State University of New York Polytechnic Institute

School of Information Science and Technology

Department of Telecommunications

SECURITY CHALLENGES IN SDN IMPLEMENTATION

PRESENTED BY

Pradnya Patil

A research project submitted to the Faculty of Graduate Studies in partial fulfillment of

the requirements for the degree of

Master of Science in Telecommunications

May 2018

State University of New York Polytechnic Institute

SECURITY CHALLENGES IN SDN IMPLEMENTATION

A research project submitted to the Faculty of Graduate Studies in partial fulfillment of the requirements for the degree of

Master of Science in Telecommunications

Author

Pradnya Patil

Date of Successful Defense:

The Telecommunications Department has accepted the research project in partial fulfillment of the requirements for the degree of the ***Master of Science in Telecommunications*** at the ***State University of New York Polytechnic Institute.***

Dr. Larry Hash (Advisor) **Date**

Dr. Joshua White **Date**

Dr. Ali Tekeoglu **Date**

Abstract

This study analyzes how security challenges caused by data and control layer separation in the SDN, such as Denial of Service attacks and unauthorized access attacks, limit SDN deployment. This study also offers network engineers' views on preventing those security issues and whether implementing SDN is a good idea in the first place. This study was conducted in order to answer three questions:

1. How does data and control layer separation in SDN cause DoS and unauthorized access attacks?
2. What are the best practices and measures to minimize such security threats from the engineer's point of view?
3. Do security threats at the lower layer affect the decision to implement SDN?

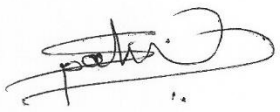
These questions were answered by reviewing research papers and interviewing engineers from the telecommunication field. DoS and unauthorized access attacks are due to vulnerabilities in OpenFlow, SDN switches and SDN controllers. Table 6 presents solutions for preventing DoS and unauthorized access attacks. Most of the network engineers said SDN should be implemented based on cost, limited risk, customers' positive views, and company projects, despite the current security challenges.

Declaration

I declare that this thesis represents my work, except where the due acknowledgment is made, and that it has not been previously included in a thesis, dissertation or report submitted to this university or any other institution for a degree diploma or other qualifications.

Pradnya Shankar Patil

Author



Date: 16th May 2018

Acknowledgment

Working on this thesis has been one of my most significant academic achievements and it would not have been possible without the following people's guidance and support.

My sincere and heartfelt thanks to Dr. Larry Hash, the advisor of this study, for being a constant inspiration and providing me with patient guidance, encouragement, and advice throughout my time as a student. I have been extremely lucky to have an advisor who cared so much about my work, and who responded to my questions and queries so promptly.

My special thanks to Dr. Joshua White for giving me the opportunity to meet so many interesting technical experts and for providing constant support and guidance.

My sincere thanks to Dr. John Marsh for his comments and suggestions to make this a rigorous study.

My humble thanks to Jessica Rivers for offering writing assistance.

I am thankful to all interviewees for offering their valuable insights.

Dedicated to my parents, husband, and friends

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

Technology has advanced rapidly. It has been an interesting journey in fields like computers, cell phones, software, processors, storage, virtualization, cloud computing, datacenters, artificial intelligence, Internet, and telecommunication. Networks are no exception. Traditional networks have changed tremendously and soon end users will have the power to choose and configure their networks with a single click.

Shortcomings of traditional networks

Traditional networks are difficult to manage and upgrade. Remember when network engineers had to go to locations to set up and manually configure network devices. If network service providers wanted to provide new services to the customers, they had to go through long procurement cycles (Doherty, J., 2016). Then, they had to hire skillful engineers and completely rely on their skills for accurate configuration of each device in the network (Doherty, J., 2016). Misconfiguration of devices could delay getting the services to the customers due to troubleshooting and reconfiguration of devices (Doherty, J., 2016). Also, each device had a limited life period in which it can perform efficiently (Doherty, J., 2016). Also, if there were customer service upgrades needed, then devices had to be upgraded or even replaced (Doherty, J., 2016). The network service providers realized they needed a network where automation, flexibility, scalability, reliability, and performance, could be achieved (Doherty, J., 2016). All these factors affected service provider's revenue (Doherty, J., 2016). In this 21st century, efforts of researchers have paid off. The invention of Software Defined Networking (SDN) made networks intelligent (Doherty, J., 2016).

Need for SDN

SDN is an approach to new network design (Doherty, J., 2016). It's a completely different way to build a network compared to the traditional networks. In traditional networks, control plane and data plane reside in the network device. The control plane is used to enforce network policies. It determines how individual packet can be handled. This information is pushed to the data plane. The data plane acts based on instructions provided by the control plane. SDN holds the possibility of leaving the endless loop of rebuilding networks, to keep them current (Doherty, J., 2016). In SDN, the controller is logically separated from the networking devices (Doherty, J., 2016). This design makes it easier to program the network This programming feature of the networks provides many profitable benefits. It provides automation, flexibility, scalability, and lower Opex and Capex (Doherty, J., 2016). With SDN, we can configure an entire network with a few clicks

We have never experienced this before! Now everyone is considering implementing SDN. The executive vice president of Juniper's software solutions division, Bob Muglia, said, "If you don't embrace the S.D.N. model, you'll be in trouble" (Hardy, 2013). If SDN is so beneficial, then why has it not already been implemented everywhere?

SDN implementation challenges

There are four challenges for SDN implementation: performance, security, scalability, and interoperability (Sezer, S., et al., 2013). Sezer at al. argue it is very difficult to achieve programmability/flexibility as well as high performance (processing speed) since multi-core CPU, NPU, PLD, ASSP and custom ASIC processors used for

network control either provide high processing speed or flexibility (Sezer, S., et al., 2013). it is difficult to achieve scalability for the controller and network nodes as it will add a lot of complexity in processing and operation of the controller (Sezer, S., et al., 2013). there is a need to develop hybrid SDN infrastructure so that traditional and SDN-enabled devices can work together (Sezer, S., et al., 2013). The cost is another most significant challenge to implementing SDN-infrastructure as decision-makers may not be willing to invest money in replacing traditional networks with SDN networks. The authors show the biggest concern, though, is security issues associated with SDN model (Sezer, S., et al., 2013).

Problem statement

This study mainly focuses on security issues, such as denial of service attack and unauthorized access attacks, associated with SDN. How do these security issues affect the choice of implementing SDN for engineers from the telecommunications field? What SDN architectures and implementation solutions are there according to engineers from the telecommunications field?

Thesis Statement

"Determine the effects of DoS and unauthorized access security exposures have on network engineers' choice to implement SDN."

Delimitations

This study focuses on denial of service attacks and unauthorized access attacks due to configuration out of six security issues present at the lower layer of SDN, which are discussed in greater detail in chapter 4. These attacks are easy to launch and affect entire network. The paper claims that 1000 bot infected computers can be rented just for

$25 in the US to launch a DoS and, if a DoS is not prevented within 3 seconds then entire network will get affected (Shin, S., & Gu, G., 2013. Also, there are no mandatory and robust security provisions made in SDN to prevent unauthorized access attacks as it completely relies on engineer's willingness and actions. However, the cost, one of the challenges for SDN implementation, has not been studied as engineers from the telecommunication field may not willing to share company's financial details. Also, performance, scalability and interpretability have not been studied as the researcher believes these are not as significant as security.

Significance of the problem

1. On reading this thesis, technical personnel will know best practices and measures to prevent DoS and unauthorized access attacks for the SDN.

2. If best practices are implemented, it may improve security in the network.

3. On reading this thesis, manufacturers or researchers will know the best SDN architectural approach to prevent DoS and unauthorized access attacks.

Limitations

1. The genuineness of information provided by each interviewee could be limited.

2. There is no certainty that the suggested measures and practices to prevent security attacks will increase the deployment rate of the SDN in the future.

For this study some background information is needed. Therefore chapter 2, 3, and 4 discuss aspects of SDN: definition of it, three approaches to SDN architecture to provide security, and security challenges for it. Chapter 5 presents a literature review regarding SDN security issues and implementation. Chapter 6 describes the research methodology. In addition, it contains information on how this study was analyzed and

validated. Chapter 7 includes details of pilot interviews. Chapter 8 presents a summary of the interview data. Chapter 9 contains the conclusion of the interview summary and recommendations for reducing security threats. In the last chapter, recommendations for the SDN community and for the further study are given.

We will begin by understanding software defined network architecture models in detail in the next chapter.

Chapter 2: SDN

What is SDN?

According to Open Networking Foundation SDN is ‘‘an emerging network architecture where the network control is decoupled and separated from the forwarding mechanism and is directly programmable’’ (O.N.F., 2012). Figure 1 is drawn from the information present in both the papers "Software-defined networking: A survey" and "A survey of software-defined networking: Past, present, and future of programmable networks".

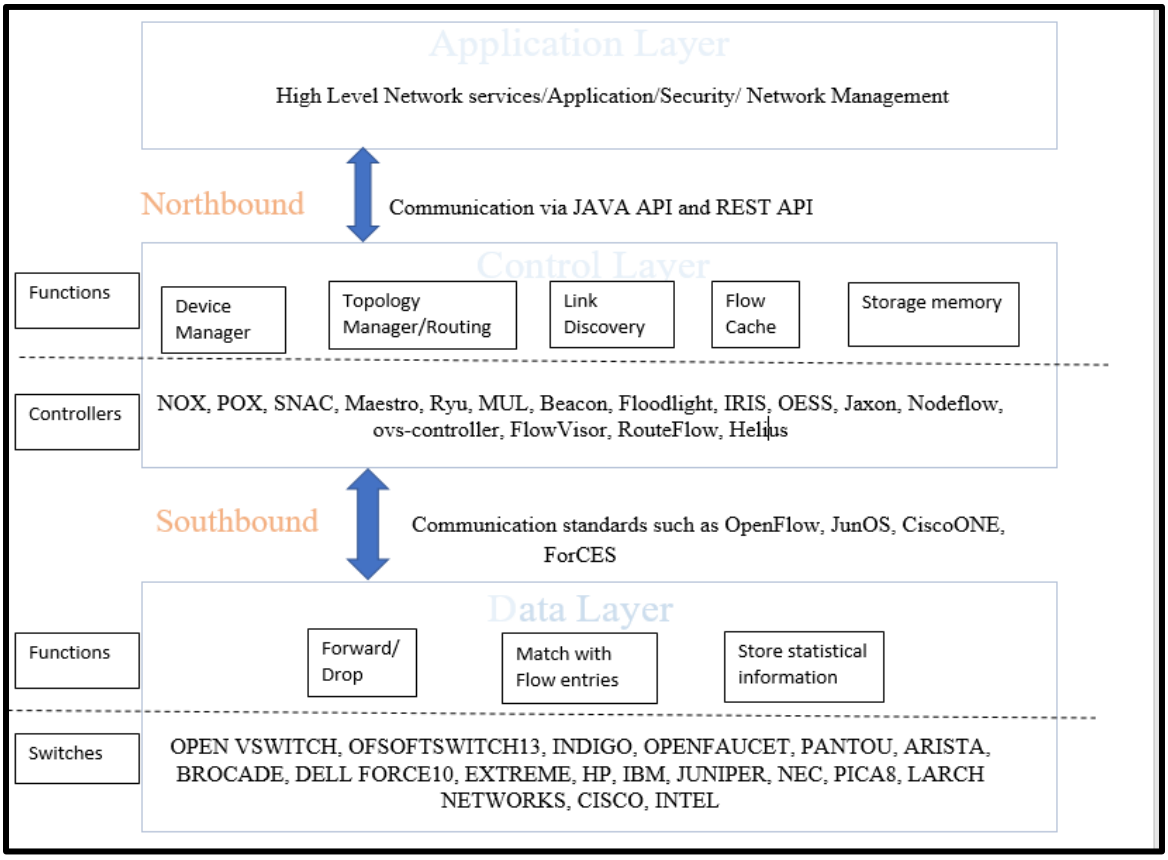


Figure 1: SDN Architecture

There are five main components for SDN (Farhady, H., Lee, H., & Nakao, A., 2015).

i. Data plane

ii. Southbound

iii. Control plane

iv. Northbound

v. Application plane

The data plane, control plane and application plane are also referred as layers of SDN architecture. And, southbound and northbound are referred as interfaces between data and control layer and the interface between control and application layer respectively.

Data Plane:

The forwarding devices can be routers, switches, NAT, firewalls or function which process on packet handling rule (Farhady, H., Lee, H., & Nakao, A., 2015). These forwarding devices can be categorized into Pure and Hybrid devices (Nunes, B. A. A, et al., 2014). Pure devices are completely dependent on the controller for forwarding decisions (Nunes, B. A. A, et al., 2014). However, Hybrid devices are dependent on both OpenFlow as well as traditional operations and protocols (Nunes, B. A. A, et al., 2014). Hybrid Switches are available commercially (Nunes, B. A. A, et al., 2014). The list of the SDN switches is given in figure 1.

There are various approaches when it comes to processing and installing forwarding rules. Some research papers talk about adding general purpose CPU on the switch or nearby to offload complex ASCIC design, which is present in the traditional network devices (Nunes, B. A. A, et al., 2014). Some papers suggest using network processor-based acceleration card or Linux systems to reduce packet delay and improve

throughput (Nunes, B. A. A, et al., 2014). Primary Openflow forwarding devices support a few hundred, thousand rules, which are complex, and TCAM is used to store these rules, which is expensive and power draining (Nunes, B. A. A, et al., 2014). Various papers show concern about memory limitation in the forwarding devices (Nunes, B. A. A, et al., 2014).

Southbound:

This layer is responsible for communication between data and control plane. The popular standard that makes this possible is ONF standardized the OpenFlow standard (Nunes, B. A. A, et al., 2014). The details of OpenFlow haves been provided in the second section. There are few vendor specific commercial standards such as CiscoONE, JunOS, etc. (Farhady, H., Lee, H., & Nakao, A., 2015).

Control plane:

The control plane consists of centralized or distributed and physically or logically separated controllers (Nunes, B. A. A, et al., 2014). These controllers provide a programmatic interface to implement management tasks and offer new functionalities to the network (Nunes, B. A. A, et al., 2014). Built-in controller modules communicate with Java based applications and other applications through JAVA API and REST API respectively (Nunes, B. A. A, et al., 2014). Controllers provide high scalability and performance to the network. OpenFlow controller NOX-MT can handle up to 1.6 million new flow requests per second and new controller McNettle, which is under development, claims to manage 5000 switches (Nunes, B. A. A, et al., 2014). Current controllers are implemented in Python, C++, Java, C and Java script programming languages (Nunes, B. A. A, et al., 2014). The list of the controllers is given in figure 1.

Northbound:

There has been no standard for communication between controller and application. This interface is defined in software and implemented on an ad hoc basis per application (Nunes, B. A. A, et al., 2014).

Application plane:

The application layer is responsible for high level network services such as network management, load balancing, providing security, and traffic engineering (Nunes, B. A. A, et al., 2014).

OpenFlow

Figure 2 shows the architecture of the lower layer of OpenFlow based SDN.

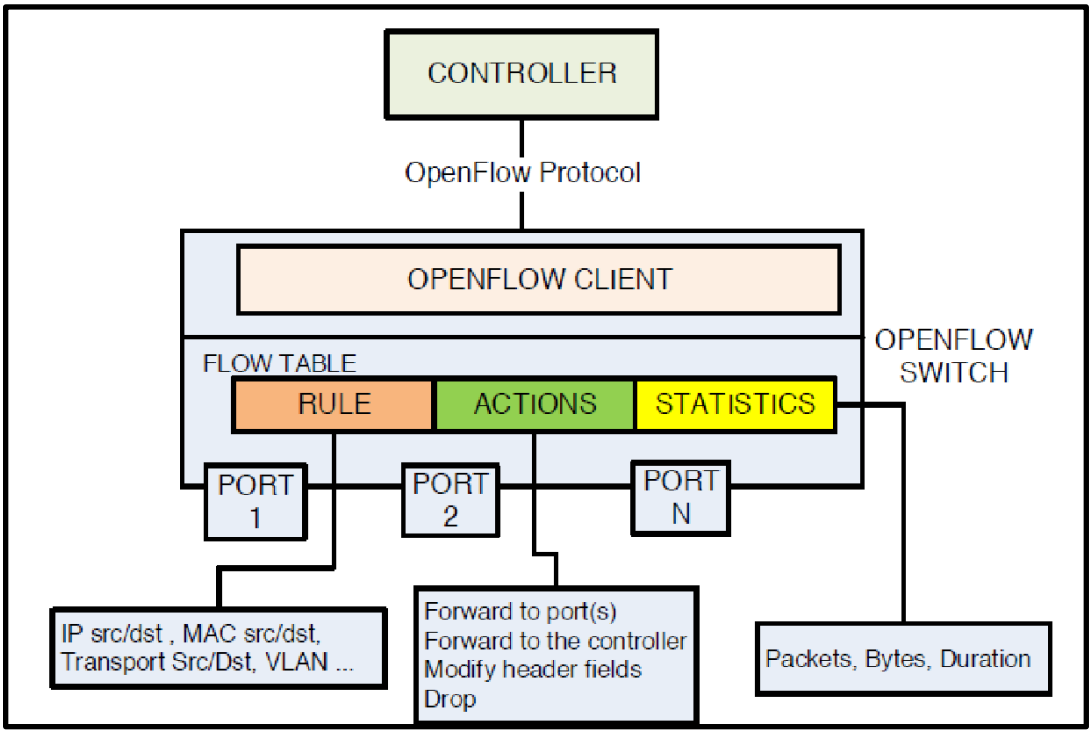


Figure 2: Working of OpenFlow Protocol

Source: Figure 2 has been retrieved from https://hal.inria.fr/hal-00825087v5/document

Forwarding devices include one or more flow tables (Nunes, B. A. A, et al., 2014). Flow tables consist of many flow entries, which define process and flow of the packet (Nunes, B. A. A, et al., 2014). Flow entries consist of match fields, counters and set of instructions (Nunes, B. A. A, et al., 2014). When a packet arrives at the forwarding device, it tries to match information present in the packet header, ingress port and metadata to the flow entries (Nunes, B. A. A, et al., 2014). If packet information matches with flow entry, appropriate actions or set instructions go to the packet (Nunes, B. A. A, et al., 2014). If the packet does not match with flow entries of any of the flow tables, it is sent to a controller or dropped or forwards using IP forwarding schemes (Nunes, B. A. A, et al., 2014). Counters are responsible for collecting statistical data such as the number of packets, number of Bytes and duration (Nunes, B. A. A, et al., 2014). With the help of OpenFlow protocol, the controller can update forwarding devices proactively or reactively (Nunes, B. A. A, et al., 2014). OpenFlow protocol supports IPv6 extension header, MPLS BoS bit, optical ports, and capability of flexible classification of flow matching (Farhady, H., Lee, H., & Nakao, A., 2015).

Chapter 3: SDN architectural approaches

There are three SDN architectures approaches to mitigate SDN security issues. These approaches can be used to monitor networks, to detect attacks or instructions, or to authenticate users.

More control to switches for security

Nowadays enterprise security is heavily dependent on middleboxes and host security. However, this creates problems when implementing protocols to interact with each other. It also slows down the response to the attack. Nayak et al. suggest Resonance system secure enterprise networks by implementing dynamic access control policies based on alerts and flow level information (Nayak, A. K., et al., 2009). Resonance systems are nothing but programmable switches that take care of security threats at the lower layers (Nayak, A. K., et al., 2009). These programmable switches either drop or redirect the packets based on higher level security policies and inputs from monitoring and interference systems (Nayak, A. K., et al., 2009). Today's networks rely on reactive or ad hoc approaches. Middleboxes or intrusion detection systems are used to prevent unauthorized or other types of attacks. Interacting with these boxes and maintaining security could be crucial. Instead, Resonance controls traffic as controller suggests the switches by implementing policies and monitoring state and security class of the end users (Nayak, A. K., et al., 2009).

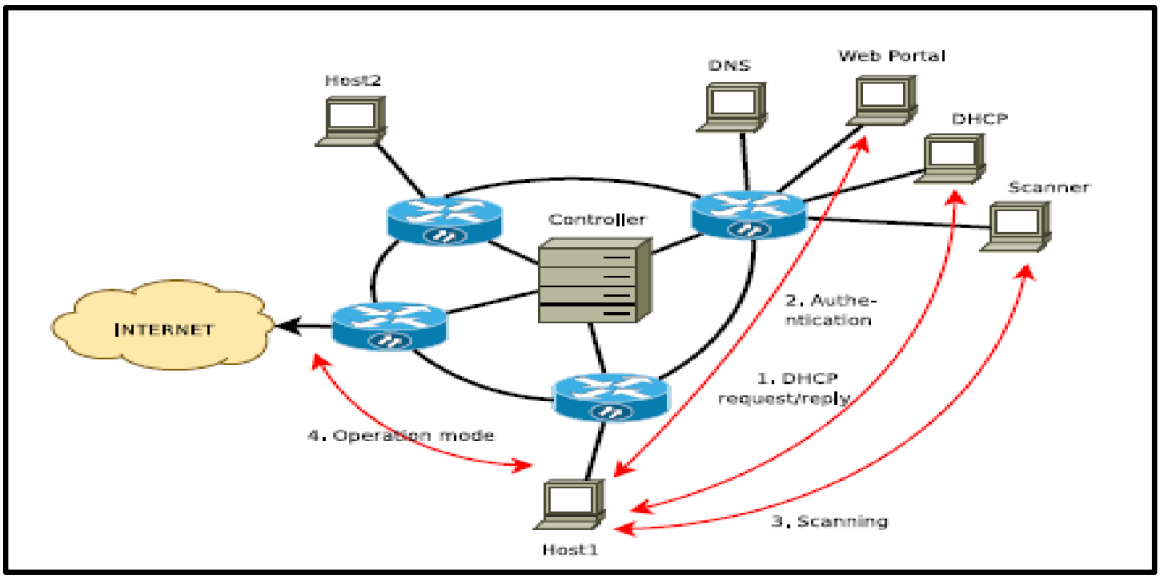


Figure 3: Network Diagram to explain Resonance System

Source: Figure3 has been retrieved from

https://www.cs.princeton.edu/courses/archive/fall10/cos561/papers/Resonance.pdf

In figure 3, there are 2 hosts, 1 controller, 4 Openflow switches and 4 servers which are DNS, Web Portal, DHCP and scanner (Nayak, A. K., et al., 2009). When a new host is introduced into the network, the controller checks it for three events in a registration state (Nayak, A. K., et al., 2009). First, if the host requests DHCP and ARP communication, then the controller installs forward packets flow entry to the switch (Nayak, A. K., et al., 2009). Second, if the host requests http request, then the controller installs redirect traffic flow entry to the switch, to redirect traffic to the web registration portal and scanner to authenticate host (Nayak, A. K., et al., 2009). Lastly, controller installs drop packet flow entry into the switch if above two events do not take place (Nayak, A. K., et al., 2009). Once the host is authenticated, the controller installs flow table entries into switch based on security class and state of each MAC address for

normal operation (Nayak, A. K., et al., 2009). Then, the controller listens for the state change update for the MAC addresses with the help of network monitoring alerts (Nayak, A. K., et al., 2009). The state can be changed according to set of transition defined by policies for the host (Nayak, A. K., et al., 2009). If the controller detects state transition, then controller again update flow entries in the switch in which host will be again asked to authenticate (Nayak, A. K., et al., 2009). The important feature of the resonance system is that it enables dynamic access control (Nayak, A. K., et al., 2009). This is possible as resonance is coupled with distributed interference-based alert system and programmable switches (Nayak, A. K., et al., 2009).

Integrating Middleboxes for security

Openflow standard is based on an easy match/action interface. It can be advanced for deep packet inspection and can operate at a higher layer (Bilal Anwar., et al., 2013). However, this requires advance hardware and standardization which can't be achieved immediately (Bilal Anwar., et al., 2013). On the other hand, current middleboxes have high processing and storage capacity to provide high performance and security (Bilal Anwar., et al., 2013). The paper presented on SIMPLE (Software-DefIned Middlebox PoLicy Enforcement) approach suggests that SIMPLE can allow the network operator to specify logical middle-box routing policy and automatically translate into OpenFlow-based forwarding rules (Qazi Z. A., 2013). This is an excellent approach to work within confines of existing SDN capabilities without modifying middlebox implementation (Qazi Z. A., 2013). To integrate middleboxes into SDN networks, three challenges need to be addressed: middlebox composition, load balancing and packet modification (Qazi Z. A., 2013).

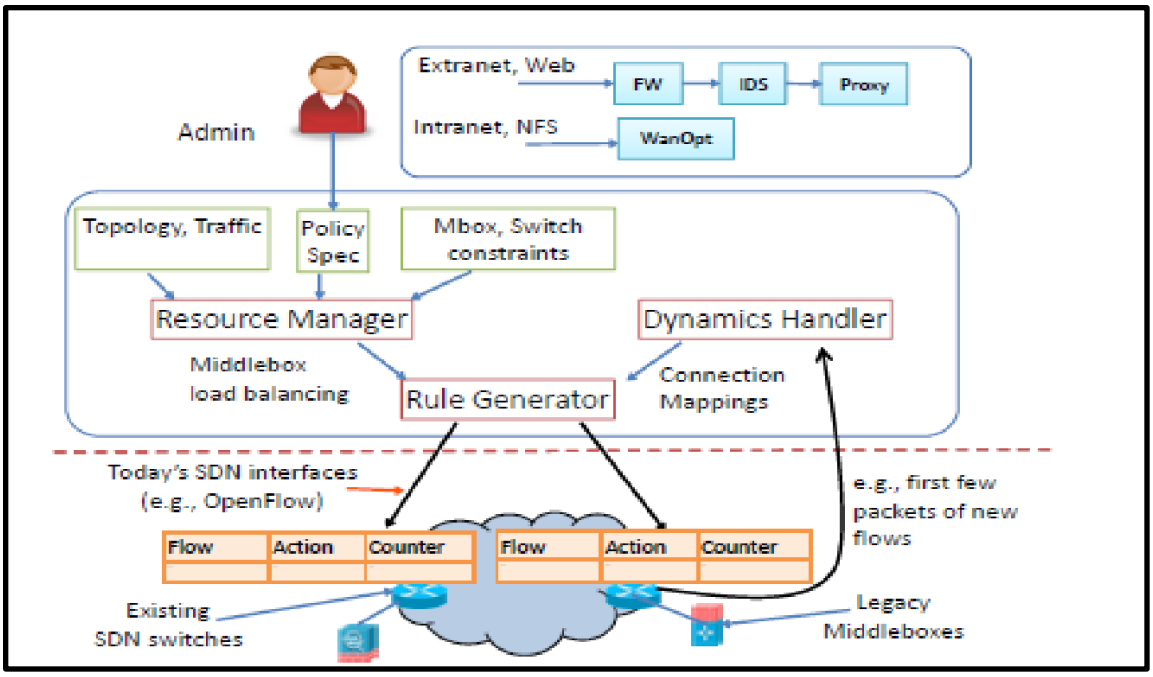


Figure 4: SIMPLE Approach

Source: Figure 4 retrieved from

https://www2.cs.duke.edu/courses/cps296.4/fall14/Papers/SIMPLIFY-sigcomm13.pdf

Figure 4 shows an overview of the SIMPLE approach (Qazi Z. A., 2013). There are three important modules in SIMPLE: Resource Manager, Rule Generator and Dynamics Handler (Qazi Z. A., 2013). The resource manager takes network traffic data, topology and policy requirement as input and outputs middlebox processing allocation (Qazi Z. A., 2013). The Resource Manager balances out the load on switch and middleboxes by using hard offline components for switches and efficient online components for middleboxes (Qazi Z. A., 2013). Switches have limited TCAM space and middleboxes get overloaded because of processing of deep packet inspection. The Dynamics Handler uses lightweight flow correlation mechanism with inputs from SDN network reports (Qazi Z. A., 2013). Middleboxes and SDN switches should know where

packet header and payloads have been changed. This information is required to maintain an accurate sequence of physical devices (firewall + IDS + PROXY) for web traffic (Qazi Z. A., 2013). However, because of proprietary logic inside of middleboxes, lightweight correlation mechanics do not work efficiently (Qazi Z. A., 2013). Therefore, SIMPLE also describes using SIMPLE data planes, in which tunnels between switches and packet header are tagged with processing state tags if switches are connected in loops (Qazi Z. A., 2013).

On the other hand, Slick architecture proposes decoupled control planes for middleboxes (Anwer, B., et al., 2013). It includes three elements: Control plane protocol, programming model and slick controller (Anwer, B., et al., 2013). A Slick control plane protocol allows the controller to run multiple concurrent pieces of code on middleboxes (Anwer, B., et al., 2013). In the slick programming model, policies are enforced by applications that split into multiple executables and run across middleboxes simultaneously (Anwer, B., et al., 2013). The slick controller supports heterogeneity, element placement and traffic steering (Anwer, B., et al., 2013).

Defense mechanism on top of network OS

Monitoring applications or defense mechanisms are used to prevent attacks. The paper mentions using random virtual Internet Protocol addresses to hide real IP addresses, using Self Organizing Maps to detect abnormal flows, using CloudWatcher to inspect packets, or using ALARMS policy to manage and route traffic with the help of SDN controller (Scott-Hayward., et al., 2013). Figure 5 depicts overall architecture for CloudWatcher. There are 3 main components in CloudWatcher such as device and policy manager, routing rule generator and flow rule enforcer (Shin, S., & Gu, G., 2012).

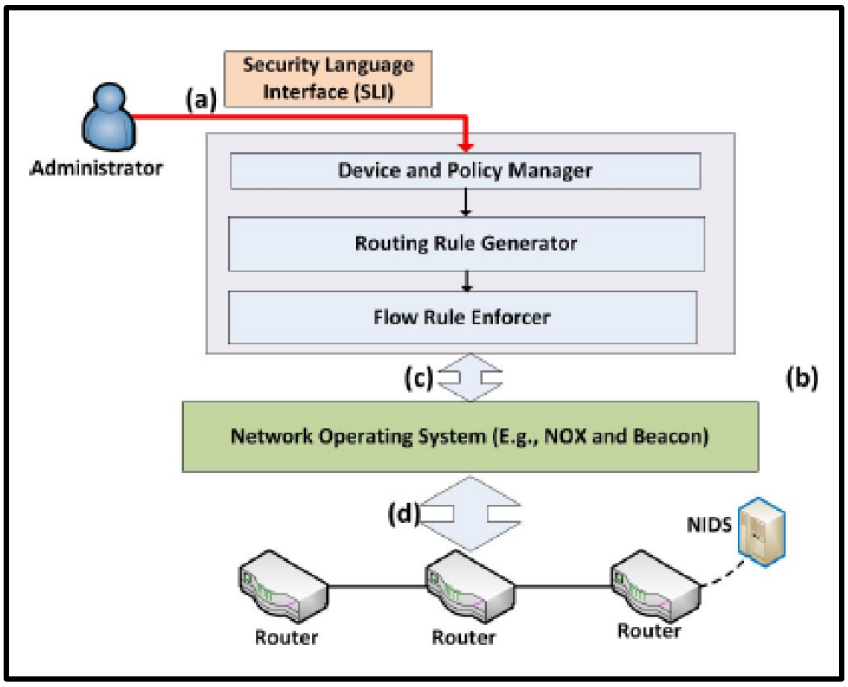


Figure 5: CloudWatcher

Source: Figure 5 retrieved from http://faculty.cs.tamu.edu/guofei/paper/CloudWatcher-NPSec12.pdf

The device and policy manager manage security device information such as device ID, location function, mode, type, etc. (Shin, S., & Gu, G., 2012). The routing rule generator is responsible for packet handling rule for each flow (Shin, S., & Gu, G., 2012). For example, the administrator can create a security policy with two fields such as flow condition and device set (Shin, S., & Gu, G., 2012). The flow condition represents a flow to be investigated and a device set display necessary for security device investigation (Shin, S., & Gu, G., 2012). The flow rule enforcer passes down generated flow rules to switches. If CloudWatcher finds packets meeting flow condition, then it will route packets to satisfy security requirements (Shin, S., & Gu, G., 2012).

Chapter 4: Security issues at lower layers of SDN

As we know, SDN can achieve flexibility, scalability, creativity, automation, and rapid innovation in the network since the control layer (software) has been decoupled from the data layer (hardware). However, this facility can lead to various security issues. there are six key security issues associated with the lower layer: unauthorized controller access, data leakage, data modification, malicious application, denial of service attacks due to controller switch communication floods and switch flow table flooding and configuration problems (Scott-Hayward., et al.'2013).

Data leakage

According to a Seungwon Shin and Guofei, an attacker can fingerprint the SDN network (Shin, S., & Gu, G., 2013). The authors demonstrated an SDN fingerprinting attack on remote networks with the help of a HFC (Header field change) scanner (Shin, S., & Gu, G., 2013). There are two common assumptions. First, the remote network can allow TCP connections or ICMP ping. Second, SDN network flow is controlled with fine-grained level (4 tuples i.e. IP addresses and ports of source and destination) to provide better load balancing and control compared to traditional networks. Researchers can fingerprint SDN network by collecting and analyzing data of response times of the probing packets (Shin, S., & Gu, G., 2013).

Denial of service attack

an attacker can launch denial of Service attacks on the control and data layer by flooding forge packets (Shin, S., & Gu, G., 2013). After a successful attempt of identifying SDN network, researchers further consumed resources of data and control layer of SDN network, which resulted into denial of service attacks (Shin, S., & Gu, G.,

2013). If attackers rent 100 bot infected hosts who send packets at 200 bps as well SDN network is using HP 5406zl switch which supports OpenFlow functions and 1500 flow rules (Shin, S., & Gu, G., 2013). Then, denial of service attacks can't be prevented if attacking packets have not stopped within 3 seconds at data layer even though SDN networks might have defending mechanisms (Shin, S., & Gu, G., 2013). In addition, this attack can be launched by an attacker with the minimal cost since it is possible to rent 1000 hosts for only 25 dollars in the US (Shin, S., & Gu, G., 2013). However, the authors have suggested some possible defending techniques. First, we should change the condition of the flow rule to compress flow rules even though it compromised load balancing (Shin, S., & Gu, G., 2013). Second, the control layer should provide variable setup times to infuse the HFC scanner, which will fail attempts of SDN fingerprinting (Shin, S., & Gu, G., 2013).

Configuration issues

The unauthorized access to control layer or data layer is one of the major concerns related to OpenFlow protocol-based switches and controllers. OpenFlow protocol has introduced TLS (Transport Layer security) to prevent unauthorized access. However, TLS has been made optional in the OpenFlow (Benton, K., et al., 2013). In addition, it needs higher technical configuration such as generating a sitewide, controller and switch certificates (Benton, K., et al., 2013). Next, devices sign the certificates with the site-wide private key (Benton, K., et al., 2013). Finally, all the devices should be configured with installing the correct keys and certificates (Benton, K., et al., 2013). If SDN network has distributed controllers then using TLS will increase the complexity (Sezer, S., et al., 2013). In addition, the specification of the TLS in the Openflow standard has not

mentioned (Sezer, S., et al., 2013). This vulnerability in the OpenFlow specification may allow an attacker to impersonate the controller, which can lead to fraudulent rule insertions and rule modifications resulting in man-in-the-middle attacks and Dos attacks (Benton, K., et al., 2013). Though TLS resolves most of the unauthorized security issues, it can add to costs of implementation (Benton, K., et al., 2013). Further, we can use auto-generated keys and trust-of-first-use method, but it will require skillful operators and time (Benton, K., et al., 2013).

Unauthorized access attack

Some SDN switches support additional "listener mode" which is used for easy debugging and verifying rule states without adding load to the controller (Benton, K., et al., 2013). This mode does not have any built-in security mechanism to control access or to authenticate users (Benton, K., et al., 2013). This mode accepts connection from any sources, therefore any source can write rules in switches or read information from them (Benton, K., et al., 2013).

Data modification

There are a few SDN switches and controllers available which support TLS for authorization (Benton, K., et al., 2013). The Openflow switch vendors who do not support TLS are HP, Brocade, Dell, Indigo and Pica8 (Benton, K., et al., 2013). The openflow switches OpenWRT, OpenvSwitch and only IP8800 model from NEC support TLS (Benton, K., et al., 2013). The popular Openflow controller vendors who do not support TLS are POX, Beacon, Floodlight, Mul and FlowVisor (Benton, K., et al., 2013). The NOX controller verifies switches with certificates, but it does not authenticate switches (Benton, K., et al., 2013). The FlowVisor controller can be configured with

TLS, but it does not provide TLS connection for switches (Benton, K., et al., 2013). Only Open vSwitch controller supports TLS (Benton, K., et al., 2013).

Due to the absence of TLS, an attacker can gain access to the switch or controller and can modify rules to modify packet (Scott-Hayward., et al.'2013).

Malicious applications

The Flowvisor and Fortnox are used to rewrite controller-created rules to restrict their effects or to add role-based authentications to execute many Openflow applications (Benton, K., et al., 2013). Attackers can masquerade as these applications to modify, record, duplicate or block network traffic (Benton, K., et al., 2013). With malicious applications, the controller can be hijacked and lower layers of the SDN can be affected (Scott-Hayward., et al.2013).

Chapter 5: Literature Review

Research papers summary

The first paper claims that the security of the SDN is one of the main challenges in the SDN-based cloud (Yan, Q., Yu, F. R., Gong, Q., & Li, J., 2016). The paper lists many security threats in SDN such as unauthorized access, data leakage, data modification, malicious applications, configuration issues and Denial of service attacks (Yan, Q., Yu, F. R., Gong, Q., & Li, J., 2016). In addition, the paper mentions seven potential threats such as forged or faked traffic flows, attacks on vulnerabilities in switches, attacks on control plane communications, attacks on and vulnerabilities in controllers, lack of mechanisms to ensure trust between the controller and management applications, attacks on and vulnerabilities in administrative stations, and lack of trusted resources for forensics and remediation (Yan, Q., Yu, F. R., Gong, Q., & Li, J., 2016). However, the paper mainly provided a comprehensive survey to prevent the DDoD attack since the SDN-based Cloud is still in a concept phase (Yan, Q., Yu, F. R., Gong, Q., & Li, J., 2016).

The second paper provides a comprehensive survey of SDN/OpenFlow implementation, in which the pros and cons of security concerning SDN have been included (Hu, F., Hao, Q., & Bao, K., 2014). The paper states that SDN has created new targets such as SDN controller, virtual infrastructure and OpenFlow network for potential security attacks (Hu, F., Hao, Q., & Bao, K., 2014). The paper describes several schemes such as Intrusion Detection, Modular security, SDN traffic anomaly Detection, Language-Based security, Loop Detection Problems and SDN failure recovery that overcome natural fault and intentional attacks (Hu, F., Hao, Q., & Bao, K., 2014).

The third paper claims that security is one of the challenges for implementation of SDN (Sezer, S., et al., 2013). The paper suggests that there must be more focus on security as there has been a limited discussion on security from industry and research community (Sezer, S., et al., 2013). The paper shows concern regarding authentication and authorization mechanism present across SDN platform (Sezer, S., et al., 2013). Also, the paper shows concern regarding DoS attacks which happen due to bottlenecking the switch memory element and easily hackable SDN by using open interfaces and known protocols to program networks (Sezer, S., et al., 2013).

Uniqueness

The third paper highly influences this study. However, the study only concentrates on DoS and unauthorized access attack and gathers information from telecommunications engineers to find solutions for the security issues and opinions regarding SDN implementation. In additions, it provides the best SDN architectural approaches to mitigate security issues.

Chapter 6: Methodology

Why interview?

Qualitative and quantitative methods are used to collect data for empirical investigations (Kuada, J., 2012). A qualitative method such as interviewing was employed to provide insight regarding the best measures and practices to prevent DoS and unauthorized access attack within SDN. The views and opinions of the engineers from the field of telecommunications were sought regarding SDN implementation.

Qualitative interviews can be structured, semi-structured or unstructured (Edwards, R., & Holland, J., 2013). A Semi-structured qualitative interview methodology was employed for this study. The Semi-structured interview method is beneficial as it allows the participant to express their feelings, opinions, and perspectives (Edwards, R., & Holland, J., 2013). The semi-structured interview helps discover fresh insights into the theories rather than confirming existing findings.

Qualitative interviews provided deeper insight about SDN and their benefits and issues. Researcher was benefited with new learnings such as SDN products, integration of multiple technologies with SDN. It allowed to find exceptions to the generalized information. For example, exceptions to the benefits of SDN. The qualitative interviews helped to find the solutions on the security issues which is used by the network engineers in their daily job duties.

Participant selection criteria

The interviewees from the field of networking and network security were sought as a part of this study. Participants' backgrounds:

i. Professor

ii. IT consultants
iii. Network Software Engineer
iv. System Administrator
v. Cloud specialist

One of the methods to select interviewees is called snowballing (Edwards, R., & Holland, J., 2013). In this method, contact is made with the participants through any route available, and then other contacts are found through these first participants.

The following routes were employed to find participants:

i. Through family and friends' network
ii. Through colleague's network
iii. Through professor's network
iv. By posing a question to SDN interest group on the internet, LinkedIn, Researchgate.
v. By searching YouTube videos related to SDN and contacting presenter through contact information mention in the description of the video.

One participant was found through a personal connection. Two participants were found through friend and family connections. Five participants were found through a professor's connection. Many requests were sent to members of the SDN interest groups on LinkedIn. Two participants were found via LinkedIn.

The interviewees' selection was not based on gender or ethnic background. Participants were healthy during the process of interviews. The eligibility of the participants was assessed through their answers to screening questions sent through text

messages. In addition, the interview questions were sent via email to the prospective interviewees before interviews were scheduled with advisor's feedback and approval. The email helped interviewees to understand the objectives and commit to participate in the interview process.

Development of interview questions

The Interview draft was designed for engineers with experience in the field of networking and network security. There were 13 to 15 questions, mostly open ended. The interview questions were semi-structured. The questions were written in such a way that participants would not feel threatened about sensitive data. The questions were formed using the researcher's area of interest and existing literature. Also, valuable feedback and suggestions from Dr. Larry Hash were incorporated into the interview questionnaires. The interview questions draft has been included in appendices.

The Institutional Review Board (IRB) reviewed the research methodology and interview question drafts to assure that appropriate steps had been taken to protect the rights and welfare of humans participating as subjects in the research. An IRB Exemption approval letter was approved before commencing interviews. With advice from Dr. Michael Manning, IRB Chair SUNY POLY, the researcher successfully completed training in "Students in research (ID: 1321)" module/course. The "Students in research (ID: 1321)" completion report and Exemption approval letter are included in the appendices.

Furthermore, the pilot interviews were conducted to improve interview questions and to evaluate the feasibility of the study. All details related to pilot interviews are included as part of chapter 7: Pilot interviews.

Interview procedure

All 10 interviews were planned to be in-person. Two interviews were set-up in-person in Utica, NY. Three interviews were attended via video/audio conference. Four interviews were scheduled over the phone and one interview response was obtained via email. All interviews were successfully completed on first scheduled date and time except one. The researcher experienced saturation at around 10 interviews as there were no additional learnings gained. Hence, in total 10 interviews were conducted as part of this study.

The duration of the interview was scheduled for 30 to 45 minutes so that the interviewees could take time to get comfortable and answer the questions without any stress. The actual duration of the interviews varied from 15 to 45 minutes.

At the start of the interview, the objective of the study was explained to participants. Then, the researcher requested participants' permission to record the interview. Also, they were informed about their rights. Participants were free to decline to answer any question at any time and participants were free to withdraw from this study/interview at any time. Interviews were started by asking easy questions regarding professional experience or about SDN to make interviewees comfortable. Then, questions related to security incidents, preventive measures, SDN security, SDN architectural approaches were asked to the participants.

Data collection

The data was collected by audio taping or video recording. in-person interviews were recorded through Voice Memo, an in-built application in iPhone 6S mobile. Skype conversation was recorded through Evaer by purchasing a standard license key. Other web conferences were recorded on Voice Memo.

The researcher transcribed the recorded responses. Consequently, the researcher summarized the transcribed data and used summarized data to conclude. A Summary of the interviews has been included in chapter 8.

Data analysis

All transcripts were read in detail, labeled, and highlighted relevant words, phrases, etc. The relevance was decided based on the data presented in scientific articles or repeatability of the concept or importance to the study or surprise factor. Several sections/themes such as the definition of SDN, benefits of SDN, factors against the choice of SDN, best architectural approach, solutions to prevent security issues, opinion on TLS and opinion on SDN implementation were recurring in all the transcripts. However, there were other themes such as security incidents that were not repeated but relevant to the study. In this way all transcripts were summarized, and all sections/ themes were written without interpreting the data. The summary was shared with the advisor to check for unbiasedness.

Further, the researcher looked for connections between themes, hierarchy, relevant statements, relevant quotes to draw a conclusion. Finally, the summary was interpreted and discussed under heading summary conclusions based on theories and other relevant aspects. The opinion of the researcher regarding study is included in overall conclusions.

Data validation

According to Bryman and Bell, qualitative studies can be evaluated based on trustworthiness and authenticity (Kuada, J., 2012). Evaluation of trustworthiness is based on credibility, transferability, dependability, and conformability (Kuada, J., 2012). And, authenticity involves fairness of the investigations (Kuada, J., 2012).

The credibility of the research was achieved by sending interview transcripts to the interviewees after the interview. So, the researcher confirmed that she had understood responses correctly. Transferability was achieved by providing details regarding past and present research work through the literature review and stating uniqueness of the study so that future researcher can refer to the study. Dependability was achieved by maintaining records of the research phases such as problem statement formulation, interview transcripts, etc. Conformity was achieved by maintaining all necessary standards, rules and laws related to the study under the thesis advisor's guidance. In this way, the trustworthiness of the study was achieved. Finally, authenticity was achieved by including all sources in the bibliography.

Chapter 7: Pilot interviews

Why pilot interviews?

Pilot interviews play a significant role in a qualitative research methodology. Three pilot interviews were conducted to test mentioned areas:

Questions are structured properly.

i. The questions do not offend Participants.
ii. Proper posture of the interviewer/researcher where interviewees will not get offended.
iii. Questions are arranged properly.
iv. Questions are unbiased.
v. If there is need to add, change or remove the questions.

The first pilot interview was conducted over a Skype video call with the researcher, pilot participant 1 and the thesis advisor. Second and third pilot interviews were in – person interviews with the researcher. These interviews helped the researcher learn about interview protocols.

Pilot participants detail

All pilot participants were found through a personal connection. Being a master's student in Computer and system networks field, t was easy to connect with classmates and schedule interviews.

The first pilot participant is a Master's in telecommunication and working as a network administrator in IT company which provides services like cloud computing, enterprise application, content management, information assurance, etc. The second pilot participant is a master's in Telecommunications and has worked as a Network

Technician, IT engineer and system administrator for various systems, networking devices, security devices, servers, IT infrastructure related applications and services. The third pilot participant is pursuing a master's in Telecommunication and working on SDN related project as part of degree work.

Pilot interviews summary

All pilot interviews were recorded using Voice memo in iPhone 6s and Evear application for Skype. Recordings were transcribed by the researcher and validated by pilot participants. Later, transcribed pilot interviews were summarized and used to draw conclusions.

For the first pilot participant, the question "Are you considering implementing SDN?" was asked. Pilot participant 1 answered that they are not considering implementing SDN presently therefore he can't say much about SDN, but he is aware of the technology. Pilot participant 1's careful selection of words reshaped the interview questions. The question was replaced with another question "what is SDN?" This question was asked to all remaining pilot participants and all participants.

From now on wards Pilot Participant will be noted as PP. Numbers are given as per chronological order.

According to PP 2, SDN is the next step in networking. PP2 also compared traditional networks and SDN model and stated that in traditional networks, each device has full control over decision making and configuration. In contrast, SDN has a programmable software which is run on single or group of devices to provide control information and configuration. PP 3 stated that SDN provides architecture with decoupled control and

data plane. The network operator can control and manage networks through centralized programmable control plane.

All PPs believe that SDN is beneficial. According to PP1, SDN is more beneficial to larger companies compared to smaller companies because of its automation feature. According to PP2, SDN simplifies operation for end devices and increases efficiency because of centralized controller resulting in the low financial cost. All PPs said that adding new applications, adding services, and upgrading is very easy in SDN.

For PP1, the question "is security one of the major components in the field of networking? Do you believe security is better in SDN" was asked. PP1 stated that there are possibilities of security issues because of a human configuration error, in that case SDN is better. This question was replaced with "what are the factors that will lead to choosing SDN in the network?" for all other PPs and all participants. This change was made as Wh-questions allow participants to respond openly. PP2 and PP3 stated that SDN would be chosen for its ability to fast upgradation of services and network without any downtime.

No PPs had experienced any security breach in their networks. PP1 said that in their company they separated management and data traffic by providing required access and privileges to the employees. Also, all unused open ports are disabled. According to PP2, the most important security aspect of the network is preventing a Denial of Service attack as it can lead to no service for the customer resulting in a financial loss. Therefore, in the company, security applications and security devices are used to provide security at different layers. All devices are secured physically too. PP2 said using secure VPN and wireless networks for less privileged users mitigate some security risk. According to

PP3, the most important aspect of security for the network is preventing unauthorized access, viruses, worms, malware, spyware, and identity theft. PP3 also said that fully functional and updated firewalls and IDS are an important part of the security. PP3 said that we could configure security related virtual network functions with control plane in SDN which is different from implementing security in traditional networks. According to PP2, the configuration will be easy and simpler in SDN compared to traditional networks. PP2 suggested that using the encrypted channel between controller and devices would reduce the risk of unauthorized access attacks. PP3 mentioned that based on reviewed research papers on SDN, using AMQ (Automated Malware Quarantine) can detect and isolate any network device which tries to act strangely in a network.

PP2 and PP3 believe that SSL or TLS or DTLS (TLS over UDP) is a great way to secure communication between controllers and end devices.

All PPs believe that SDN should be implemented with measures set to prevent attacks immediately. PP2 suggested that network engineers should be informed about the importance of TLS implementation and importance of security in SDN through seminars.

Pilot interviews conclusions

SDN is the future of networks. The programmable and separated control plane is more advantageous compared to the coupled data and control plane in the traditional networks. None of the choices of implementing SDN has changed because of security threats at the lower level of the SDN. PPs suggested AMQ and TLS for preventing DoS and unauthorized access attacks.

The first pilot interview with PP1 was extremely beneficial. It was a Skype group video call among Thesis advisor – Dr. Larry Hash, PP1 and the researcher. Most of the

interview questions were finalized after this pilot interview. The researcher was highly benefited with the feedback from PP1 and Dr. Hash.

PP2 provided detailed information on layered security for the company which provided researcher deep insight on the topic. PP2 and PP3 suggested various options to prevent DoS and unauthorized access attack in the SDN. These suggestions confirmed that current security measures present for unauthorized access attack in traditional networks could be implemented for the SDN.

All PPs appreciated the centralized and programmable controller as SDN reduce CAPEX, OPEX and, brings faster and easy service and network upgradation.

Chapter 8: Interview summary

Participants background

Table 1 lists number of the participant, years of experiences and roles performed in their career.

Participant No.	Years of Experience	Roles
1	6	Server Support Engineer, Technical specialist (Microsoft Azure), Technical Analyst (Microsoft Azure), Enterprise cloud solution consultant
2	18	Wireless Engineer II, Chief Security officer, Director of Research and Development in Cyber operation, Senior computer Engineer, Professor, Executive Vice President of Engineering
3	12	Network Software Engineer
4	21	Technical Solution Architect, Network Security Architect
5	31	Electrical and computer Engineer
6	15	System Analyst, System admin, Support Engineer
7	30	Software Engineer, Cloud consultant
8	30	SONAR technician, network Analyst, Senior Information Technologist, Network Consultant, Network manager, Network Operations manager
9	30	Network Engineer, Mgr. data engineering, mgr. system engineering, senior consultant, Manager of Information Technology
10	5	Network Engineer

Table 1: Participants details

All participants are experienced engineers in the field of networking or cloud computing or system administration or software engineering or IT services. Participant 1 works in a company that helps customers and businesses to adopt cloud and migrates their running application or existing infrastructure on to Azure or AWS based on customers feasibility. Participant 2 has worked for state and federal government in some network related capacity since 2001. Associating with networking experience, participant 3 has developed Samsung switches, Samsung routers, Cisco's first virtual switch Nexus 1000v, Intel SDN switch FM 6000, Open SSL and layer 2- layer 3 protocols such as STP, RSTP, MSTP. Participant 4 has been working in one of the largest networking companies and is responsible for network security for all the products that the company sell, including SDN implementation on the network side. Participant 5 and 7 have been working for the Air Force in cloud computing technologies. Participant 6 administers 50 to 100 servers and 50 workstations for the New York Power Authority. participants 8 and 9 have 30 years of experience. Both the participants have worked in different networking technologies and different sectors such as finance, healthcare, IT services, etc. Participant 10 works for one of the leading provider of customized, integrated and managed communications solutions and, works on SD-WAN devices.

SDN Definition

All participants focused on the capability of separating control plane i.e. software and data plane i.e. hardware in SDN as its definition. Also, many participants mentioned its beneficial functionalities. table 2 shows relevant words and phrases used to define SDN by participants.

Participant No	Words used to define SDN
1	software, no vendor specific hardware
2	software on specialized hardware
3	Vendor interoperability, separation of control plane
4	software-based controller, black box hardware, performing networking functions, configuring statistics
5	control and observability with different networking components, very quickly and more flexibility to create and configure and can tear down whole networks, Openstack Neutron
6	No proprietary devices, instead of a piece of equipment with the ability to perform different networking function
7	network virtualization capabilities, isolation of collision domain, isolation of software and physical hardware
8	software console to relocate network resources, manipulate network through software
9	separation of data and control plane
10	programmatically designed network, control plane and data plane are separated, centralized control console

Table 2: SDN definition

According to participant 1, SDN is something that you are doing to all your networking activities, such as routing, segmentation of networks, switching using software not with vendor specific appliance. participant 2 stated definition and mentioned as an example that virtual switches work on top of regular switches and can be upgraded to support any specific protocol or process as per requirement. Interestingly, participant 4 said that SDN could be discussed in two different ways where the first case can be found in Google, Facebook or in some service providers and the second case can be found in Cisco. In the first case, the controller does all network control functionality as well as reliable connections. In the second case, the controller does all network control functionality but does not control lower layer-connection settings. Participants 5 and 7 said that their experience regarding SDN has been with OpenStack Neutron project. Participant 3 and 9 stated definitions and mentioned that SDN is an outcome of R&D department where they are trying to develop a protocol for vendor-interoperability.

Is SDN beneficial?

All participants believe that SDN is beneficial. Table 3 lists all relevant words and phrases when participants explained why SDN is beneficial. Many participants mentioned that SDN is cost-effective, supports rapid changes and provides flexibility. Participant 4 said, “We committed to it as the primary way going forward.” Participant 1 said, “Here, I am working for what I want, not on what I got.” Some participants compared SDN in different scenarios. Participant 3 said that SDN is more beneficial to service providers compared to customers as service providers can provide new services quickly. However, participant 8 said that SDN is more beneficial to bigger companies

compared to smaller companies due to cost. Participant 10 mentioned that SDN is far better than SNMP to manage networks.

Participant No	SDN Beneficial?	
1	Yes	cost effective, high reliability, rapid changes, independent of hardware
2	Yes	rapid changes, independent of hardware
3	Yes	independent of hardware
4	Yes	automation, Smart GUI
5	Yes	flexibility, cost effective, rapid changes, automation
6	Yes	cost effective, fewer engineers
7	Yes	useful in Cloud, independent of hardware
8	Yes	beneficial to bigger companies
9	Yes	security, network visibility
10	Yes	central controlling

Table 3: SDN beneficial?

Reasons not to choose SDN

The question "what are the factors that would not lead to choosing SDN over the traditional network?" was asked to participants 3, 4, 5, 6, 7, 8, 9 and 10. Participant 6, participant 8 and participant 9 mentioned the security of the SDN could be one factor not to choose SDN over traditional networks. Table 4 lists reasons not to choose SDN from participants' perspective.

Participant No	Factors not to choose SDN
3	cost, programming skill, Infrastructure which supports SDN
4	heavy programming skills, expecting automation with smart GUI
5	failure to adopt SDN Universally- network capabilities relied on existing vendors
6	security and redundancy
7	Infrastructure which supports SDN
8	Security, difficult to approve and pass decision through the board in large govt. sectors
9	Security, Complexity, cost
10	Redundancy

Table 4: Factors not to choose SDN

Participant 6 and 10 mentioned redundancy as one of the factors to not choose SDN, which was not mentioned in the literature review. Participant 10 learned on the job that SD-WAN product Velocloud device is the only point of control when a WAN network is taken as input to handle customer facing LAN network, which collapses network in case of failure. According to participant 3 and participant 4, networking staff stick with traditional networks as they don't have heavy programming skills which are required in SDN networks. In addition, participant 4 said, "Maybe 95% of the existing enterprises are kind of built around this model, where they're looking for SDN to be primarily a very smart GUI for them. So, they don't really want to get into the programming."

Security breach incidents

The question “Can you please share any security breach that happened in your network?” was asked to all participants except participant 3 and 9. Participant 5 and participant 7 could not share any information as it’s classified information for their organization. Participant 6, participant 8 and participant 10 have not experienced any security breaches in their networks. Participant 1, participant 2 and participant 4 talked about unauthorized access attacks.

Participant 1 said that developer team on the customer side needed SSH or RDP access on a system in their environment so that they could run scripts. Developers raised a request for SSH access, but they never informed to close the ports. As a solution, they created a script, which checked ports of the VM exposing. It compared the list of open ports with the list of ports provided with the script. The script will implement deny access rule on the ports.

Participant 2 said that they had a developer a while back who had access to their development network and the developer also had corporate access where he could do his emails or normal corporate work. He accidently sat down at a non-corporate machine instead of development machine which was on the same desk and he sent out information which was company confidential. It wasn’t classified but their competitor could have seen that information and potentially used to get ahead of them. It wasn’t the biggest security breach, but he was confused on which workstation had which classification. It was scary because if he had sat down at the secret or top-secret system then it would have been worst. As a solution, they swapped out keyboards, monitors and mice so that it was visually separate when users sit down at the different computers, so computers did not

look like the same computer. Even though all computers were classified, they had new banners to the screen, so the user can see whether it's a developer computer or un-classified. On the networking side, they tagged VLANs in a way so that information couldn't be emailed out of one specific VLAN and only out of the other. Companies' watch list and blacklist everything else would get applied to it.

Participant 4's company works on all the large breaches which are mostly focused on the customer side. Attackers use some phishing techniques or malware frauds on an end device to move across networks and try to perform data exfiltration. Almost all breaches which participant 4's company deals with are organized attacks, performed by some military intelligence agency of the different companies. One of the ways to mitigate these breaches is using modern malware agents such as Cisco AMP for end-points. Another way is to use anomaly analysis type software that works by analyzing the net flow, the connection information and web proxy logs on an anomaly basis. This is excellent for data hoarding and for data ex filtration.

Solution used to prevent DOS and unauthorized access

Participant 1 mentioned that whenever Microsoft DDOS finds a vulnerability in their network it updates Network Watcher. Network Watcher has the facility to send emails to mention email Ids. DDOS will not allow traffic unless and until it gets approved. Participant 2 said that there are many manufacturers out there such as Vivio and Nap attack, both companies have created software defined V switch technology that runs on custom hardware. V switch designates different ports as being part of the VLA., It physically separates them at the circuit level using FPGA so that there is no chance that traffic can jump and be part of some other domain. In addition, participant 2 said that

people are using spoofed playback and similar techniques to create DoS, but a lot of WAN level protocols truncate and encapsulate groups of IP packets and do the statistical processing to find a spoofed IP outside of the range of the all known IPs within that trunk. Participant 3 said that unauthorized access attacks could be prevented with SSL implementation. Participant 4 said that denial of service can be detected with next generation IPS or anomaly-based analysis engines such as Cisco Stealthwatch and remove attacking end-points. In response to prevent DoS within 3 seconds, participant 4 said that it's just a matter of how quickly you have those tools integrated into a response that you can trace that back and get that removed from the network itself. Furthermore, participant 4 said that unauthorized access could be prevented by using best practices such as SSH, CACKEY and various types of encryption. Participant 10 said that the data plane layer in any SDN is vulnerable to a variety of attacks and using TLS on the initial level to SNMPv3 to extreme enforcement of security can save the network from attacks. Participant 10 also mentioned that SDNs could easily and smartly reroute the inbound (IB) traffic along with aggregating flow timeouts and rules in any network to minimize the effect of DoS attacks on the SDN. Table 5 lists all solutions provided by participants.

Participants 5 and 7 did not mention any solutions as this information is confidential for their organization. Participants 6, 8 and 9 mentioned solutions to prevent DoS and unauthorized access attacks in traditional networks as they were not aware of all the aspects of SDN.

On the next page, table 5 depicts suggestion from participants to mitigate DoS and unauthorized access attacks.

Participant No	Suggested measures to prevent DoS and unauthorized access attack
1	Microsoft provides DDOS protection + Azure network watcher.
2	V Switch Technology by Vivio and Nap Attack; statistical processing on WAN level protocols to find spoofed IP.
3	Use of SSL for authentication and built-in mechanism of servers to prevent DoS.
4	Next Generation IPS, Cisco stealthwatch, Encryption, Port security function
6	Dedicated Servers and personnel to mine the system.
8	A layered approach to prevent DoS, VPN for user access.
9	Firewalls, segregation of management and data traffic.
10	TLS on the initial level to SNMPv3 to extreme enforcement of security

Table 5: Solutions on DoS and unauthorized access attacks

Participant No	TLS mandatory?	
1	yes	
2	yes	need to prevent spoofing, un-authentication routes and changes being made
3	No	processing overhead
4	Not Sure	there are always add-ons
5	Not Sure	pluggable so that easy to replace
6	No	The efficiency of server decreases
7	Yes	good sign for security
8	Yes	Any kind of system that enforces encryption should be mandatory
9	Not Sure	Adding security with a lot of complexity will make people hesitant but if its easy then include
10	N/A	not a security person

Table 6: TLS mandatory

Should TLS be mandatory?

All participants said that there must be some sort of secure option implemented in the SDN. Participants 1,2,4,7 and 8 believed that TLS should be mandatory in the Openflow standard. On the previous page, table 6 shows relevant words and phrases used to reason the importance of TLS.

Best SDN architectural approach

Most of the participants believed the 3rd architectural approach for the SDN is beneficial to minimize DoS and unauthorized access attacks. Table 7 shows favored approaches to mitigate the security issues.

	controller provides security with the help of security applications	Integrating middle boxes to provide network security	Providing more control back to the network devices for security
P1			
P2		✓	
P3			✓
P4	✓	✓	✓
P5			✓
P6	✓		✓
P7		✓	
P8			✓
P9			✓
P10			✓

Table 7: Best SDN architectural approach

Opinion on SDN implementation

The question “According to one of the research papers, if DoS attack is not prevented within 3 seconds then entire network will get affected. Despite these security challenges,

do you believe one should implement SDN in their networks? Why?" was asked to all participants. All participants said that one should implement SDN with good monitoring and mitigating system as it has a lot of benefits over traditional networks. Table 8 shows relevant words and phrases used to reason about SDN implementation.

Participant No	Despite Security issues, SDN?	
1	Yes	Go with SDN with good monitoring and mitigating systems.
2	Yes	In the long run the granularity of control over the devices, take care of security
3	Yes	many options available to make SDN safe.
4	Yes	Drive for automation, DoS doesn't happen that often. Service Provider- fix the problem.
5	Depend on risks, cost and project	
6	Depend upon security importance	SDN is good, require enhancement for adoption
7	Yes with hope	Able to mitigate challenges and deploy SDN
8	Depend upon companies view	SDN is with great ideas
9	Depend on customers	If customers have a benefit then outrage the risk of some of the DoS, then go for SDN
10	Not sure	

Table 8: Opinions on SDN implementation

In summary, all participants believed that SDN is beneficial because of it's programmability, automation, vendor interoperability, flexibility and lower capex and Opex. All participants believe there should be some security options involved in SDN to prevent unauthorized access attacks. Most of the participants believed 3rd architectural

approach for the SDN is beneficial to minimize DoS and unauthorized access attacks. Most of the participants listed preventive measure and practices to prevent DoS and unauthorized access attacks.

Chapter 9: Conclusion

Interview summary conclusions

Some participants focused on SDN's beneficial functionality while defining SDN. Nowadays, "Software-defined networking (SDN) is an umbrella term encompassing several kinds of network technology aimed at making the network as agile and flexible (Rouse, M., 2015)." Interestingly, some participants stated cost as choosing as well as not choosing factor for implementation. However, SDN should be implemented to reduce CAPEX and OPEX. participant 9 said, "It is beneficial to the bigger company compared to a smaller company." The quote deserves more attention and could be a separate research study. In this study, half of the participants were not aware of the security issues. This could be due to marketing associated with SDN. That said, most of the participants said there should be built-in security in SDN despite being from different sectors such as networks manufacturing companies, IT services for private companies, IT services for Air Force, IT services for a government company, cloud computing. The solutions presented in the study may or may not work with respect to SDN as they are not evaluated practically. Participant 4 said that the reality is that DDOS and DOS can happen in the traditional networks, but he doesn't see many of them occurring inside of the enterprise networks themselves. And some of the participants shared their experience with security breach which included unauthorized access attacks. The reason could be that attacker is more benefited with unauthorized access compared to DoS. However, both attacks are equally significant in case of centralized SDN controller. Most of the participants said that 3rd SDN architectural approach is beneficial to prevent DoS and unauthorized access attacks. However, the contracted research slick controller under US

navy proposes decoupled control plane for middle boxes on which applications split into multiple executables and run across middleboxes concurrently to enforce policies efficiently (Anwer, B., et al., 2013). Therefore, 2nd as well as 3rd architectural approaches are beneficial to improve security.

Overall conclusion

From the study, we can conclude that there is uncertainty whether one should implement SDN when security is considered. Half of the participants did not say firmly that it should be implemented despite security issues. I agree that SDN is a future network as it provides many exciting features. However, it should not be implemented at present as there are important security challenges that need to be solved. There is definitely a need for security standards. We may want to go one step back and implement the de-centralized approach in SDN to secure devices at customer side. If the SDN community automates security in the SDN there will definitely be an increased rate of SDN deployment.

Chapter 10: Recommendations

Recommendations to SDN community

We request that the SDN community take into consideration an automated mandatory security mechanism for authentication in the OpenFlow standard. Most of the participants see SDN as automating tool to provide network functions and services. If SDN provides automation for security, then security issues such as configuration issues, and data modification will mitigate. This will ease network engineers in configuring complex security features like TLS. From literature review, we understood that there are no security standards. For example, listener mode in SDN switches, OpenFlow controller and OpenFlow SDN switches do not support TLS. If SDN place security standards for SDN controllers and switches, then it will minimize unauthorized access attacks. Most of the participants believe, the 3rd architectural approach (giving some control back to end devices) in SDN implementation to mitigate security issues. Therefore, we request SDN community to implement decentralized approach in which SDN switches will mitigate security issues such as unauthorized access attacks, system vulnerability attacks, etc.

Suggestions for further study

The future researcher can evaluate solutions presented in table 6 by an experimental setup. The solutions presented in the study are not verified due to limitations of the methodology and limited time. Three architectural approaches mentioned in the study can mitigate security issues. However, the best SDN architectural approaches can be evaluated with the simulations and/or experimental setup to mitigate DoS and unauthorized access attacks. This will provide future researcher or SDN community an opportunity to tackle security issues in a faster way as latency and

performance could affect security defense in various SDN architectures. Qualitative or experimental research can be implemented to study all factors such as security, performance, scalability and inter-operability which limit SDN implementation. One of the participants said it is beneficial to larger companies compared to smaller companies. This could be an interesting study to determine effects of SDN implementation.

Bibliography

Anwer, B., Benson, T., Feamster, N., Levin, D., & Rexford, J. (2013, August). A slick control plane for network middleboxes. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 147-148). ACM.

Benton, K., Camp, L. J., & Small, C. (2013, August). OpenFlow vulnerability assessment. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 151-152). ACM.

Doherty, J. (2016). SDN and NFV simplified: a visual guide to understanding software defined networks and network function virtualization. Addison-Wesley Professional.

Edwards, R., & Holland, J. (2013). What is qualitative interviewing? London: Bloomsbury.

Farhady, H., Lee, H., & Nakao, A. (2015). Software-defined networking: A survey. Computer Networks, 81, 79-95.

Fundation, O. N. (2012). Software-defined networking: The new norm for networks. ONF White Paper, 2, 2-6. Retrieved from https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf

Hardy, Q. (2013, January 15). Juniper Jumps Into Software Networks. Retrieved from https://bits.blogs.nytimes.com/2013/01/15/juniper-jumps-into-software-networks/

Hu, F., Hao, Q., & Bao, K. (2014). A survey on software-defined network and openflow: From concept to implementation. IEEE Communications Surveys & Tutorials, 16(4), 2181-2206.

Kuada, J. (2012). Research methodology: A project guide for university students. Samfundslitteratur.

Nayak, A. K., Reimers, A., Feamster, N., & Clark, R. (2009, August). Resonance: dynamic access control for enterprise networks. In Proceedings of the 1st ACM workshop on Research on enterprise networking (pp. 11-18). ACM.

Nunes, B. A. A., Mendonca, M., Nguyen, X. N., Obraczka, K., & Turletti, T. (2014). A survey of software-defined networking: Past, present, and future of programmable networks. IEEE Communications Surveys & Tutorials, 16(3), 1617-1634.

Rouse, M. (2015, August 17). What is software-defined networking (SDN)? Retrieved from https://searchsdn.techtarget.com/definition/software-defined-networking-SDN

Scott-Hayward, Sandra, Gemma O'Callaghan, and Sakir Sezer. "SDN security: A survey." Future Networks and Services (SDN4FNS), 2013 IEEE SDN For. IEEE, 2013.

Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., & Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. IEEE Communications Magazine, 51(7), 36-43.

Shin, S., & Gu, G. (2012, October). CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as

a service in clouds?). In Network Protocols (ICNP), 2012 20th IEEE International Conference on (pp. 1-6). IEEE.

Shin, S., & Gu, G. (2013, August). Attacking software-defined networks: A first feasibility study. In Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking (pp. 165-166). ACM.

Yan, Q., Yu, F. R., Gong, Q., & Li, J. (2016). Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. IEEE Communications Surveys & Tutorials, 18(1), 602-622.

APPENDICES

Appendix A: Exemption approval letter

SUNY Polytechnic Institute
Institutional Review Board

Ms. Pradnya Patil
Dept. of Computer and Network Security
SUNY Polytechnic Institute
100 Seymour Rd.
Utica, NY 13502

December 21, 2017

RE: "How security challenges caused due to data and control layer separation in the SDN..." (IRB # 2017-12-19-(1))

Dear Ms. Patil:

The Institutional Review Board (IRB) of SUNY Polytechnic Institute is pleased to inform you that it reviewed the research project, entitled above, in accordance with federal regulations at *45 CFR 46* on 12/21/2017. Your project was reviewed by myself, as IRB Chair, and it was determined that your project is exempt from all requirements of *45 CFR 46* under paragraph *46.101(b)(2).*

You are required to notify this IRB prior to any changes that would make the status of this project non-exempt. You are also required to notify this IRB if unexpected or serious adverse events result from this research.

If you have any questions about the contents of this notification letter, please feel free to contact the Office of the IRB at 315-792-7236 or by email at manninmb@sunyit.edu.

The Institutional Review Board of SUNY Institute of Technology subscribes to and functions within the requirements of **Title 45 Code of Federal Regulations Part 46 *"Protection of Human Subjects."***

Sincerely,

Michael B. Manning, Ph.D.
chair, Institutional Review Board
SUNY Polytechnic Institute

100 Seymour Road
Utica, NY, 13502
315-792-7343

Appendix B: Interview question draft

Hi, I'm Pradnya. I am a telecom graduate student at SUNYPOLY. And currently working on the thesis in which "how security threats at a lower level of the SDN affects the implementation" will be analyzed. And, I want to sincerely thank you for agreeing to participate in this process/project. I would like to record this interview, so I will not miss out any information. Can you please let me know, if you agree to allow me to record this interview?

I would also like to mention that you are free to decline to answer any question at any time. Also, you are free to withdraw from this process/project/interview at any time.

Date: Time:

Place: Participant:

1. Can you please tell me about yourself and give little overview about your professional/academic experience?
2. Can you please explain in your words, what is Software Defined Networks?
3. Nowadays, SDN has gained a lot of popularity. Do you believe SDN is beneficial?
4. How do you anticipate SDN in your network?
5. What are the main factors that would not lead to choosing SDN over the traditional network?
6. What are the important aspects of security in your network?
7. Can you please share your experience regarding security any breach that happened on your network?

8. What were the preventive measures that you used to prevent this kind of security breach?
9. What are the preventive measures that have been taken to prevent security breaches in your company?
10. How do you think preventive measures for the traditional networks will change for the software defined networks?
11. Can you please suggest any provisions or best practices prevent DoS or unauthorized access attacks (control-switch communication flood and switch flow table flooding) in SDN network?
12. Did you use TLS in your network?
13. TLS is optional in the widely used OpenFlow communication protocol in SDN. Do you believe it should be mandatory?
14. There are many approaches when it comes to SDN architecture. One approach is – controllers are responsible for global policy enforcement with the help of security applications. The second approach is integrating middle boxes to interact with SDN controller to provide network security and another approach is giving some control back to network devices for gathering additional information to provide security.

    Can you please let me know which approach is the most beneficial to prevent DoS and unauthorized access attack?
15. According to one of the research papers, if DoS attack is not prevented within 3 seconds then entire network will get affected. Despite these security challenges, do you believe one should implement SDN in their networks? Why?

Appendix C: Completion report of Students in Research module

COLLABORATIVE INSTITUTIONAL TRAINING INITIATIVE (CITI PROGRAM)

COMPLETION REPORT - PART 1 OF 2
COURSEWORK REQUIREMENTS*

* NOTE: Scores on this Requirements Report reflect quiz completions at the time all requirements for the course were met. See list below for details. See separate Transcript Report for more recent quiz scores, including those on optional (supplemental) course elements.

- **Name:** Pradnya Patil (ID: 6833304)
- **Institution Affiliation:** SUNY - College of tech. at Utica/Rome (ID: 2477)
- **Institution Email:** patilps@sunyit.edu
- **Institution Unit:** Telecommunication
- **Phone:** 3157239158

- **Curriculum Group:** Students conducting no more than minimal risk research
- **Course Learner Group:** Students - Class projects
- **Stage:** Stage 1 - Basic Course
- **Description:** This course is appropriate for students doing class projects that qualify as "No More Than Minimal Risk" human subjects research.

- **Record ID:** 25585962
- **Completion Date:** 20-Dec-2017
- **Expiration Date:** 19-Dec-2020
- **Minimum Passing:** 80
- **Reported Score*:** 80

REQUIRED AND ELECTIVE MODULES ONLY	DATE COMPLETED	SCORE
Students in Research (ID: 1321)	20-Dec-2017	4/5 (80%)

For this Report to be valid, the learner identified above must have had a valid affiliation with the CITI Program subscribing institution identified above or have been a paid Independent Learner.

Verify at: www.citiprogram.org/verify/?ke08718b4-493b-4a21-9e0f-b0c832470bf1-25585962

Collaborative Institutional Training Initiative (CITI Program)
Email: support@citiprogram.org
Phone: 888-529-5929
Web: https://www.citiprogram.org