Analysis of Vulnerability Threat and Attack over Network Architecture

Swapnesh Taterh
Associate Professor
Amity Institute of Information Technology
Amity University Rajasthan

Abstract— In this paper, the SDN architecture provides a keen-sighted view over the network facilitating a flexible, reliable and a better managed network architecture in terms of flow of data that control facility of the data is moved to a centralized controller enabling a wider and broader view of the network. This paper is planned with a concept of network and its architecture. It also provide the security solutions for the network and leveraging threats and type of attack possibilities in network. This paper concludes with the requirements of security factors of network.

Keywords—.Network Traffic, Agents, Open Flow (OF), Open Network Foundation (ONF), Control Plane, Data Plane, Application Programming Interface (API), Spoofing, Distributed Denial of Service (DDoS), Tampering, Centralized Controllers

I. Introduction

On talking about the next generation in networking, the prime focus should be on Software Defined Networking. Decoupling the data plane from the control plane of the network enables the SDN design to be capable enough to provide a manageable, reliable and flexible network [1].

This design makes the physical devices such as routers and switches to act only as a forwarding agents of the network traffic which in turn makes them vendor-independent, cost effective and moreover flexible and creative network design. The physical devices, being only the forwarding agents, the

Focusing on the various advantages of SDN, the loop holes and the drawbacks of SDN also needs primary attention. Fixing the drawbacks and increasing the advantages of SDN only will increase the implementation factor of SDN Networks. With all the exciting features and flexibility that SDN provides to a network, the security factor of the network requires more functionality and high concern of improvability [1].

On various platforms where the SDN Implementation factors are discussed, the experts recommend to address the security issues around SDN. The Software Defined Networking architecture poses various internal and external threats and vulnerabilities because of its centralized controller design, which questions the integrity and security of the Software Defined Networking [1]. Because, the controller has the entire network on it, the controller itself can be easily used for additional attacks and collapsing the network.

One of the weak points in Software Defined Networking is, the advantages itself pose a variable threat to the network. As discussed in the above paragraph about its centralized controller design, it's another prime functionality - the programmability also poses a strong threat to the network, due to malicious code exploits and attacks.

Additionally, the denial of service attacks and side channel attacks and easily targeted in the southbound interface of the SDN network. Outraging the current scenario, cyber-attacks are piece of cakes for the intruders or attackers in a Software Defined Networks which will cause more damage to the network, on comparing with the legacy networks.

Concentrating on improvising the security features in Software Defined Networking, each layer of SDN needs to be focused on achieving better secured environment instead of implementing security overall to a network, because each layer has different implications and different requirements.

Main focus of security in SDN, is the controller which requires dynamic, robust and strong security policies. SDN is already a flexible, reliable and managed network architecture and its further needs a scalable and secured environment, for which this paper paves a pathway for the researchers to achieve the loopholes in Software Defined Networking.

This paper further discusses the security solutions which are available with Software Defined Networking and further threats and attacks possibility on SDN networks. This study concludes with a note on required steps to be taken in achieving a secured SDN Network.

II. SDN ARCHITECTURE DESIGN

This part of the paper discusses in detail about the Design and the security concerns of SDN Architecture. The basic cling between the existing network design and the SDN is its separation of control and data plane and the facility of programmability in the control plane [1].

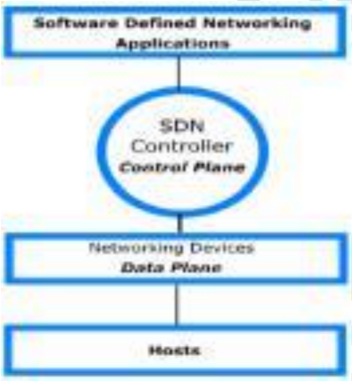

Figure 1: SDN Architecture

Figure 1 gives a clear insight on the Architecture of Software Defined Networking where the Third Party Applications sit on the SDN Controllers in the control plane which is decoupled from the data plane enabling improvised network operations. With reference to the Figure 1, the Software Defined Networking is a three layered architecture. The data plane is the physical networking devices, controlled by the control plane through various protocols. The management plane is the software platform which is helpful to control the entire network flow. Software Defined Networking focuses on Dynamic Flow Control, Network wide visibility with Centralized Control, Network Programmability and Simplified Data Plane. A network application program (management plane) will be controlling the data planes in Software Defined Networking [3]. There are different controllers available in which few are listed in the Table 2 [4]. The physical networking devices in SDN will act as only a forwarding device and the "where and how" part will be done by the Control Plane [5].

The application layer in the SDN is responsible to provide services and run applications related to security as such, Intrusion Detection, Prevention Systems, Load Balancing, Deep Packet Inspections, security monitoring tools, access controls etc.

III. SECURITY TOOLS AVAILABLE FOR VARIOUS SDN LAYERS

The SDN Architecture, classified as North Bound, South Bound, Control, Data and Application Layers have various tools available to secure the network. This part of the paper discusses on the existing tools available in securing SDN's.

Fresco, Fortnox, Avant-Guard, OpenWatch [6] are few tools which focus on the security design and analysis of the SDN Network. They work on various layers in SDN. Fresco is an OpenFlow security specific application which focuses on secure design development [1]. It is developed for NOX Cotroller, in the year 2013, works on Application Layer, Control Layer, North and South Bound Interfaces [6]. Fresco focus on capturing the application programming interface (API) scripts to combat with security threats by developing security monitoring features in an SDN Architecture [1]. FortNox is also similar to Fresco, working on North and South Bound and the Control Layer. It is not focusing on the Application Layer [1]. FortNox focuses on interpreting the security rule conflicts arising during security authorizations in a security enforcement kernel [1].

Avant-Guard focus on the security analysis of the SDN Network, working on the Data Layer, Control Layer and North South Bound Interfaces. OpenWatch is also similar tool like Avant-Guard focusing on the security analysis of the SDN Network, however working on the Application Layer also along with data, control, north and south bound interfaces. These security analysis tools are proposed with a systematic approach to collect more information about the data plane. The collected information are used to gradually reduce the interactions between the data and the control plane keeping in mind the Denial of service attacks.

Tools like Verificare, SDN Debugger works on the security audit of the SDN Architecture. Verificare works on the Data, Control and North & South bound interfaces whereas the SDN Debugger works on the Application Layer and South Bound Interface.

To enforce the security policy, tools like VeriFlow, Flyover are implemented which works on the various layers on SDN Architecture. Enforcement of security policy plays a vital role in SDN Environments. Flyover [8] application was proposed to address the security enforcement policy by checking the flow policies in contradiction with the network policy deployed. FleXam [8] is another tool works with OpenFlow, which is designed to provide access to the controller of the OpenFlow to receive packet level information. The FleXam also seizes the low setup time and also minimizes the load of the control plane. The above is the list of few tools which are working on the security aspects of SDN.

IV. Threats and Attacks in SDN Architecture

Discussing more on the existing tools and security measures in an SDN Architecture, gives a vast idea on the current threats and attacks which are possible in the network. The Security aspects in the SDN Environment are prone to be the key factor of research in today’s development is because of the reason that SDN environment did not consider security as a prime factor during its initial design [1].

Based on the available applications or tools in SDN, a clear factor reveals that contributions in secure design of the SDN is limited. More research works focus on the security enforcement policy rather than the security enhancement and security analysis. Threats and attacks in a SDN Architecture needs to be focused individually proportionate to different layers or interfaces in the SDN Architecture rather than developing a common solution for SDN. There are various different possible threats, attacks and exploits targeting each layers of the network. The various security mechanisms like access control, intrusion detection and prevention, encryption, authentication, authorization needs to be focused based on the security requirements in each interfaces. Major part of SDN networks are designed based on the OpenFlow standards, our further research is focused on securing and defending OpenFlow Networks.

Security threats in an SDN networks are grouped under the following categories.

1. Alteration
2. Modification
3. Authorization
4. Impersonation

Altering the Operating System, the data configuration files, user data are classified under Alteration. Modifying the software framework, Creating a software and hardware failure and extraction of data configuration files are classified under Modification. Unauthorized access to the network is classified under Authorization and Impersonating as an authorized SDN Controller in the network is classified under impersonation [1].

The operating system, when altered shall cause a high impact of damage to the components like controller and forwarding nodes in SDN Networks. This type of threats can be handled by ensuring high system integrity protection. In order to achieve a high system integration, trusted computing is required. This type of threat can always attack all the layers of SDN Network. Like the alteration of Operating System, the alteration of data configuration files is also a high impact threat factor which can cause damage to the data that are essential in performing effective SDN Operations. This type of threat can always attack the control layer, the data layer and the control-data interface. Alteration of user data is another alteration threat which troubles the user data like their profiles. Mostly this type of threat affect the data layer. Both the data configuration and user data threats can be handled by ensuring data integrity in the SDN Network.

The modification type of threat, Software framework alteration damages the middleware and the components of the software framework. Software framework alteration also attacks all the layers of the SDN Network. Like the alteration of Operating System threat, this threat can also be mitigated using high system integration. The software and hardware failure is one of the common threats highlighting the general software and hardware resource failure. Improving the robustness of the software and high configured hardware can be a way of mitigating the threats. The software failure can target all the layers whereas the hardware failure affects the control and data layers of SDN architecture. One of the challenges in securing the network is based on data security. The configuration data extraction threat is a threat where the attackers gathers information from various sources and various methods. The data collected is accumulated to perform subsequent attacks. In order to mitigate this threat, data integrity and confidentiality needs to be improvised. This threat targets on the control and data layer including the control – data interface.

Unauthorized Access in Authorization is a type of threat where possibility of security breach happens. High level of security policy and security administration is required to mitigate this type of threat. This type of authorization threat can target all the layers and almost all the functionalities in the network architecture.

Impersonation of the SDN controller is one of the toughest threats in SDN which compromises the entire SDN architecture. SDN Controller, being the heart of the SDN Network if masqueraded leads to a damage of entire network without the knowledge of the network itself. Techniques such as digital signatures, public key encryptions can mitigate this type of threats.

V. Securing the SDN Architecture

In the perception of securing the SDN Architecture, few changes in the architecture shall be suggested based on the above classifications. Policy reinforcement can be done in the first position to secure the network. Having a high enforced policies in the network shall mitigate attacks related to policy enforcement in the south bound, data and control layers. Availability related attacks requires more attention as they are the basic steps taken in tightening the security in a network. Availability of devices and other resources in a network can cause damages in both the extreme. Availability and over load of the network. The application, north bound and the control layer requires high level of security in the focus of availability of resources. Authorization related attacks are generally damages the south bound, data and control layers whereas the Authentication related attacks damages the application, north bound and the control layer. Securing the network from both these attacks are highly efficient by providing digital certificates and using public key encryption of data. Data Alteration, Controller Impersonation are few security breaches which attack the south bound, data and control layers. Unauthorized rule insertions and side-channel attacks are also few attacks which cause damage to the application, north bound and the control layer.

VI. Conclusion

The emerging trend in the networking domain – Software Defined Networking is highlighted for adoption from the legacy network architecture. On this point, the security factor is focused as a prime factor in reducing the implementation of SDN taking over from the legacy networks. Concentrating on the existing security aspects of the SDN architecture, the requirements of new mitigation schemes are widely discussed in this study. Factors such as Identity management, Threat Isolation deployment are required to mitigate the threats and attacks.

REFERENCES

[1] Securing Software Defined Networks: Taxonomy, Requirements and Open Issues, IEEE Communications Magazine, April 2015.

[3] L. X. S. H. G. G. Seungwon Shin, "Enhancing Network Security through Software Defined Networking (SDN)," in 25th International Conference on Computer Communication and Networks (ICCCN), 2016.

[4] F. M. V. R. P. E. V. C. E. R. S. A. S. U. Diego Kreutz, "Software-Defined Networking: A Comprehensive Survey," Proceedings of the IEEE, vol. 103, no. 1, pp. 14-76, 2015.

[5] K. C. M. H. O. Kannan Govindarajan, "A literature review on Software-Defined Networking (SDN) research topics, challenges and solutions," in Fifth International Conference on Advanced Computing (ICoAC), 2013.

[6] P. P. V. Y. M. F. G. G. M. T. Seugwon Shin, "FRESCO: Modular Composable Security Services for Software-Defined Networks," in ISOC Network and Distributed System Security Symposium, 2013.

[7] P. Porras et al., "A Security Enforcement Kernel for OpenFlow Networks," Proc. 1st Wksp. Hot Topics in Software Defined Networks, ACM, 2012, pp. 121–26.

[8] S. Son et al., "Model Checking Invariant Security Properties in OpenFlow," Proc. IEEE ICC, 2013, 2013, pp. 1974–79.

[9] S. Shirali-Shahreza and Y. Ganjali, "FleXam: Flexible Sampling Extension for Monitoring and Security Applications in Openflow," Proc. 2nd ACM SIGCOMM Wksp. Hot Topics in Software Defined Networking, 2013, pp. 167–68.