Security of Software Defined Networks: Taxonomic Modeling, Key Components and Open research area

Ramanpreet Kaur, Amardeep Singh, Sharanjit Singh, Shruti Sharma

Dept. of Computer Science and Electronic Engineering

G.N.D.U Amritsar, India

Email: ramangill091@gmail.com

Abstract

Software defined networking promises network operators to dramatically simplify network management. It provides flexibility and innovation through network programmability. With SDN, network management moves from codifying functionality in terms of low-level device configuration to building software that facilitates network management and debugging[1]. SDN provides new techniques to solve long-standing problems in networking like routing by separating the complexity of state distribution from network specification. Despite all the hype surrounding SDNs, exploiting its full potential is demanding. Security is still the major issue and a striking challenge that reduces the growth of SDNs. Moreover the introduction of various architectural components and up cycling of novel entities of SDN poses new security issues and threats. SDN is considered as major target for digital threats and cyber-attacks[2] and have more devastating effects than simple networks. Initial SDN design doesn't considered security as its part; therefore, it must be raised on the agenda. This article discusses the security solutions proposed to secure SDNs. We categorize the security solutions in the article by presenting a thematic taxonomy based on SDN architectural layers/interfaces[3], security measures and goals, simulation framework. Moreover, the literature also points out the possible attacks[2] targeting different layers/interfaces of SDNs. For securing SDNs, the potential requirements and their key enablers are also identified and presented. Also, the articles sketch the design of secure and dependable SDNs. At last, we discuss open issues and challenges of SDN security that may be rated appropriate to be handled by professionals and researchers in the future.

KEYWORDS: SDN Architecture, FRESCO, FORTNOX, Cloud Watcher, L-IDs

I. INTRODUCTION

The appearance of the software defined networking (SDN) model has created great potential and hope to beat out the need for flexible, secure, reliable, and well managed next- generation networks. The extremist concept of SDN has brought radical change to the traditional vertical integration of the network by separating the forwarding hardware (data plane) from the control well managed next- generation networks. The extremist concept of SDN has brought radical change to the traditional vertical integration of the network by separating the forwarding hardware (data plane) from the control logic of the network (control plane).Subsequently, just the switches and routers are used for forwarding the traffic; however, the control functionality is simply managed by the centralized logical controller[4]. Control logic of SDN is moving to an external entity known as an SDN controller provides an abstract view of the underlying network resources to achieve smooth facilitation for the programs of forwarding hardware. Moreover, the abstraction of flow broadly unifies the behavior of different SDN agents. Obviously, these remarkable features of SDN provide with more flexible, innovative, programmable, evolvable, vendor-agnostic and cost-effective, network architecture. In spite of all these exciting features, industry observers/developers are worried about the security of SDNs. The security of SDNs is still considered the open issue, and a key concern, topmost priority and an equally striking challenge have recently begun to receive the attention they deserve. Besides, the architecture of SDNs raises new external and internal threats and vulnerabilities. Generally, the integrity and security of SDNs remain unproven when the point comes that management functionality is handled by a single centralized virtual server. Subsequently, It becomes the primary potential attack target when the whole network is compromising through a single point. The programmability aspect of SDNs leads attackers more vulnerable to a number of malicious code exploits and attacks. Further- more, the abstraction of different available flows and underlying hardware resources at the SDN controller significantly supports harvesting intelligence from the existing resources. After-ward, it can be effortlessly used for further attacks, exploitations, and particularly reprogramming the entire network. Likewise, the southbound interface (between data plane and control plane) of an SDN can also easily be targeted with diverse denial of service and side channel attacks. Equally important, configuration errors of SDNs can have more serious consequences than in traditional networks. Besides, SDN agents can also potentially be targeted for injecting false flows. By keeping eye on the features and architecture of SDN, it is proved that cyber attacks launched by SDN have even more annihilating effects than simple networks. Initial SDN design does not include security as its part, even each SDN layer/interface has its own security concerns, requirements, issues .Although, security must be delivered as service for all connected resources ensuring integrity and privacy. Security and dependability is still far away from SDN architecture, according to some researchers. Oppositely, it is complementary to state that security can be effectively enhanced and implemented by SDN; meanwhile, security becomes top most priority in SDN.

Following are some contributions of this article regarding SDN security:

1. The various possible attacks are highlighted effecting different layers/interfaces.
2. The approved security solutions are identified according to different category.
3. For secure and dependable SDN, the key components are also identified.
4. Taxonomic modeling on classification of different security solutions on the basis of layers/interfaces, security objectives, security mechanisms, simulation environments.
5. At last, open research area for security researchers are given.

II. SDN ARCHITECTURE (LAYERED AND SIMPLIFIED) :

This section provides with the layered architecture[4] of SDN which is simplified. This view of architecture helps the readers to understand the security concerns with respect to architecture of SDN. With the separation of control plane from data plane that lays the ground to SDN networking paradigm.

In SDN network switches become useful for forwarding purposes and control logic is implemented in logically centralized controller. Programming ability is provided on the control plane.

The simplified view of SDN consists of three major layers with their corresponding interfaces:

The top most layer is application layer (Application plane) provides several services and applications like access controls, intrusion detection and prevention system (IDS/IPS)[5], WAN optimization, load balancers.

The next layer is control layer (Control plane) of SDN which consists the controller. Controller is basically a software platform, known as brain of SDN model. The management functionality is the responsibility of controller that provides paths and flows in SDN.

The data layer (Data plane) is also known as infrastructure layer. This layer provides with hardware components used for forwarding like switches and routers. This layer helps the control layer by implementing the management functionality of controller by enabled switches to forward packets, collect the network information and send it to the control layer.

Both the interfaces of SDN are application programming interfaces (API). The Southbound interface enables communication between control layer and data layer, whereas northbound provides link between infrastructure and application layer.

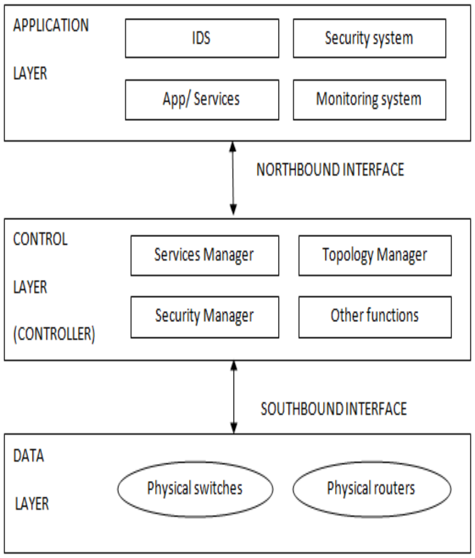

Figure1: Layered Architecture of SDN

III. POSSIBLE SECURITY ATTACKS/ISSUES

There are various types of attacks[2] affecting the security of SDN. As shown in table layers/interfaces are targets for particular attacks. These all issues disturb the overall security of SDN. Authorization related attacks taken place by unauthorized access to controller which affect the control and data layer as well as southbound interface. Unauthenticated applications are also unauthorized access and can harm upper three layers. Data leakage can be done by Side channel attack. Input buffers affect the data layer and can discover paths and flow rules. Forward policy can be discovered by packet processing timing analysis. Data can also be modified by Flow rule modification. Malicious injection attacks used by attacker to introduce code into a vulnerable computer program and change the course of execution. The result of successful code injection is often disastrous. Controller hijacking and fraudulent rule Insertion attacks are types of malicious applications. DOS (Denial of services) are related to availability related attacks. Type of DOS attack is Controller-Switch Communication Flood between the switch and the main controller. Another major DoS attack is Switch flow table flooding corresponds to flooding attack and effects the data layer of SDN. There are also some configuration issues ,due to lack of TLS or other Authentication techniques lower layers are badly effected , whereas Policy enforcement issues effect application and control layer and northbound interface.

IV. CATEGORIZATION OF SECURITY SOLUTIONS:

This section represents classification of security solutions. The literature presents that SDN is not mature (secure) enough. The article shows 2 trends exist in research. First trend is more curious about security of SDN, Other deals with enhancement of security using SDN.

A. Secure Composition: There are two solutions worked on security of design of SDN. These are:

1..FRESCO: Shin et al, P.A.Porras works on this phase. He proposes FRESCO[6] which has major contribution towards secure programming. It also has great impact on all layers and interfaces except data layer. It is an OpenFlow[3] security application. It is intended to address various key issues that can accelerate the design of new SDN enabled security services. It also exports a scripting API that enable security experts to code security monitoring and threat detection logic as modular libraries.

2. FORTNOX: Fortnox[2] is a new security policy enforcement kernel. It deals with authorization and rule conflicts and has direct impact on both interfaces and control layer.

B. *Security Audit*: There are two types of proposals in it:

1. VERIFICARE: R. Skowyra et al. gives model that satisfies design requirements. This proposal as the name suggests works as verification platform that verify network correctness and specification modeling.

2. SDN DEBUGGER: SDN debugger helps the researchers to find out the root cause of bug. It capture and reconstruct the sequence of events leading to the errant behavior. Debugger helps the researchers in solving logical errors and helps network operators in collecting bug reports then submit it to vendors.

Security Attacks/Issues	SDN layer Affected				
	Application layer	Northbound layer	Control layer	Southbound layer	Data layer
Unauthorized Access					
Unauthorized controller access	N	N	Y	Y	Y
Unauthenticated application	Y	Y	Y	N	N
Data Leakage					
Flow Rule Discovery(Side channel attack on Input Buffer)	N	N	N	N	Y
Forwarding Policy Discovery(Packet Processing Timing Analysis)	N	N	N	N	Y
Data Modification					
Flow Rule Modification to Modify packets	N	N	Y	Y	Y
Malicious Applications					
Fraudulent Rule Insertion	Y	Y	Y	N	N
Controller Hijacking	N	N	Y	Y	Y
Denial of Services					
Controller-Switch Communication Flood	N	N	Y	Y	Y
Switch Flow Table Flooding	N	N	N	N	Y
Configuration Issues					
Lack of TLS(Authentication Technique)Adoption	N	N	Y	Y	Y
Policy Enforcement	Y	Y	Y	N	N

Fig ure2: Table showing different attacks on each layer/interface

*C. Security enforcement policy***:** This section deals with 3 different recommended solutions:

1. VERIFLOW: Veriflow[6] basically verifies the network-wide invariants in real time. It is a layer between a SDN controller and network devices that checks the real time invariants violations dynamically as each forwarding rule is inserted modified and deleted.

2. FLOVER: Flover[6] proposed by Son.et al is basically a checking model that determines and verify flow policies against the network security policy. It facilitating design of sophisticated threat detection and mitigation modules.

3. *Perm OF:* Third proposal is Perm-OF, a fine grained permission system that consists of various OF-specific permissions. These are designed by considering the concepts like

a) Control messages in OpenFlow.

b) Application functional requirements

c) Threat vendor Model.

d) Isolation Mechanism

D. Security Enhancement: It includes 3 major concepts:

*1. FleXam***:** It is proposed by Sajad et al. FleXam is a sampling extension for OpenFlow that permit the Controller to define which packets should be sampled, what parts of each packet should be selected, and where they should be sent. FleXam enables the controller to dynamically adjust sampling rates, thus it reduces the control plane load.

2. CLOUDWATCHER: It is a new security monitoring service model that monitors clouds

CLOUDWATCHER[7] changes the routing paths for network traffic flows, and it makes the flows transmit through network nodes where security devices reside.

3. L-IDS: It is learning intrusion detection system (IDS).L-IDS is security service of mobile devices for their protection in a particular area or location.

E. Security Analysis:

1.OpenWatch: It is a program that takes as input different anomaly detection applications and decides what flows should be monitored.

*2.AVANT-GUARD***:** S. Shin et al. propose AVANT-GUARD[5] in SDN. It integrates two important techniques. First technique is a connection migration which significantly reduces data-to-control plane interactions which produces due to DOS attacks on the southbound interface. Another technique is an actuating trigger that addresses the responsiveness challenge by providing condition-triggered push capability in SDN devices.

*3.HEADER SPACE ANALYSIS***:** J.Wang et al. propose an approach to resolve problems and conflicts in an SDN firewall by checking firewall flow space and authorization space. Function of this approach is searching the flow paths in the whole network and determines the flow paths against all firewall deny rules for determining the issue. The effectiveness of this approach is examined by header space analysis.

V. KEY COMPONENTS FOR SDN SECURITY:

For a secure SDN, it is necessary to ensure the security of each and every components of SDN. But some of the important requirements are given below which ensures secure SDN. These requirements are:

*A. Securing the control layer (SDN controller***):** Control layer is middle layer of SDN that contains the controller of SDN. Controller is known as brain of SDN or central decision point where all the functionalities take place. Controller is famous for overall management of network. Being as a central point, controller is attack-target of interest to hackers. It is considered a single point of failure and high value target for bad actors. Potential attackers can try to get control of the network, pretending to be SDN controller or just break into the controller itself. There are several types of DDoS attacks trying to exploit potential sealing limits of SDN infrastructure. To secure the SDN controller, strong access control is required, DDoS protection, anti-virus and other threat

Categorization of security solutions	Approved solutions	SDN layers/interfaces				
		Application layer	Northbound interface	Control layer	Southbound interface	Data layer
Design security	FRESCO	Y	Y	Y	Y	N
	Fortnox	N	Y	Y	Y	N
Satisfactory audit	Verificare	N	Y	Y	Y	Y
	SDN debugger	Y	N	N	Y	N
Enforcement of security policy	Veriflow	Y	Y	Y	Y	N
	Perm OF	Y	Y	Y	Y	N
	FLOVER	Y	Y	Y	Y	N
Security enhancement	FleXam	Y	N	Y	Y	Y
	CloudWatcher	Y	Y	Y	Y	N
	L-IDS	Y	N	Y	Y	Y
Analysis of security	AVANT-GUARD	N	N	Y	Y	Y
	Open Watch	Y	N	Y	Y	Y
	Header Space analysis	Y	N	Y	Y	Y

Figure3: Categorization of Security Solutions

prevention and detection, mitigation techniques are needed.

B. Securing traffic flow: SDN ensuring the end-to-end communication .SDN is based on intelligent forwarding traffic flow. It is major part of SDN functioning, so it must be secured. A successful injection of fraudulent flow may lead to failure of entire network. These attacks can infect the connected resources of controller. The flow paradigm can be secured by AVANT-GUARD, Open Watch security solutions[7].

C. Layered Taxonomy of SDN Security: In this section we categorized the existing Security solutions based on the following factors: solution category, SDN layers/interfaces, security mechanisms, simulation framework, security goals.

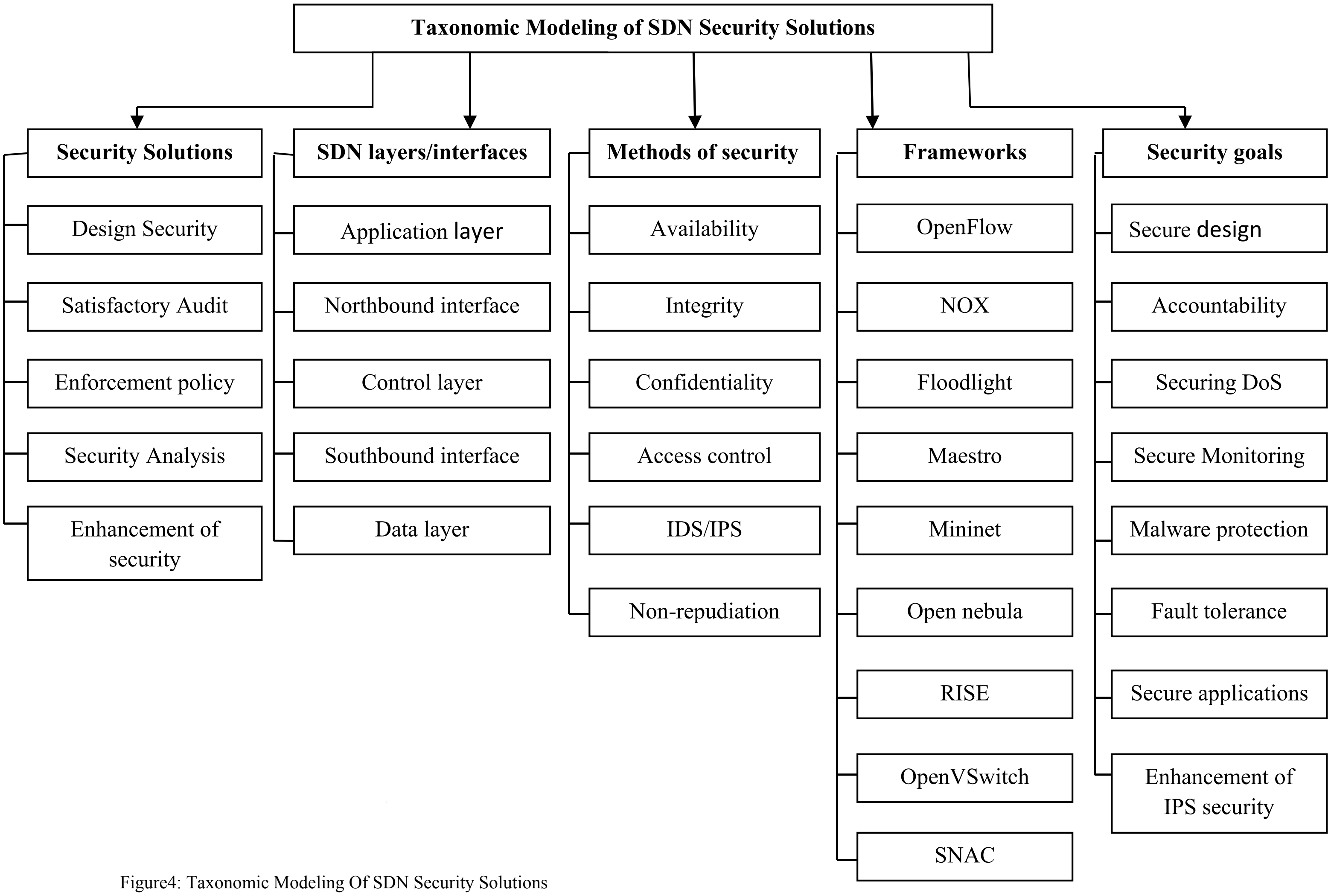

Figure4: Taxonomic Modeling Of SDN Security Solutions

In this section we categorized the existing Security solutions based on the following factors: solution category, SDN layers/interfaces, security mechanisms, simulation framework, security objectives[5]. Security is the top most priority of SDN. As SDN is not part of initial design, some of the proposals are given in this area, but that are not enough for SDN secure design. Therefore secure design area requires more attention. The great work is done on auditing of SDN environment. Valuable work is done by researchers on security improvement and on enforcement of security policies but very little in the area of security analysis.

The security also classified on the basis on layers and interfaces. The section also address attacks on different layers and interfaces. Every layer/interface is considered as target for particular attack. Different security mechanisms are presented like authorization, integrity, access control, availability, intrusion detection/prevention[5]. The literature also represents the ranking based on simulation framework**.** Various types of simulation environments are given but the OpenFlow (OF) is considered as best. At last the security objectives category is specified that represent accountability and auditing as major ones. Further security monitoring and secure design objectives are shown to control several issues. Some other considered objectives are securing denial of services, fault tolerance and Security enhancement.

VI. OPEN RESEARCH AREA FOR SDN SECURITY:

SDN is considered as most secure and dependable network which has several features. But, there exist many issues which can be solved by programmers to ensure security. As, security plays an significant role in every network so, adequate measures are taken to secure SDN. This part of article identified some of the issues which are not addressed properly for ensuring the security of SDN.

A. Operating system alteration: An operating system is a software that manages network hardware and software resources and provides common services for network programs. Therefore, if the alteration in operating system takes place, the results will be dangerous enough. It can infect the all layers and interfaces and can affect application management functionalities. The operating system alteration can be protected by trusted computing, but researches required to do work in this area.

B. Unauthorized Intrusion: It is an act of illegally gaining access into any network. So, any illegal actions into network lead to network disaster. All layers and interfaces are target for these types of attacks. It can ruin all functionalities of network. Secure administration module is required as protection technique. So, there is great need to pay attention in this particular area.

C. Several attacks: There are several types of attacks that should be carefully determined for SDN security. Most of the attacks are cured by researchers but there exist several other attacks that are still unaddressed like spoofing attack. Spoofing attack[6] is a situation in which a program successfully masquerades as another by falsifying data and hence gaining an illegitimate advantage.

VII. CONCLUSIONS

Various features and separation of planes of SDN make it very efficient technology which is going to be the future of networking. In this paper we appeal for the need to consider security while designing SDN. The literature defines the various possible attacks on different layers/interfaces of SDN. After that various security solutions given by researchers are presented. The taxonomic modeling of security solutions are represented based on solution category, SDN layers/interfaces, security mechanisms, simulation framework, goals of security. Further, top priorities or key components for SDN security are discussed. At last, the unaddressed area in SDN security is given by further research.

VIII. REFERENCES

[1] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, “Security in Software Defined Networks : A Survey,” no. c, 2015.

[2] S. Hong and H. Wang, “Poisoning Network Visibility in Software-Defined Networks : New Attacks and Countermeasures,” no. February, pp. 8–11, 2015.

[3] D. Kreutz, F. M. V Ramos, P. Verissimo, C. E. Rothenberg, S. Azodolmolky, S. Member, and S. Uhlig, “Software-Defined Networking : A Comprehensive Survey,” pp. 1–61.

[4] C. Engineering, “Review On Architecture & Security Issues of,” pp. 6519–6524, 2014.

[5] A. Akhunzada, E. Ahmed, A. Gani, M. K. Khan, M. Imran, and S. Guizani, “Securing the Software Defined Networks : Taxonomy , Requirements , and Open Issues,” pp. 1–10, 2014.

[6] S. T. Ali, V. Sivaraman, and A. Radford, “A Survey of Securing Networks using Software Defined Networking,” pp. 1–12.

[7] 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 ?).”

[8] J. Hizver, “Taxonomic Modeling of Security Threats in Software Defined Networking,” 2015.