A Novel Security Analysis Model for Software Define Networking

J.David Sukeerthi Kumar

Abstract

Software Defined Networking (SDN) approaches to networking management which improves networks performance and monitoring than traditional network. As there are many security threats in SDN. To handle the issues many security measures and measurement tools have been developed to ensure internal security. However, the measures can ensured and provide security for SDN with proper procedure approach for evaluating the security position of SDN. In this article, Threat Vector Hierarchical Attack Representation Model(TVHARM) in formal with Novel graphical security model which provides a particular systematic approaches regarding threat, attack and security metrics, security assessment and other security measures also. It also indicates the counter measure and security measures through TV-HARM in SDN. Experimental results, showed the counter measure attacks and also apprehend the various security attacks to SDN.

Keywords: Software Define Networking, Security Analysis, Security threats, TVHARM, Counter measures.

1. Introduction

Software Defined Networking (SDN) is an emerging domain. It has been attracting a lot of attention from scholars, service providers and industrialists. Regarding the scope of SDN, here have a short glance on the SDN and its functionalities. Traditional networks or the networks that are currently used by most of the industry comprise of dedicated hardware which are application specific. This makes the network static and inflexible. The data to be forwarded, the receiver, the sender and the traffic is handled by the same unit. With the advent of SDN, the control plane and the data plane the plane that executes these decisions and forwards traffic are separated and hence the abstraction of lower network infrastructure functionality is introduced**.** SDN attempts to centralize network intelligence in one network component by disassociating the forwarding process of network packets from the routing process. The control plane consists of one or more controllers which are considered as the brain of SDN network where the whole intelligence is incorporated. However, the intelligence centralization has its own drawbacks when it comes to security, scalability and elasticityand this is the main issue of SDN.The TV-HARM captures different threats and their combinations, enabling security risk assessment of SDN.

In addition,it define three new security metrics to represent security of SDN.The experimental results showed that the proposed security assessment framework can capture and evaluate various security threats to SDN, demonstrating the applicability and feasibility of the proposed

framework. SDN is one of emerging networking technologies, allowing system administrators to modify network configurations in real-time for performing various network optimization functionalities e.g., optimizing network performance through load balancing.These new functionalities allow more efficient network management and control without disrupting network operations. Because of this, it has been used as the new networking architecture for promising applications such as mobile edge computing, fast networking, and tactile internet. Although SDN security has been studied previously, existing studies used SDN devices and their attributes e.g., vulnerability to evaluate the security posture of SDN. To the best of our knowledge, no prior work used graphical security models to deal with the threat vectors existing in SDN. Security risk analysis via the graphical security models incorporates the complex relationships between vulnerabilities in SDN. This can be used to evaluate the changes in the attack surface and formulate the most effective countermeasure to be deployed for SDN environments.

The SDN controllers have vulnerabilities in SDN applications and communication protocols, where traditional networks do not have such components. An attacker can perform eavesdropping or launch a privilege escalation attack. In such cases, those new vulnerabilities need to be considered the security risk analysis which the traditional methods of security assessment may not be able to capture and analyse. One systematic approach leverages the power of graphical security models to evaluate the security posture and compare the effectiveness of different defines mechanisms. TV-HARM perform can Capture dynamic changes of SDN and assess complex attack and defines scenarios, and represent the security posture using various security metrics in SDN.

Software Defined Networking (SDN) extends capabilities of existing networks by providingvarious functionalities, such as flexible networking controls.

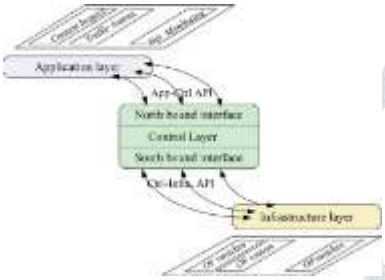
In this article there is a novel security risk analysis framework for SDN by incorporating various threat vectors.

2. Literature Review

A Systematic approach to threat modelling and security analysis for SDN provide a frame work dynamically adjust and re-program the data plane with use of rules. Software Defined Wide Area Network (SD-WAN) applies technology to the wide area network where it commonly associated with the open flow protocol for the remote communication with network plane elements for the purpose of determining the path of networks packets and networks switches. However, there are many attacks, threats and security issues in SDN are which easily approached through particular architecture. In this article propose a novel framework to systematical model and the analysis of security of SDN. The model named TV-HARM provides the threats, attacks and security assessments for SDN.The threat vector which captures different attacks. Unfortunately, SDN introduces new threat vectors that need to be taken into account for an in depth security risk assessment. For example, there are new types of networking components in SDN to support the new networking functionalities. As a result, there may exist vulnerabilities that may have not been considered in the traditional security assessment methods.The SDN controllers have vulnerabilities in SDN applications and communication protocols, where traditional networks do not have such components. An attacker can perform eavesdropping or launch a privilege escalation attack. In such cases, those new vulnerabilities need to be considered the security risk analysis whichthe traditional methods of security assessment may not be able to capture and analyze. One systematic approach leverages the power of

graphical security models to evaluate the security posture and compare the effectiveness of different defense mechanisms.There are new types of networking components in SDN e.g., the SDN controller to support the new networking functionalities. As a result, there may exist vulnerabilities that may have not been considered in the traditional security assessment methods i.e., the inability to capture the security properties of new networking components of SDN. As a result, various work has been performed to improve the security of SDN

Fig: Software Defined Networking



- Application Plane: It contains SDN for various functionalities, such as network management, policy implementation and security services.
- Control Plane: Itisalogicallycentralizedcontrolframe-workthatrunstheNOS,maintainsglobalviewofthe network,andprovideshardwareabstractionstoSD Napplications.
- Data Plane: Itisthecombinationofforwardingelements usedtoforwardtrafficflowsbasedoninstructionsfr omthecontrolplane.

SDN decouples network configuration and traffic engineering from the underlying hardware infrastructure to ensure holistic and consistent control of the network using open APIs.The exploding volumes of data traffic, complex network architecture and growing demands to improve network performance renders the traditional approach to network management as obsolete. Traditional network architecture offers minimal flexibility to coordinate between fixed function network devices that must be configured manually. A single change can have a cascading effect on the network performance and has the potential to bring down the entire network.

3. Security method for Software Define Networking

In recent years, SDN has been a focus of research. As a promising network architecture, SDN will possibly replace traditional networking, as it brings promising opportunities for network management in terms of simplicity, programmability, and elasticity. While many efforts are currently being made to standardize this emerging paradigm, careful attention needs to be also paid to security at this early design stage. This paper focuses on the security aspects of SDN. Begin by discussing characteristics and standards of SDN. On the basis of these, discuss the security features as a whole and then analyze the security threats and countermeasures in detail from three aspects, based on which part of the SDN paradigm they target, i.e., the data forwarding layer, the control layer and the application layer. Countermeasure techniques that could be used to prevent, mitigate, or recover from some of such attacks are also described, while the threats encountered when developing these defensive mechanisms are highlighted. The past security has been a daunting task in communication networks due to the underlying network complexities, proprietary and perimeter-based security solutions that are difficult to manage, and the weak notions of identity in IP networks. Similarly, the Internet architecture that defines procedures for usage of the underlying

infrastructure inherits the problems arising from the infrastructure, is ripe with security challenges and is stagnant to innovation. Therefore, many proposals have been put forward for architecting the Internet to curtail its inherent limitations, and to minimize its complexities and security vulnerabilities. In this section, discuss which either had an impact on network security or network security has been its important objective besides other objectives.

Admin

In this the admin module consists of the particular information of all the users and the users are also displayed in this module. The Virtual machine is created in the admin module and then the created or the existing virtual machine is allotted here. This virtual machine is which used for the avoiding of the attackers on the data or the file. In the admin module it plays an emerging role where the every particular end user information is stored in this particular database. If the threats occur the counter measures are easily identified in order to safeguard the data.

End user

In this the end user is the one who sends the request to the other user and if there are any data collections are also verified in the collection of data in this end user itself. Where if there are any sort of attacks performed on the data is also checked in the security assessments and the counter measure. In this in order to send a data to another user we create a virtual machine because so no attacks will occur to the particular end user, where there if the other user accepts the request and send the data in back step then the particular attack is performed on the user. So in order to avoid to this attacks the virtual machine is allotted.

Attacker

In this module the particular attacker is the one who performs the attack on the end user where the virtual machine is only not allocated and the data is then controlled by the attacker where the particular attacker can also see the data of the end user. The attacker can only perform the attack on the control flow data and the data flow. In these cases if the users can send messages without any security metrics there the attack is performed and the data is performed by the attacker. In which the attackers' control and data plane is also viewed by the attacker. And at the end we can check the attack and the action is also abolished.

4. System study

4.1 Feasibility Study

Preliminary investigation examine project feasibility, the likelihood the system will be useful to the organization. The main objective of the feasibility study is to test the Technical, Operational and Economical feasibility for adding new modules and debugging old running system. All system is feasible if they are unlimited resources and infinite time. There are aspects in the feasibility study portion of the preliminary investigation:

- Technical Feasibility
- Operational Feasibility
- Economic Feasibility

4.1.1 ECONOMIC FEASIBILITY

A system can be developed technically and that will be used if installed must still be a good

investment for the organization. In the economic feasibility, the development cost in creating the system is evaluated against the ultimate benefit derived from the new systems. Financial benefits must equal or exceed the costs.The system is economically feasible. It does not require any addition hardware or software. Since the interface for this system is developed using the existing resources and technologies available at NIC, There is nominal expenditure and economic feasibility for certain.

4.1.2OPERATIONAL FEASIBILITY

Proposed projects are beneficial only if they can be turned out into information system. That will meet the organization's operating requirements. Operational feasibility aspects of the project are to be taken as an important part of the project implementation. Some of the important issues raised are to test the operational feasibility of a project includes the following:

- Is there sufficient support for the management from the users
- Will the system be used and work properly if it is being developed and implemented
- Will there be any resistance from the user that will undermine the possible application benefits

This system is targeted to be in accordance with the above-mentioned issues. Beforehand, the management issues and user requirements have been taken into consideration. So there is no question of resistance from the users that can undermine the possible application benefits.The well-planned design would ensure the optimal utilization of the computer resources and would help in the improvement of performance status.

4.1.3 TECHNICAL FEASIBILITY

The technical issue usually raised during the feasibility stage of the investigation includes the following:

- Does the necessary technology exist to do what is suggested
- Do the proposed equipment have the technical capacity to hold the data required to use the new system
- Will the proposed system provide adequate response to inquiries, regardless of the number or location of users
- Can the system be upgraded if developed
- Are there technical guarantees of accuracy, reliability, ease of access and data security

Earlier no system existed to cater to the needs of Secure Infrastructure Implementation System. The current system developed is technically feasible. It is a web based user interface for audit workflow at NIC-CSD. Thus it provides an easy access to the users. The database's purpose is to create, establish and maintain a workflow among various entities in order to facilitate all concerned users in their various capacities or roles. Permission to the users would be granted based on the roles specified. Therefore, it provides the technical guarantee of accuracy, reliability and security. The software and hard requirements for the development of this project are not many and are already available in-house at NIC or are available as free as open source.

Conclusion

The summarization of thepotential new threats in SDN. It have carried out threat modelling and

security assessment to evaluate the security of SDN. It have used three security metrics including the Network Centrality Measure, Vulnerability score, and attack impact metrics using the Threat model using TV-HARM. For our experimental analysis,and have observed different countermeasures and their effectiveness, demonstrating the applicability of the framework and TV-HARM to capture various threat vectors in SDNTraditional networks are complex and hard to manage. One of the reasons is that the control and data planes are vertically integrated and vendor specific. SDN created an opportunity for solving these long-standing problems. Some of the key ideas of SDN are the introduction of dynamic programmability in forwarding devices through open southbound interfaces, the decoupling of the control and data plane, and the global view of the network by logical centralization of the network brain. While data plane elements became dumb, but highly efficient and programmable packet forwarding devices, the control plane elements are now represented by a single entity, the controller or network operating system.

References:

[1] X. Sun and N. Ansari, "EdgeIoT: Mobile Edge Computing for the Internet of Things," IEEE Communications Magazine, vol. 54, no. 12, pp. 22–29, 2016.

[2] M. Maier, M. Chowdhury, B. P. Rimal, and D. P. Van, "The Tactile Internet: Vision, Recent Progress, and Open Challenges," IEEE Communications Magazine, vol. 54, no. 5, pp. 138–145, 2016.

[3] D. Kreutz, F. M. Ramos, and P. Verissimo, "Towards Secure and Dependable Software-defined Networks," in Proc. of the 2nd ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking (HotSDN 2013), 2013, pp. 55–60.

[4] D. Kreutz, F. Ramos, P. Veríssimo, C. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-Defined Networking: A Comprehensive Survey," IEEE, vol. 103, no. 1, pp. 14–76, 2015.

[5]M. Banikazemi, D. Olshefski, A. Shaikh, J. Tracey, and G. Wang, "Meridian: an SDN platform for cloud network services," *Communications Magazine, IEEE*, vol. 51, no. 2, pp. 120–127, 2016.