Security Issues in Software Defined Networking (SDN): Risks, Challenges and Potential Solutions

Maham Iqbal[1], Farwa Iqbal[2], Fatima Mohsin[3], Dr. Muhammad Rizwan[4], Dr. Fahad Ahmad[5]
Department of Computer Science
Kinnaird College for Women, Lahore, Pakistan

***Abstract*—SDN (Software Defined Networking) is an architecture that aims to improve the control of network and flexibility. It is mainly connected with open flow protocol and ODIN V2 for wireless communication. Its architecture is central, agile and programmatically configured. This paper presents a security analysis that enforces the protection of GUI by requiring authentication, SSL/TLS integration and logging/security audit services. The role based authorization FortNOX and ciphers like AES and DES will be used for encryption of data and improving the security of SDN environment. These techniques are useful for enhancing the security framework of the controller.**

***Keywords*—SDN; wireless SDN; security threats; AES; DES; FortNOX; TLS**

I. Introduction

SDN has emerged as a flexible, secure and well-managed network. The architecture of SDN provides a central network control and its management via controller [1]. It segregates the data forwarding functions from the control plane of network. The control is transferred to a centralized controller to take decisions related to routing and then communicate those decisions to the data-forwarding plane [2]. Despite of all its features and functions, security of SDN is still considered to be a major concern. The configuration errors can lead to serious consequences as well as the aspects of programmability makes it vulnerable to attacks. The authentication, security and integrity of the network are severely affected. The architecture of SDN can be exploited to improve network security by providing security monitoring, analysis and response system [3]. The basic architecture has been shown in Fig. 1. SDN is cost-effective, dynamic, manageable and adaptable. Initially, it was being used for wired networks but with swift increase in the use of devices including smartphones and tablets has led to a great increase in data traffic in these devices. WLANs are used in homes, businesses and in public environments. There is a one-to-one mapping between a client and a light virtual access point with a unique and different BSSID. The client can switch control from one AP to another without any notification that connection was reestablished. There is no delay in communication or hardware as one device can move LVAP form one device or AP to another. This paper focuses on the security issues of SDNs. It presents some specific design issues of securing SDN. Subsequently, this paper also analyzes the state of software-defined security in order to improve the security properties which are confidentiality, integrity and availability [4]. The remaining paper is organized as follows. Section II provides a detailed literature review on SDN Section III contains problem statement, security issues in SDN. Section IV explains proposed methods and solutions, whereas Section V explains the results and further conclusions are drawn in Section VI.

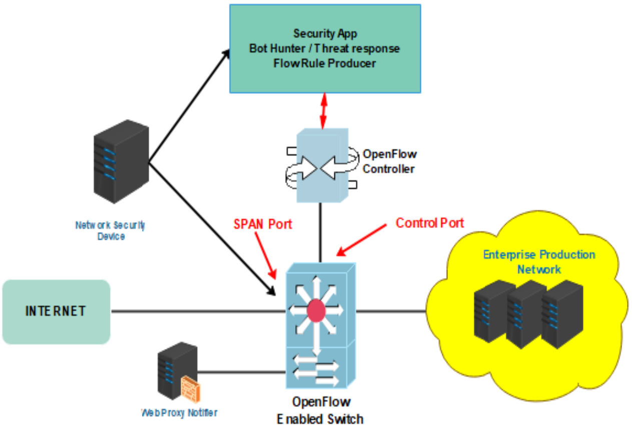

Fig. 1. SDN Structure.

II. Literature Reveiw

A. Security Issues in SDN

These are the main issues related to SDN

Forwarding Device Attack: The network traffic can be disturbed by access points or switches, which results in malicious users launching denial of service (DoS) attack that can result in network failure or disruption.

Threats in Control Plane: Due to the use of central controller, any problem arising in the network results in the failure of the central controller. The approach that is being used to solve this problem is to use either horizontal or hierarchical controller distributions.

Vulnerability of Communication Channel: SDN southbound API's such as Open Flow protocol uses TLS for data-control channel communication security but it is often disabled administratively and is prone to man-in-the middle attacks thus not suitable for implementation of channel security.

Fake Traffic Flows: A non-malicious faulty device or an attacker can launch this or DoS attack to dissipate the resources in forwarding devices or controllers.

Authenticity: It refers to the property that entities in networks are actually the ones they claim to be. The issue of authenticity for forwarding devices in SDWN networks is similar to that in traditional networks; it can result as hindrance in network performance [2], [4].

Confidentiality: it prevents from the expose of information to unauthorized users, if not ensured can lead unauthorized users to access network information or data [5].

Availability: It means that authorized users can access data, devices, and services whenever they need.

Open Programmable API: The open nature of API makes the vulnerabilities more transparent to attackers.

Man-in-the-Middle-Monitors: The switches and the controllers are not directly connected for the transmission of information, which "man-in-the-middle" monitors can steal or misuse the information without being caught thus leading to black hole attack. Some of threats in SDN and their impact are shown in Table I.

B. *Securing Wireless Software Defined Networks*

SDN is decoupling the data plane form control plane thus providing efficient network management, thus replacing traditional networks. The present paper reviews the hard work and challenges required to enforce security in software defined networks. Distributed SDN network remains a concern for dependent networks at architecture level, as wireless SDN with wired SDN is discovering applications in multiple fields to provide centralized network and traffic engineering. Wireless SDN inherits both pros and cons of wired SDN with added concerns like large number of threats due to high monitoring overhead, multiple operator and users of network, security and compatibility [1] [6]. Here are some concerns related to wireless SDN.

- The network traffic can be disturbed by switches or access points and denial of service (DoS) attack can be launched by unauthorized users.
- Any problem in SDN controller can create problems in whole network as central controller is used.
- SDN API is susceptible to man-in-the middle attacks so is not suitable for implementation of channel security.
- Authentication and security is required in servers and compromise in this can put whole network operation in risk and danger.
- Authentication, integrity, security, efficient event detection, data and control plane consistency are very important in wireless networking and can be easily endangered.

Wireless SDN amidst all these concerns provide great opportunity for improving network security through global monitoring, real-time programmability. SDN's centralized control network provides with the facility of tracking and alleviating security threats. Central controller functionality can be easily distributed in different servers on network. Global network visibility provide a great view to check real-time network, statistics of traffic and help to fulfill the changing network security requirements.

TABLE. I. THREATS IN SDN

Attack	Effected SDN Layer	Affected Security Aspect		
		Availability	Confidentiality	Integrity
Distributed DoS Attack	Control, Data	×		
DoS Attack	Control, Data	×		
Hijacked Controllers	Control, Data, App	×	×	×
Malevolent Applications	App		×	×
Man-in-the-Middle	Control, Data, Link between control and data		×	×
Black Hole	Control, Link between control and data	×	×	
Eavesdropping	App, Control, Data		×	

C. *Securing Software Defined Wireless Networks*

Securing network is important requirement for any network whether it is SDN or traditional networks. SDWN physically separates the data and control planes of various elements in the wireless structure, and have a central controller for controlling the overall functions of network [7]. However, the centralized and fine-grained control that comes with SDWN introduces a greater risk of outages due to errors made by network administrators. In this paper, security threats in SDN and issues in architecture to make it secure and their counterparts are discussed. SDWNs bring the benefits of network programmability and logically centralized control, it is exactly these benefits that expose SDWNs to new threats or those treats that are harder to exploit in traditional networks. SDWN networking is responsible for providing effective network management, but unfortunately turn out to be more weak to attacks than traditional networks where authenticity, confidentiality, integrity, availability, consistency, control traffic of network is affected due to attacks on forwarding devices, controllers thus leading network vulnerable to security attacks and issues. The security issues in SDN can be controlled by using some approaches that are:

- The problem of forged attacks can be solved by an authentication mechanism.
- Applications require security model to separate data forwarding and network management resources thus role-based authorization like FortNOX can be used.
- Attacks by hackers or unauthorized person can be reduced by using security technology like TLS.
- Communication between controller and forwarding device can be encrypted to ensure confidentiality.
- Dos attacks can be mitigated by rate-limiting mechanisms and redundant controllers.

- Flow timeouts can be adjusted to decrease the effects of DoS attacks.
- Flow timeouts can be randomized to introduce unpredictable behavior, so the attacker cannot view states of network.

D. *Security Analysis for SDN Environment*

Software defined networks are replacing the traditional networking systems due to its centralized control approach. The privacy, integrity and confidentiality of the system may get affected due to the attacks on the system's vulnerabilities which ultimately reduce the performance and efficiency of the network [8]. This paper provides a security analysis to enforce security within SDN through attack graph and alert correlation model to lessen the false positive alerts. The security challenges to SDN include open programmable API in which the open nature of the API's makes the vulnerabilities more visible to the attackers. An unauthorized access to the central controller may cause a huge damage to the information and inject malicious codes into the system. More attacks faced by SDN consist of application layer attacks, control layer attacks and infrastructure layer attacks.

Application layer attacks include:

- **Rules insertion:** creating and implementing security rules for SDN in different domains lead to various conflicts.
- **Malicious Code:** injecting different programs lead to various attacks where attackers inject malicious code which leads to the corruption or loss of data.

Control layer includes the following attacks:

- **Denial of Service Attacks:** these attacks can occur at channel, controllers or between the controller and the switches.
- **Attacks from Applications:** the attacker who gets illegal access from the application layer gets the sensitive data about the network which leads to attacks against control layer.

Infrastructure layer attacks:

- **Dos Attack:** An attacker can dowse the buffer flow and the flow table by transmitting frequent large mysterious packets, which will generate new rules to be inserted into flow tables.
- **Man-in-the-middle Attack**: The switches and controllers are not directly connected for the transfer of information so the "man-in-the-middle" monitors can intercept important information without being detected ad can result in eavesdropping and black hole attack.

Security is analyzed through attack graph and alert correlation model. Attack graph measures the ability to overcome the attacks whereas the alert correlation model classifies the alerts.

E. *SDN Architecture Impact on Network Security*

The architecture of SDN separates the data plane from the control plane. It provides decisions for forwarding the datasets. The protocol being used for communication between SDB controller and network data is Open Flow. This paper discusses the features of SDN that can be used for improving the security of the network [3]. The automatic exposure of threats can be handles by reconfiguring flow tables in switches. An amalgam approach is based on the local and universal study of the traffic pattern. One of the methods for detecting the threats is called frequent set. The local frequent set analyzer is placed on SDN switch for the detection of threats. In this way, the malicious activities can be detected locally, and an appropriate action is executed in response. Along with it Global Frequent Analyzer is also used which is placed on the SDN controller. LFSA inserts new rules into the flow tables that plunge the packets which contain malicious data resulting in the reduction of attacks, protection from DoS attacks. These attacks are controlled more accurately in the access switch rather than the aggregation switch. The anticipated DFSA system that makes use of features of SDN network, can be used for effective and unswerving detection of numerous network attacks that are observed nowadays in IP networks.

F. *Securing Software Defined Networks*

In this paper, many exterior and interior threats are being explored in the architecture of SDN. As the integrity and security of SDN is still not proven in terms of the functionality management settlement in a single central server. Cyber-attacks which are launched throughout SDN have bigger destructive effects as compared to simple networks [9].

Every layer of SDN architecture has its separate requirements of security such as the configuration errors. If these requirements are not provided, they may result in various categories of security threats and attacks. The communication flooding attack linking the switch and the controller will have an effect on all the corresponding three layers. The upper three layers can be affected from the policy enforcement security attacks. Authorization attacks may result in prohibited access to the controller.

For a safe SDN environment, it is necessary to make sure that every component of SDN is secured. The primary task is to ensure that the SDN controller is secured as it controls the complete management of the network. The operating system should also be secured. If the SDN controller gets compromised, it will cause the failure of the whole network. The flow model of SDN should be secured by encrypting the flows so that the injection of malicious flows is avoided. An SDN agent constitutes the environment therefore its security is very essential. The installation of identity management modification techniques and threat isolation is the main requirement. IPS, IDS, and firewalls should be dynamically updated. The communication channel must be protected between each layer. Secure coding, digital signing of the code and deployment of integrity checks are the security measures taken for this purpose.

G. Critical Analysis

Approximately 64% of the false positive alerts are reduced by the alert correlation when compared with the original false positive alert. Security analysis is performed by the combined use of the attack graph and alert correlation method [8]. TLS uses better algorithms for providing security between control plane and data plane as compared to SSL but unfortunately many implementations of TLS/SSL undergo man-in-the-middle attacks. Hence, TSL may not be the optimal choice because it may fail to handle the future security issues [1]. Role based authorization, FortNOX, is a potential solution for the authorization and authentication concerns of network resources. It resolves the situation for the controller to handle inconsistent flow rules from the two different applications. Nevertheless, role-based authorization is not sufficient to deal with the complexity of SDWN to isolate applications or resources [7]. The conflicts in an SDN firewall are resolved by checking firewall authorization. The conflict resolving strategies differ from the processes which are involved in the flow entries and flow rules. The effectiveness and efficiency of the proposed approach is examined using header space analysis [9] [10].

III. Problem Statement

Applying SDN to improve performance, scalability of network is being widely used in industry for some years, for both wired and wireless connections. One of the challenges of SDN is to ensure the quality of service for various functions of network by resisting against intrusions, malicious attacks and liabilities, how to develop an authentication between a control plane and a data plane and how the sufficient security services can be provided in networks in future in an economic way [5].

IV. Proposed Solution

A hybrid approach including the data link layer, control link layer and encryption would be used for ensuring a much better security of SDN.

A. Security of Control Plane in Network

FortNOX is a security enforcement kernel responsible for implementing role-based verification to regulate the authorization of each OF applications [11]. The major work is to secure the programming and it directly impacts the application and control layer and on communication between these layers. Another t contribution of FortNOX is to conflict rules from different applications in network thus resolving issues in control layer and north and south bound interfaces. It uses the controller to define three standard authorization roles among the flow rule producers

1) OF Operator Role–define imposing the policy of security

2) OF Security Role-flow constraints are added to fight against live threat activity

3) OF Application Role–authorization of OF Applications

The basic architecture of FortNOX is shown in Fig. 2.

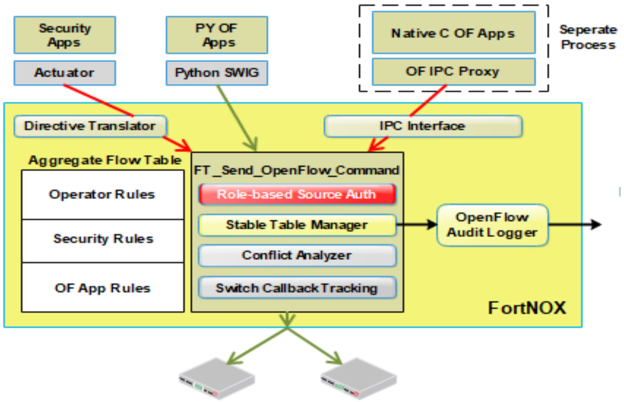

Fig. 2. Architecture of FortNOX.

B. Transport Lyer Security Protocol

The use of Transport Layer protocol for ensuring the security of SDN aims to protect the privacy of information communicated over the internet between the data and the control plane [10] [12]. For managing the authentication, the server has to prove its identity to the client and the client needs to prove its identity to the server by using the private keys. These keys are created using the cypher suites for encrypting the information. The message authentication code (MAC) is applied to the outgoing messages and are verified at the receiving end. The basic working of TLS is shown in Fig. 3.

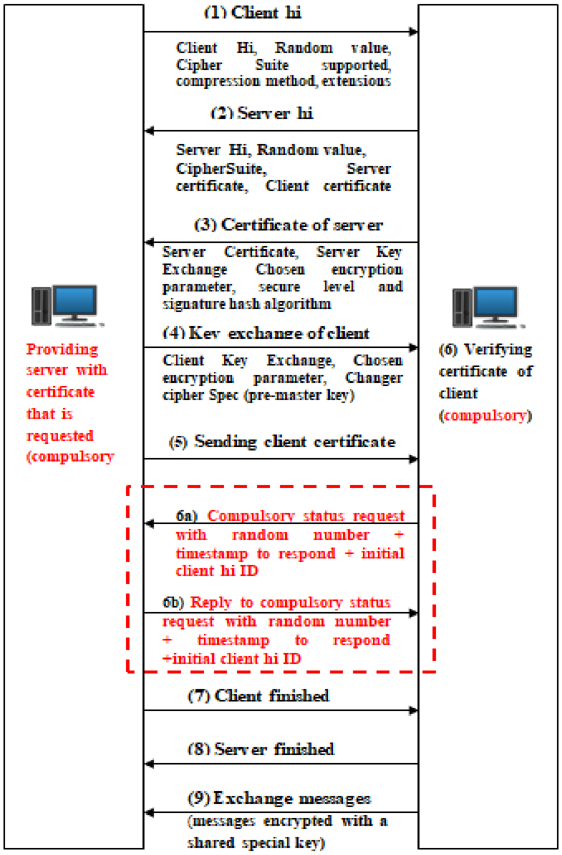
(1) Client hi
Client Hi, Random value, Cipher Suite supported, compression method, extensions
(2) Server hi
Server Hi, Random value, CipherSuite, Server certificate, Client certificate
(3) Certificate of server
Server Certificate, Server Key Exchange Chosen encryption parameter, secure level and signature hash algorithm
(4) Key exchange of client
Client Key Exchange, Chosen encryption parameter, Changer cipher Spec (pre-master key)
(5) Sending client certificate
Providing server with certificate that is requested (compulsory
(6) Verifying certificate of client (compulsory)
6a) Compulsory status request with random number + timestamp to respond + initial client hi ID
6b) Reply to compulsory status request with random number + timestamp to respond +initial client hi ID
(7) Client finished
(8) Server finished
(9) Exchange messages (messages encrypted with a shared special key)

Fig. 3. Working of TLS.

C. Encryption of Data

a) Advantages of Encryption: Encryption is used to attain complete security. Data is most defenseless when it is being transmitted from one location to another. Encryption works during data transmission, in order to shield delicate data, including personal information for individuals. Encrypted data maintains integrity of data by informing the recipients of the data to detect the corruption or cyber-attack. It aids in ensuring privacy and decreasing chances for surveillance by both government agencies and criminals.

Advanced Encryption Standard: AES is a symmetric block cipher used for the protection of classified information by the encryption and decryption of sensitive data. By encryption data is changed into cipher text while decryption transforms cipher text into text form of data, it is applied in hardware and software to protect digital information in several forms data, audio, video etc. from unauthorized users. As it is a security protocol, therefore it is commonly used for wide range of applications such as wireless communication, financial transactions, e-business, encrypted data storage etc. However, AES is difficult to implement in software as it takes both performance and security into considerations since every block is always encrypted in the same way. The basic working of AES is shown in Fig. 4.

b) Data Encryption Standard: Data Encryption Standard or DES is a symmetric block cipher. It takes 64-bit plain text and 56-bit key as input and produces 64-bit cipher text as output. In DES, encryption and decryption uses the same algorithm. The key is taken in opposite order.. An attack on a 56-bit key in encryption is impractical. However, DES is insecure beacuse the 56-bit key size being too small. DES is a very slow algorithm such that Triple DES (3DES) [12] [13].

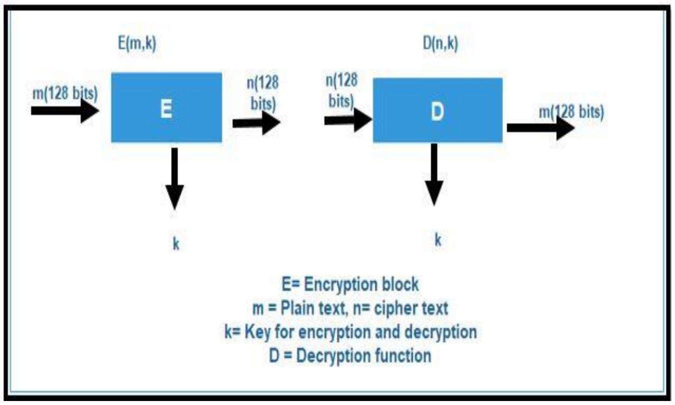

Fig. 4. Working of AES.

V. Result Discussion

The TLS protocol is used to provide encryption, authentication, and data integrity. TLS provides particular alerts about problems with a session and documents when these certain alerts are sent. Transport layer Security is divided into two layers Record and handshake and uses public key cryptography to ensure a secured communication. Client sends requests to server who respond with information that is required for its authentication, both, client and server exchanges several keys and client's authentication key is stored. The use of extended security system of TLS protocol provides a more secure data communication between the client and the server. It protects the loss of data by man-in-the-middle attacks. An additional feature of time stamp indicates the entry of each packet in the network. The time stamp measures the delay and packet loss thus reducing the loss of data as no exchange of metadata occurs between the switches. Once the authentication block is over, and client's authentication is given a CA certificate secured communication is established, but it just ensures secure delivery of data but does not secure data for which encryption of data is necessary which is done through AES and DES ciphers. DES uses cryptographic key for block of a code, it converts the message into 64-bit blocks. These blocks are then encrypted into key whereas decryption in it is done by using the encryption process in reverse, whereas AES uses same key to encrypt and decrypt [14] [15]. FortNOX – A new security enforcement kernel for OF networks is used in SDN to ensure secure data communication. It assigns a key to the devices in network and stores that key or rule. It checks the key of devices that make a request for information, if key does not match it generates an error otherwise access to information is given.

VI. Conclusion

The emergence of the Software-defined network has overcome the requirement and need of secure, trustworthy, flexible and well-managed networks. However, due to the separation of the two planes, SDN is vulnerable to more attack vectors than traditional networks. This means that the availability, consistency, authenticity, confidentiality, and integrity of network and control traffic could be rigorously affected. This paper highlights some of the basic threats to the SDN and discusses various solutions which have been suggested. WSDN also suffers security concerns which are much similar to the framework of wireless SDN along with the issues that arises by using wireless medium. Moreover, in spite of risks or issues, the security benefits in a centralized SDN framework are being exploited by research efforts, which are real-time programmability and global traffic monitoring capability.

REFERENCES

[1] T. Bakhshi, "Securing Wireless Software Defined Networks: Appraising Threats, Defenses & Research Challenges," in In 2018 International Conference on Advancements in Computational Sciences (ICACS), 2018.

[2] C. W, L. A and W. P, "A roadmap for traffic engineering in SDN-OpenFlow networks. Computer Networks," pp. 1-30, 2014.

[3] C. K., W. J. and K. S. , "SDN Architecture Impact on Network Security," in Federated Conference on Computer Science and Information Systems, 2014.

[4] K. D, R. F. and V. P. , "Towards secure and dependable software-defined networks," in Proceedings of the second ACM SIGCOMM workshop on “Hot topics in software defined networking, 2013.

[5] Y. Zheng and P. Zhang, "A security and trust framework for virtualized networks and software-defined networking," Security and communication networks, pp. 3059-3069, 2016.

[6] R. . M. F. and K. D, "Software-Defined Networking: A Comprehensive Survey," in Proceedings of the IEEE, 2015.

[7] H. Daojing , . S. Chan and M. Guizani, "Securing software defined wireless networks," IEEE Communications Magazine, pp. 20-25, 2016.

[8] El Moussaid, T. N and El Azhari, "Security Analysis as Software-defined Security for SDN Environment," in Fourth International Conference on IEEE, 2017.

[9] A. A, A. E and G. A, "Securing Software Defined Networks: Taxonomy, Requirements, and Open Issues," IEEE Communications Magazine, vol. 53(4), pp. 36-44, 2015.

[10] Belema Agborubere and Erika Sanchez-Velazquez, "OpenFlow Communications and TLS Security in Software-Defined Networks," in IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2017.

[11] Phillip Porras, Seungwon Shin and Martin Fong, "A Security Enforcement Kernel for OpenFlow Networks," in Proceedings of the first workshop on Hot topics in software defined networks, 2012.

[12] A. e. a. S, "A Survey of securing Networks Using Software Defined Networking," in IEEE Trans. Reliability, 2015.

[13] K. K and S. F, "Distributed Attack Graph Generation," in IEEE Transactions on Dependable and Secure Computing, 2016.

[14] S.-H. S and S. S, "A survey of security in software defined networks," in IEEE Communications Surveys & Tutorials, 2016.

[15] H. J., "Taxonomic Modeling of Security Threats in Software Defined Networking," in In BlackHat Conference, 2015.