TEST Engineering & Management

January-February 2020
ISSN: 0193-4120 Page No. 15848 - 15853

Data Hiding based PKI Authentication Protocol in SDN

Sugandhi Midha, Asst. Prof. Computer Science Engineering, Chandigarh University Mohali, India,
Priya Batta, Computer Science Engineering, Chandigarh University Mohali, India
Khushboo Tripathi, Computer Science Engineering, Chandigarh University Mohali, India

Article Info
Volume 82
Page Number: 15848 - 15853
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 February 2020*

Abstract:
Software Defined Network (SDN) is a potential solution to classical network problems like binding all the three network planes like Data plane, Control plane and Management plane into one device. This gives rise to a huge problem of vendors' lock-ins who tie up networking protocols specific to machine which makes interoperability a big issue. Lack of modularity in the routing protocols where routing code is embedded into network topology code and change in infrastructure becomes difficult is one of the various factors that motivated the development of SDN. Security in SDN is completely different from security in the old networks. In this paper, we assess how host authentication is badly affected on machines on Software Defined Networks. Moreover, this paper also defines how authentication has been hampered and what the various authentication protocols are and how we can try to identify a hacker. In the nutshell, our paper presents the various challenges, problem in deploying various authentication protocols and how we can move ahead with secure deployment.

Keywords: *Host Authentication, Security, Open Flow, Data Plane, Control Plane, Management Plane, Abstraction, Public Key Infrastructure (PKI)*

INTRODUCTION

SDN addresses the issue of TCP/IP suite which uses IP addresses along with the domain names for hosts' communication over internet [1]. It works well if we are working with stationary host but mobile IP where hosts keep on shifting from one network to another, has serious limitations. SDN has evolved to cater the issue by decoupling all the 3 network planes. For the same reason, security becomes lot more different inSDN as it was in classical networks. To identify who have the access and who is permissible to enter our machine, various protocols have been laid down. To catch a thief, we need to think like a thief. Our protocol tries to identify the hackers. The 3 basic properties of a secure communication are confidentiality, integrity and availability are supported by the techniques authorization, authentication and encryption. We are trying to focus on issue of integrity to be implemented via authentication protocol.

As the name specifies, SDN is programmable network paradigm. Here, Network is not controlled by the hardware but the separation of 3 planes allows software applications to program network devices individually. Logically, there is a centralized control of the network. The disassociation of planes reduces network complexity and enables faster innovations.

SDN follows open structure, standardized protocol and new technological adoptions are according to user needs as there is no vendor monopoly. SDN uses APIs to configure as per need in contrast toprotocols of traditional networks. SDN follows open structure and standardized protocol and new technological

January-February 2020
ISSN: 0193-4120 Page No. 15848 - 15853

adoptions are according to user needs as there are no vendormonopoly.

SDN SecurityTerminology:

a) SDN Distributed Denial of Service (DDoS):- When Servers do not provide the required service to users. SDN provides us with new opportunity to deal with DDoS attack.
b) Authentication:- A process which confirms whether the claimed identity correct ornot.
c) Availability:-Ensuring that correct and timely information is available to the authorizedparties.
d) Confidentiality:-Maintaining the privacy and secrecy of information to the authorized parties.
e) Integrity:- Ensuring trust worthiness of information resources[2].
f) Reference Data: - Data Objects which are referred for the securitycontrol.

The rest of the paper is organized as follows. Section 2 of this paper highlights SDN layers and architecture. Section 3 of this paper discusses SDN machine authentication attacks. Section 4 depicts the security architecture of SDN. Section 5 proposes a new way to maintain authentication in SDN. Section 6 of this paper concludes how authenticity is obtained and what are the benefits which are achieved with the proposed protocol.

A. II SDN Architecture

Old way of configuring a network device is where application and OS are configured on forwarding hardware of billions of gates. It works as a closed equipment where software is bundled with hardware and we are provided with vendor specific interfaces. Many complex functions like OSPF, BGP, multicast traffic engineering, routing schemes are baked into infrastructure. An idea of SDN is to separate Control Programs, Network OS and packet forwarding hardware so that innovations canbemade easily and quickly & vendor monopolies can be vanished. SDN is not open flow but a concept of physical separation of data plane, control plane and management plane. Open flow is an interface between these planes of SDN architecture. Open flow can be thought of as a protocol that is used in forwarding devices and interfaces.

2.1SDNPlanes

Structure should be known before working on it and protecting it. Figure 1 [3] depicts various SDN planes and its components.

a) Data Plane or Forwarding Plane:-is the collection of simple resources (port or a queue) or complex resources (multiple resources like a network device) responsible for forwarding traffic. Data Plane comprises of South Bound interfaces and Network infrastructure. It is a firmware (e.g. Open VSwitch) responsible for handling instructions from the control plane via flow tables.
b) Control Plane:-comprises of Northbound interfaces, Network Operating System & Network Hypervisor. It makes decisions and lay down instructions for data plane. It is virtualized networkmodel.
c) Management Plane or Application Plane:- comprises of network applications, programming languages & language based virtualization. The plane is responsible for routing, load balancing, security etc.

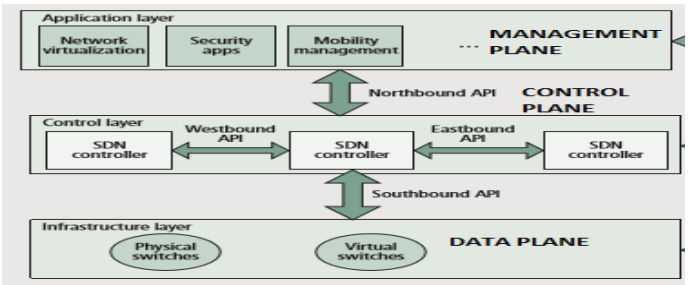

Fig. 1. SDN Planes [19]

Figure 2 [4] depicts SDN layers and its architecture.

January-February 2020
ISSN: 0193-4120 Page No. 15848 - 15853

SDN architecture can be summarized as a separation between a controlled and controller entity. It plays a vital role with the help of which controller manipulates controlled entity. North bound API is to management plane or application plane. It is an open issue and no standardization has been done. It is software based eco system. Southbound API is to control plane & is for handling instructions from control plane.

SDN AbstractionLayers

Moreover, this paper targets four abstraction layers:-

d) Data Abstraction Layer (DAL):- hides the resources of forwarding plane to control and managementplane.

e) Control Abstraction Layer (CAL):- abstracts the control plane southbound APIs from the Application Layer.

f) Management Abstraction Layer (MAL):- abstracts the Management Plane Southbound API from ApplicationLayer.

g) Network Services Abstraction Layer (NSAL):- provides service abstractions for use by applications and other services[4].

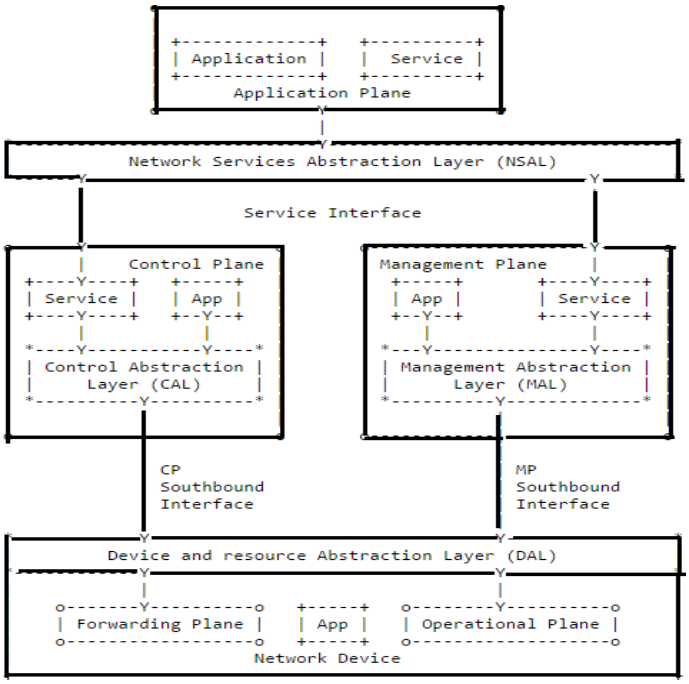

Fig. 2. SDN Layers and Architecture [4]

III *SDN AuthenticationAttacks*

3.1 Security Challenges

a) Trust Boundaries can be manipulated.

b) Conflicting rules in flow tables.

c) Manipulation in forwarding loops

d) Attacks on Centralized Controller

e) Attack on Communication Medium

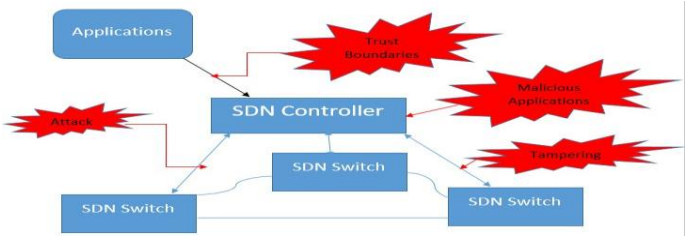

Fig 3. Security Challenges

3.2 *Security Attacks inSDN*

a) Denial of Service (DoS) Attack:- The malicious attacker will prevent the sending and receiving host from getting connected by flooding the packets on the network. When a switch constantly receive unknown packets which does not match the entries in the flow table, the packets are sent back to the controller. Figure 4 [5] explain the DoS attack process.

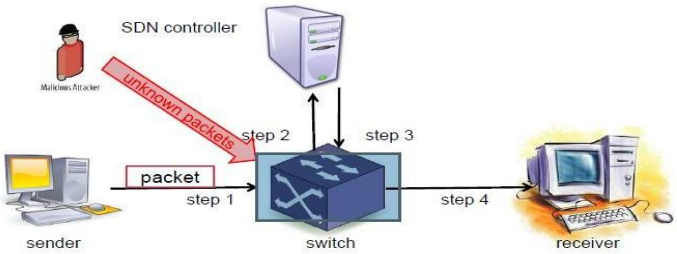

Fig 4. DoS Attack [5]

b) Man in the Middle Attack:-Malicious hacker can pretend to be a switch on network by facking its identity & may get connected to controller.

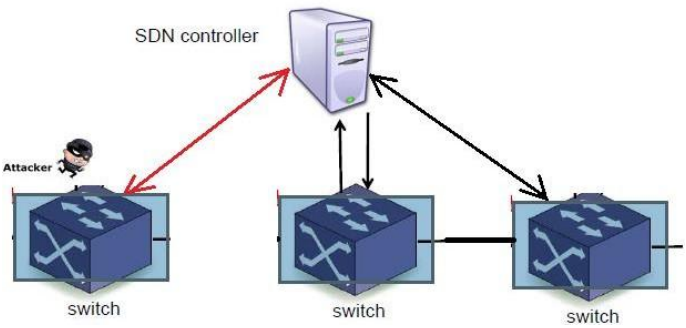

Fig 5. Man in the Middle Attack

January-February 2020
ISSN: 0193-4120 Page No. 15848 - 15853

c) Host impersonation attack: the attacker will receive packets intended to the victim and can reply to these packets on behalf of the victim[6].

IV *SDN Security Architecture*

Security Architecture of any machine is divided into three layers:

a) Local Security Authority (LSA): It acts as a securityguard.
b) Security Reference Manager (SRM): It acts as a security receptionist which is being contacted by the security guard and provide access on the basis of data in thedatabase.
c) Security Account Manager (SAM): It is a database containing all access privileges information.
d) SAM file lies in c:\windows\system32\config. The moment you start OS, the SAM file becomes inaccessible. In SAM file passwords are in the form of hash functions (H(k)) and one cannot check the password directly. H(k) is one way encryption, you cannot convert it back to the plain text. In general if user has little idea about the password length and type, there are many brute forcing techniques software available (like cain n abel) to break OS password. General steps of hacking are:

i) Foot Printing (Gaining more and more information abouttarget)
ii) Scanning (Identifying weakpoints)
iii) Gaining Access
iv) Maintaining Access
v) Tracking Access

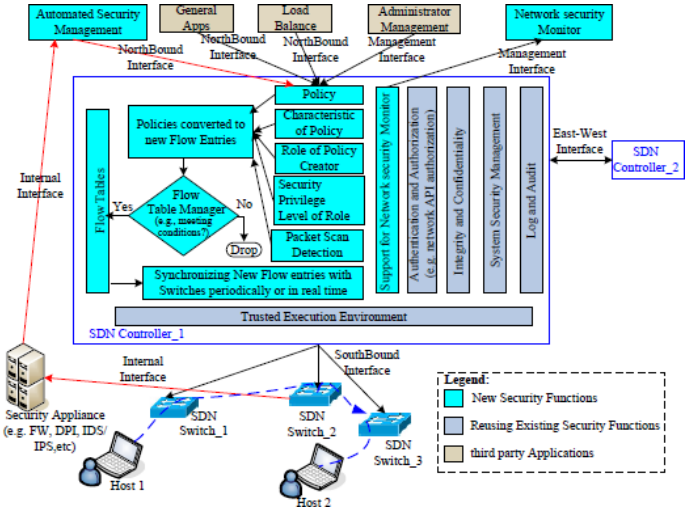

Fig 6. Comprehensive Security Architecture of SDN [7]

SDN contains mobile hosts so it becomes little cumbersome task to maintain the access of the system. But still there are many attacks as discussed in section 2 which are prone to SDN.

III *Data hidingbasedPKIAuthentication Protocol– TheProposedMechanism*

In the existing PKI based model, all key management is under the control of central administrator. Man in the middle attack becomes a bottleneck is this case.

A new mechanism is suggested where tenants in the network control the information related to its zone by themselves. They maintain all the PKIs related to its information zone. Refer to figure 7. But along with a PKI, an extra amount of information is added to this request-reply mechanism. This piece of extra information is hided under the request packet. This piece of covered writing is called steganography which is used in addition to cryptography for maintaining secured authentication process. This secret information works as an art and science for identification of genuine user.

January-February 2020
ISSN: 0193-4120 Page No. 15848 - 15853

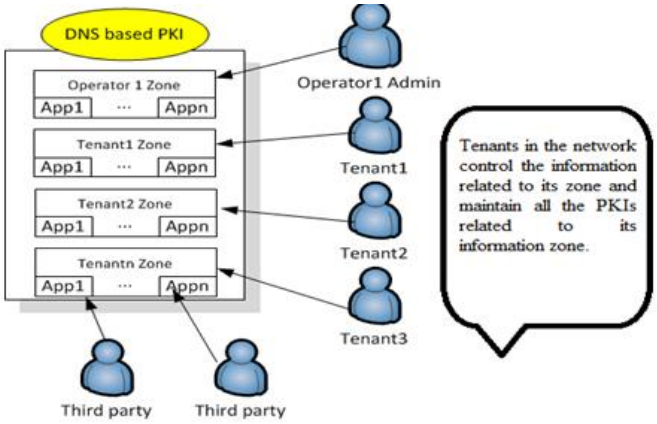

Fig. 7. Improved PKI Model

Our proposed algorithm follows the following steps:

Step 1: A 16 bit unique PKI is decided between the tenant and the third party.
Step 2: A 16 bit random sequence is selected.
Step 3: A XOR operation is performed with bits in the PKI and random sequence. The generated 16 bit sequence is then used as a watermark which is sent along with the requestedpacket.
Step 4: Generated ID along with the PKI is matched in the look up table of tenant to grant the access and to identify the authorized user.Figure 8 explain the complete process of our proposed authentication security protocol.

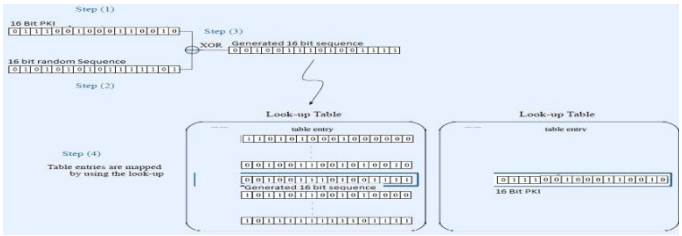

Fig. 8. An example of how data hiding based authentication PKI model works

V *Conclusion*

The proposed model reduces the scope of possible attacks on the central controller PKI servers. Multi tenancy and data hiding provide a secured authentication model for different services of SDN. Each tenant controls the authorization of its own resources where no dependency is on central controller provides a higher level solution to authentication problem. It is an addition to the cryptography and a mechanism which is supported by steganography. There is no need to maintain PKI servers. Maintenance of one DNS server is enough which reduces CapEx cost.

References:

1. I. Ahmad, S. Namal, M. Ylianttila, and A.Gurtov, “Analysis of Deployment Challenges of Host Identity Potocol”, IEEE2017.
2. noxrep. (2015, Jan.) POX: OpenFlow Controller. [Online]https://www.opennetworking.org/wp-content/uploads/2014/10/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf
3. Hengky “Hank” Susanto, Sing Lab, “Introduction to SDN”,
4. www.cse.ust.hk/~kaichen/courses/spring2015/comp6611/.../SDN-presentation.pptx
5. B. Heller, N. Handigol, V. Jeyakumar, N. McKeown,and D. Mazières. Where is the debugger for mySoftware-Defined Network? In HotSDN, August2012.
6. AdmelaJukan, Marcel Caria, Siquan Zhao, “Security in SDN”, in proceedings of IEEE conference in IEEE,2014.
7. [6]S. Son, S. Shin, V. Yegneswaran, P. Porras, and
8. G. Gu, "Model Checking Invariant Security Properties in OpenFlow." Available:http://faculty.cse.tamu.edu/guofei/paper/Flover-
9. ICC13.pdf
10. Zhiyuan Hu, Mingwen Wang, Xueqiang YAN, Yueming YIN, “A comprehensive security architecture for SDN”, in the IEEE proceedings of

January-February 2020
ISSN: 0193-4120 Page No. 15848 - 15853

18thinternational conference on Intelligence in Next Generation Networks, IEEE,2015.

11. I. Ahmad, S. Namal, M. Ylianttila, and A.Gurtov, “Security in softwaredefined networks: A survey,” IEEE Communications Surveys &Tutorials,2015.
12. S. Shin and G. Gu, “Attacking software-defined networks: A first feasibilitystudy,” in Proceedings of the second ACM SIGCOMM workshopon Hot topics in software defined networking. ACM, 2013, pp. 165–166.
13. 10] E. Al-Shaer and S. Al-Haj.Flowchecker: configuration analysis and verification of federated openflow infrastructures. In Proceedings of the 3rd ACM workshop on Assurable and Usable Security Configuration, 2010.
14. P.Porras,S.Shin,V.Yegneswaran,M.Fong,
15. 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.
16. S. Shin and G. Gu, "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," in 20th IEEE International Conference on Network Protocols (ICNP). IEEE, 2012, pp.1-6.
17. D. Kordalewski and R. Robere, “A dynamic algorithmfor loop detection in software defined networks,”2012.
18. A. Khurshid, W. Zhou, M. Caesar, and P. Godfrey,“Veriflow: Verifying network-wide invariants in realtime,” ACM SIGCOMM Computer Communication Review,vol. 42, no. 4, pp. 467–472, 2012.
19. H. Yang and S. S. Lam, “Real-time verification of networkproperties using atomic predicates,” in ICNP, theIEEE International Conference on Network Protocols,2013.
20. Z. Hu and J. Luo, “Cracking network monitoring inDCNs with SDN,” in 2015 IEEE Conference on ComputerCommunications, INFOCOM 2015, Hong Kong, China,April 26 - May 1, 2015, 2015, pp. 199– 207.
21. F. Chen, B. Bruhadeshwar, and A. X. Liu, “Privacypreservingcross-domain network reachability quantification,”in Network Protocols (ICNP), 2011 19th IEEEInternational Conference on. IEEE, 2011, pp.155–164.
22. M. J. Freedman, K. Nissim, and B. Pinkas, “Efficientprivate matching and set intersection,” in Advances inCryptology-EUROCRYPT 2004. Springer, 2004, pp.1–19.
23. Qioa Yan and F. Richard Yu, “Distributed Denial of Services Attacks in Software Defined Networking with Cloud Computing”, in IEEE Communications Magazine, April2005.
24. Sunil Kumar Muttoo, ShikhaBadhani, “Android Malware Detection: State of the Art”, Springer InternationalINDIACom17.
25. GautamiTripathi, Mohd. Abdul, “Impact of Excessive use of Internet in Cognitive Development of Youngsters”, Springer International INDIACom17.