layer should be able to prevent flow rules confliction in order to avoid mandatory network policies from being bypassed b) Control layer should be able to detect and prevent software vulnerability c) Control layer should be able to support the anti-DoS protection d) Control layer should be able to support hardware management to discover hardware failure automatically
Resource Layer	Resource layer should be able to prevent flow table overflow

B. Fine-grained SDN access control mechanism

As mentioned above, existing SDN security mechanisms have not implemented access control distinctly to different user, applications, controllers and switches. Therefore, based on the security capacities of SDN, this section proposes a fine-grained SDN access control mechanism to support a flexible and extensible access control strategy, and to achieve data confidentiality.

1) Attribute-based Encryption

The entities of attribute-based encryption include authority, access subject and access object. Traditional attribute-based encryption controls access subject by threshold, which only supports simple threshold strategy which takes the attribute as action object. That method cannot flexibly configure the value of attribute such as “and”, “or”, “nor” based on actual needs. Therefore, this paper uses the tree-structure attributed-based encryption to achieve the fine-grained SDN access control. The key steps are as follows:

a) Setup(): authority generates the public key PK and the master key MK;

b) keyGen(MK,Su): based on MK and access subject's attributes, authority generates the access subject's private key SK;

c) Encrypt(PK,M,T): based on PK,accessed resource M and access tree-structure T, access object generates ciphertext C;

d) Decrypt(C,SK): when the access subject's attributes meet the access tree-structure T, access subject uses SK to decrypt C to get accessed resourec M.

The above steps are shown in Figure 3.

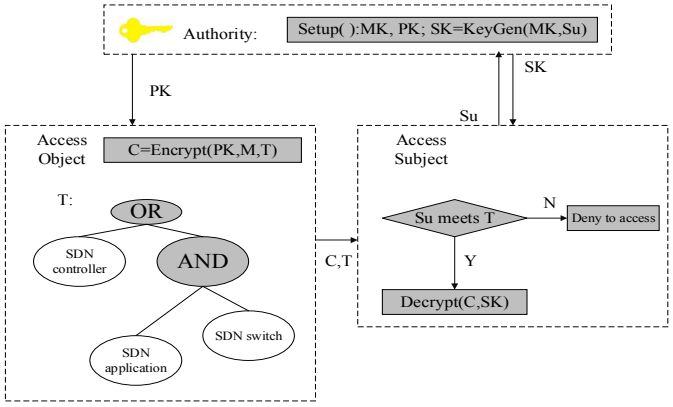

Figure 3. SDN Access Control Scheme based on Attribute-based

2) Attribute-based Encryption

According to the typical use cases and security requirements, the access control strategy can be defined as {position, action, priority}:

a) Position: the access subject who has initiated an access requirement ;

b) Action: action takes the form of tree-structure to define the access behavior of application, controller and switch, as shown in Figure 4;

c) Priority: according to the user's security permission, defining the priority as L4, L3, L2 and L1. L4 is the highest priority, represents the security administrator; L3 represents the normal administratorl; L2 represents the user; L1 represents the guest.

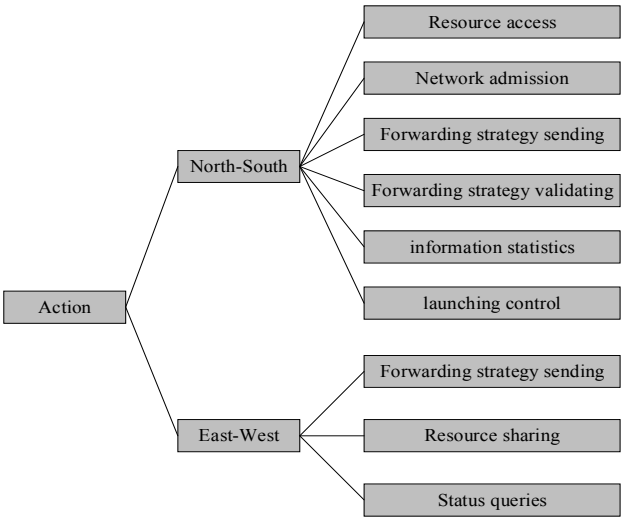

Figure 4. The Tree-structure of Access Behavior

3) Access control mechanism based on attribute-based

In conclusion, this paper constructs an access control mechanism for SDN based on attribute-based encryption as shown in Figure 5. The mechanism is composed of four components: the Trusted Center (TC), the Attributed Center (AC), the Access Subject (AS) and the Access Object (AO).

a) TC: a trusted server manage the identity of AS and AC without participating any action of access control*;*

b) AC: based on the network size and the service sitiuation, it could flexible set single AC or multi AC to manage the attribute of AS, and generate the private key for AS;

c) AS: it could be allowed to access the resource when the attribute of AS meets the tree-structure;

d) AO: define the access strategy of the resources and data which on the AO, and encrypt the related resource and data by the attributed-based method,

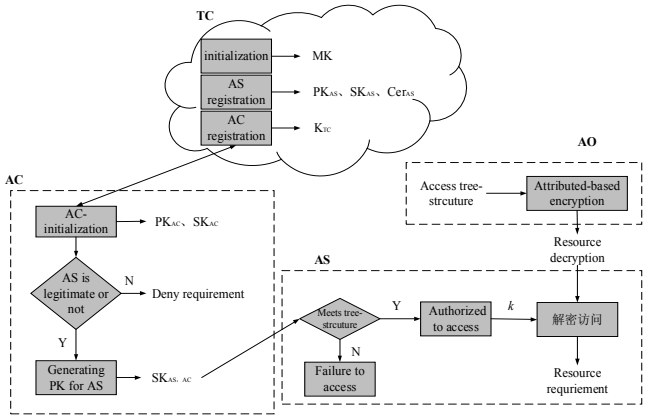

Figure 5. Access control mechanism based on attribute-based encryption

V. CONCLUSION

At present, SDN has developed from labs to field and has caused a lot of attention in academia and industry. A series of standards and technologies about SDN have been researched. However, the SDN security studies are still at an early stage. This paper introduced the background of SDN firstly, and analyzed the layered architecture of SDN. Based on that, this paper studied the security threats of SDN application layer, control layer and resource layer, and proposed a complete security architecture of SDN. After that this paper proposed the security capacities of SDN to improve the security protection ability.

ACKNOWLEDGMENT

The first author would like to thank Dr. Nan Meng and Dr. Tao Cui for proofreading and improving this manuscript. The authors are grateful to the reviewers for their detailed reviews and constructive comments.

REFERENCES

[1] ZHANG Chao-Kun, CUI Yong, TANG He-Yi, WU Jian-Ping. State-of-the-Art Survey on Software-Defined Networking. Journal of Software, 2015, 26(1): 62-81

[2] "Software-Defined Networking (SDN) Definition", Open Networking Foundation

[3] S. A. Mehdi, J. Khalid, and S. A. Khayam, "Revisiting traffic anomaly detection using software defined networking," in Recent Advances in Intrusion Detection. Springer, 2011, pp. 161-180

[4] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in IEEE 35th Conference on Local Computer Networks (LCN). IEEE, 2010, pp. 408-415.

[5] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyson, "FRESCO: Modular composable security services for software-defined networks," in Proceedings of Network and Distributed Security Symposium, 2013.

[6] D. Kreutz, F. Ramos and P. Verissimo, "Towards secure and dependable software-defined networks", in Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking. ACM, 2013, pp. 50-60.

[7] Casado, Garfinkel, Akella A, etc. “SANE : A protection architecture for enterprise networks. ” in Proc. of the 15th Conf. on USENIX Security Syrup. Berkeley : USENIX Association. 2006, 1-15.

[8] Yang M, Li Y, Jin D, Su L, etc. “OpenRAN: A software defined ran architecture via virtualization”, in Proceedings of the ACM SIGCOMM 2013 Cont. on SIGCOMM. Hong Kong: ACM, 2013, pp.549-550.

[9] P. Porras, S. Shin, V. Yegneswaran, M. Fong, M. Tyson, and G. Gu, “A security enforcement kernel for OpenFlow networks”, in Proceedings of the first workshop on Hot topics in software defined networks. ACM, 2012, pp. 121-126.

[10] Porras P, Cheung S, Fong M, etc. “Securing the software defined network control layer”, in Proceedings of the 2015 Annual Network and Distributed System Security Symp (NDSS 2015). San Diego: Internet Society, 2015, pp.1-15.

[11] Mousavi S, ST-hilaire M, “Early detection of DDoS attacks against SDN controllers”, in Proceedings of the 2015 International Conference on Computing, Networking and Communications(ICNC), 2015, PP.77-81.

[12] Software-Defined Networking: The New Norm for Networks, ONF white paper, Open Networking Foundation, April 2012.

[13] ITU-T X.1038 Security requirements and reference architecture of software-defined networking, Telecommunication Standardization Sector of ITU. ITU-T, 2017.

[14] Peng Shuping, Guo Bingli, Shu Yi, ete. “Software-Defined Optical Data Centre Networks,” China Communications, vol 12. 1-9, August 2015.

[15] Jin D, Nicol M, “Parallel simulation of software defined networks. ” in Proc of the 2013 ACM SIGSIM Conf. on Principles of Advanced Discrete Simulation. ACM，2013. 91—102

[16] Liu L, Casellas R, etc. “OpenSlice: An OpenFlow-Based Control Plane for Spectrum Sliced Elastic Optical Path Networks”, Optics Express, vol 21.4194-4204, 2013.