Design and Implementation of a New Security Plane for Hybrid Distributed SDNs

Karim Zkik, Said EL Hajji, and Ghizlane Orhanou
Laboratory of Mathematics, Computing and Applications, Faculty of Sciences, Mohammed V University in Rabat, Rabat 10060, Morocco
Email: karim.zkik@gmail.com; elhajji@fsr.ac.ma; orhanou@fsr.ac.ma

Abstract —Software defined network 'SDN' architectures can be considered as a big revolution in the field of computer networks, because they offer a lot of advantages and allow having a visibility and a total control on the equipment, services and applications deployed in the network. On the other hand, the implementation of this type of architecture is not obvious and requires great expertise and good handling and management of network equipment. So, SDN architectures have evolved towards distributed and hybrid architectures. The security of these architectures is considered to be the biggest problem in front of their deployments. In this paper we propose the integration of a new flexible security layer that allows managing security in SDN networks in order to detect and prevent against intrusion attempts and zero day attacks without impacting the performance of controllers and SDNs nodes. In this article we discuss also the challenges of the SDN; we detail the functioning of our framework and provide an implementation of our new SDN security layer.

Index Terms—Hybrid distributed SDN, Open flow, Network security, SDN security, firewalls, DDoS, Zero days attacks

I. Introduction

The expansion of information technology has given rise to several challenges such as the security of computer networks, lower bandwidth cost, and the deployment of new technologies and the management of network performance. Unfortunately, the use of standard networks architecture no longer follows this technological development. So, it has become essential to develop a new network architecture that can meet the needs of users.

Software Defined Networks (SDN) is a new software centric approach to networking that reduces capital and operational cost through programmatic control of network infrastructure, facilitating customization, optimization, and innovation [1], [2]. This new network model offers several advantages in terms of policy driven, automation and agility which make it easy to support the adoption of all kinds of technologies, services and applications.

To deploy the SDN architecture it is necessary to replace all the current network architecture by SDN nodes which are very difficult. So to remedy these problem; researches [3], [4] proposed the use of hybrid distributed SDN architecture. In this architecture, the SDN nodes coexist with the standard network devices, which will facilitate the complete migration to the SDN architecture.

Despite the apparent benefits of using SDN architectures, security remains one of the most disconcerting challenges and issues of its deployment. To overcome these problems several studies proposed solutions tailored to SDN environments [4]-[7]. Unfortunately, the uses of these solutions offer somewhat limited network usability, high configuration complexity and performance consumption and do not prevent from unknown infections and zero day attacks.

In this paper we propose architecture for securing logical distributed hybrid SDN architectures. To do so, we implement a modular security plane composed from a firewall module, a network intrusion prevention server and an anomaly detection module. We propose also the use of a security as a service Cloud platform to secure the management plane and we present a new communication protocols between controller to secure sensitive data and communication at the level of the control plane. Using this security layer we intend to secure SDN environment, ensure High availability, ensure threat mitigation and defense prevent unknown exploitation and zero day attacks.

The rest of paper is structured as follows. In section 2 we discuss some preliminaries and related works. In section 3 we present our proposed model, and we detail the conception of each part. In section 4 we present an implementation and experimental results of our work. In section 5 we present a security analysis and an extended discussion on the results. In section 6 we conclude the paper and discuss some of our future research directions for security in SDN.

II. Security Issues in SDN: Challenge and Related Works

SDN's centralized architecture and its multi-layered design make it vulnerable to multiple types of attacks and subject to several security vulnerabilities. So, In SDN architecture, there are several security issues that affect its operation:

- First, the most critical problem is that controllers are considered as points of failure, which means that if an

Manuscript received March 20, 2018; revised December 22, 2018.
doi:10.12720/jcm.14.1.26-32

attacker manages to control a controller, he can control either the entire network or a significant part of the network.

- Secondly, when using SDN architecture, we remove the intelligent and decisional part of the SDN nodes which makes them vulnerable.
- When using hybrid architecture, we also inherit traditional network security problems which multiply vulnerabilities and makes security operations even more complex.
- When using a distributed architecture, the different controllers constantly communicate with each other. Thus an attacker can listen to these communications and sniff sensitive data.
- Fig. 1 shows an overview of the different security issues in a Hybrid distributed SDN architecture.

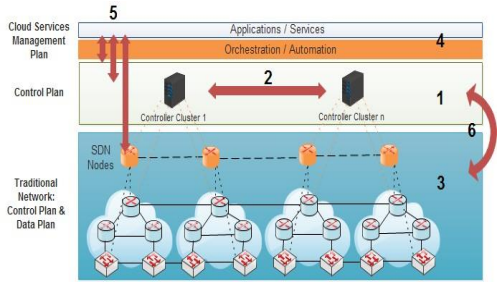

Fig. 1. Threats vectors in hybrid distributed SDN

These vulnerabilities can be exploited by several types of attacks. The following are the most destructive attacks on the SDN environment:

- **Scanning:** This type of attack permit to an attacker knows information about the whole network.
- **Spoofing:** This kind of attacks refers to identity usurpation by falsifying data and gaining an illegitimate advantage.
- **Hijacking:** This type of attacks permits to take control of a communication element in data and control plane.
- **DDoS:** This type of attack makes SDN resource unavailable by using a flood attack. This attack is very dangerous and very simple to execute.

To overcome this security issue several research projects have proposed solutions and secure frameworks. Table I lists the research work that aims to secure SDN architectures.

Note that "C" is Confidentiality, "I" is Integrity and "A" and availability.

Despite the different proposals and security solutions offered by these different research projects most of this research are focused on standard SDN architectures and does not address security solutions adapted to hybrid and distributed SDN architectures. These framework offers somehow a complex security solution which decrease performance and increase latency on the network and existing research focuses on well knowing security threats instead of unknown and zero-day attacks.

In this work we will focus on these limitations and we propose a new secure architecture for SDN which permit to secure all layers. To do so, we will propose a new modular security layer for distributed hybrid SDN architectures. In other words, we will propose a modular security plane model to provide:

- A secure modular platform against security issues in SDN
- A secure modular platform against unknown and zero day attacks.
- An architecture to provide security without impacting performance
- A secure design to ensure High availability

TABLE I: RELATED WORKS

References	Contributions	Data Plane			Control Plane			Channel		
		C	I	A	C	I	A	C	I	A
Xiao feng and al. 2017 [8]	GFT: This mechanism permits also to provide security appliances with information about paths of all the flows in SDN and have a global view on the network.				X	X		X	X	
Saksit jantila and al. 2016 [9]	Propose a new design of SDN architecture to prevent DDoS attacks. In addition, authors put a mechanism to secure data plane based on a client's access behavior.						X			X
Liyanage and al. 2015 [10]	HIP: A protocol for securing communications between SDNs nodes and controller. This model doesn't rely on IP to authenticate packets' source, but uses a secure communication model based on public key usage.							X	X	
Lara and al. 2014 [11]	OpenSEC: A security model that allows making deep inspection, intrusion detection and malware detection.	X	X	X						
Shin and al. 2013 [12]	AVANT-GUARD: A secure architecture which reduces interactions between the control and the data planes and detects changing flow on the data plane. The purpose of this framework is to protect communication channels from any infiltration and to prevent DoS attacks.							X	X	X

III. A Centralized Secure Design for Hybrid Distributed SDN Architecture

A. Proposed Centralized Design Scheme

The security of SDN architecture is one of the main concerns of expert and researchers [13-17]. Several works offer security architectures adapted to SDN environments, but there are still several points that are not yet fully covered.

- First of all, most existing architectures use standard security equipment. This is insufficient because there are several attacks that can bypass these devices.
- Existing security solutions use complex architectures and require multiple configuration operations that can impact network performance.
- Most existing security frameworks focus on the security of standard SDN architectures, and do not take into account the additional security challenges of distributed and hybrid SDN architectures.
- Existing security proposals offer solutions against standard attacks and offer few measures against zero day attacks.
- The security management plane is very little cited because the services and applications in this layer are often housed in remote cloud servers. Thus, the security of this layer comes back to secure the Cloud infrastructures and secure the deployment of these services to end users.

In this work we propose a new security model that proposes a solution to these issues. Thus, the main goal of our model is to secure all layer under a distributed and hybrid SDN architecture and to detect and prevent attacks whether it is known attacks or zero day attacks.

We propose in our architecture the addition layers of security. The first layer (Security Plan) is of two responsible for securing data and control plan and communication channels.

The security plan that we have integrated consists essentially of 3 modules:

Anomaly detection Module: In this module we implement a honey controller, a DDoS detector and an analysis behavior module to detect and anomaly or security incidents.

NIPS Server Module: In this module we propose the use of a network intrusion detection server adapted to an SDN environment to inspect the transiting packets in the network.

State full Firewall Module: In this module we propose the use of a state full firewall adapted to an SDN environment to filter the transiting packets in the network.

The second layer (SECaaS plan) is a layer that uses cloud resources to provide security services. This layer is responsible for securing the management plan and the deployment of services and applications from distant cloud servers to end users.

It is also proposed to use an inter-controller communication process at the control plane level to secure communications between the controllers. In what follows we will detail each part of our security architecture.

B. A Modular Security Plane for Hybrid Distributed SDN Architectures

The purpose of our work is to secure SDN topologies and preserve network performance. The standard use and implementation of security equipment's in SDN increases the complexity of the network and significantly impacts the performance. To remedy this problem, we propose the implementation of a new layer dedicated to the security of SDN architectures. So, we will provide a centralized layer that manages the security of flows and SDN nodes.

In this layer we have integrated 3 security modules:

- Anomaly detection Module
- NIPS Server Module
- State full Firewall Module

We note that during a real deployment we can add as much modules as we want according to the need for security.

Anomaly detection Module

An anomaly occurs in most cases following a security incident. Most anomalies occur because of zero day attacks or due to a DDoS attack. In what follows we will present the different components of this module.

Honey controller and behavior analysis detector:

Most attackers aim to infect SDN architectures. To do this they use sophisticated attacks and persistent malware to gain control of the network. Using an IPS can detect many of these infections by inspecting package signatures. Unfortunately there are a lot of malware that is not yet detectable by these security devices.

To remedy this problem, we propose the implementation of a honey controller and a behavior analysis detector. The purpose of using this module is to be able to differentiate between normal and abnormal flow and to limit the impact of security incidents.

The procedure for detecting abnormal flows and the mitigation of infections through this module is as follows:

1) Firstly we will save the connection information of all the SDNs nodes.
2) These records will allow us to define a basic pattern of normal behavior.
3) We will make then a periodic analysis on several samples of data from the different layers.
4) An alert will be lunched if any significant deviation from this pre-established basic model was detected.
5) The alerts number defines the probability of an anomaly on the network
6) Once an incident alert is generated, the stream is immediately redirected to the Honey Controller.
7) A security administrator observes the infected packets

and determines the nature and provenance of the security threat.

8) The administrator should take a correction action to mitigate the security incident
9) A report is generated and submitted to the management layer for further analysis.

This module permits to prevent against any type of security incident even if it's an unknown attacks but it remains insufficient to secure SDN architectures from all threats and attacks. Thus we will propose some additional measure and module to secure SDN networks.

DoS and DDoS detector:

In SDN environment DDoS attack can be elaborated in several ways and reach different layers. To limit the impact of this attack several researches have proposed solutions adapted to SDN networks. Unfortunately, these solutions are complex and require the implementation of several limiters of packets at all SDN layers which impacts the performance.

In our model we will use a single limiter that can block all DDoS attacks without impacting performance and with a high reaction time. We will place this process at the level of the anomaly detection server at the security plane layer. This choice is due to the fact that DoS and DDoS attacks are generally an increase in packet throughput in our information system which can be clearly considered as an anomaly.

The process of detecting and mitigating DDoS attacks is as follows:

- Firstly we will set up the normal threshold for flow rate
- Secondly we will set up the normal threshold for a DDoS attack probability
- We will make a periodic analysis on several samples of data from the different layers.
- An alert will be generated as soon as the flow rate of the packets analyzed exceeds the normal threshold
- The alerts number defines the probability of a DDoS attack
- If the probability exceeds the threshold, the connection will be dropped
- A security report will be generated and redirected to the management plane for further analysis

Stateful firewall and NIPS Module

In an SDN environment it is very important to use firewalls to filter and inspect incoming and outgoing packets from our information system.

Concerning packet filtering, most SDN architecture uses stateless firewall. The choice of this type of firewall is due to the fact that it does not impact the performance. But several attacks can easily bypass this kind of equipment. Using a statefull firewall will increase the level of security but it will greatly affect performance and increase latency.

As shown in Fig. 2, we have developed a new design of a statefull firewall adapted for distributed and hybrid SDN environment. Connections that we will filter are coming from reactive flow, proactive flow and Non SDN flows. So, the firewall must simultaneously handle packets from SDNs and Standard network devices. To do this, we use translators at the level of data plane that translate traditional packet to open flow protocol packets. The elements of our firewall are as follows:

- MessageListner which receives the packets sent from control plane and compares them with the entries in the StateTable
- StateTable which contain the connections entry
- Rules and policy handler which is responsible of defining the packet filtering rule.

Regarding the use of IPS, most SDN architecture does not use them to not impact the performance of the controllers which poses a major security problem. To remedy this problem, we propose the use of a light NIPS that detects and stops all sorts of intrusions.

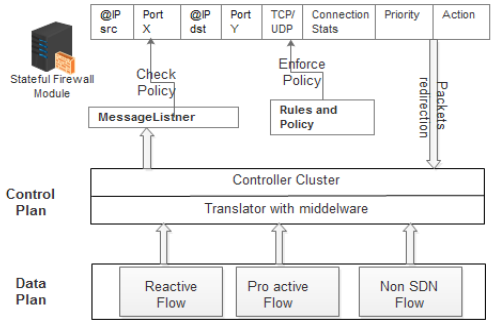

Fig. 2. Adaptive statefull firewall module for hybrid SDN

As shown in Fig. 3, we have developed a new design of a network intrusion prevention server 'NIPS' adapted to distributed and hybrid SDN environment. The elements of our NIPS are as follows:

- MessageListner which receives the packets sent from control plane
- NIPS rules table which contain the connections entry, the inspection rules, types of alerts and actions.
- NIPS Rules and policy handler which contain malwares signatures and responsible of defining inspecting rules.

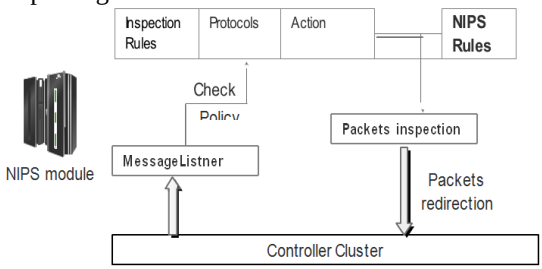

Fig. 3. Proposed network intrusion prevention module

This module makes it possible, among other things, to filter and inspect the packets transiting the network. The centralized design of this module allows it to have visibility across the entire network and it does not affect network performance.

Secure logical distributed SDN architecture

In SDN design, the main tendency is to have a single physically centralized controller. However, this architecture suffers of many security issues:

- In this architecture the controller is considered like a single point of failure. If an attacker infects the controller, he can control easily control the whole network.
- In this architecture it is easy to perform a DoS or DDoS attack at the level of the controller, which can make the whole network unavailable.
- Using a single controller pose also a serious problem on scalability and performance. With a single controller its difficult manages the whole network.

To overcome these problems several research works have proposed the use of distributed logical SDN architecture [26], [27]. In a logically distributed architecture, the controllers are physically and logically distributed. Additionally, every controller is responsible for a single area and a network and has some specifics roles. On the other hand, a logically distributed architecture goes away from the first tendency of SDN, by making several controllers have several responsibilities inside the network.

The main issue in this type of architecture is to secure communication between controllers. If an attacker sniffs these communications, he can retrieve sensitive information about the network and then perform an intrusion to the network. To overcome this issue we propose a secure communication protocol within controller clusters.

As shown in Fig. 4, we propose to implement some extension modules on each controller:

- Data collector
- Data updater
- Synchronizer
- Load balancer
- Firewall host based

The communication between the clusters will be made using secure SSL connections. To ensure the high availability and check that the others cluster are still alive we will use a heartbeat communication. Thus each controller cluster will send a heartbeat packet to other cluster periodically. If no response is sent back to the cluster an alert will be generated and redirected to the management plane.

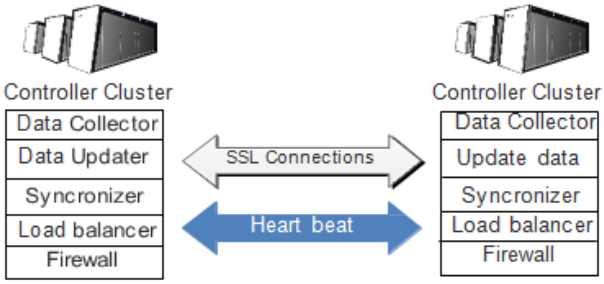

Fig. 4. Secure communication protocol on logical distributed SDN

IV. Implementation and Experimental Results

A. Experiments' Environment

In order to implement our AM-Sec model we have constructed a distributed SDN environment testbed using a PC Server HP DL380G6 with the following configuration:

- Processor Xeon quad-core E5504 2.00GHz
- 4-core4MB
- 80W
- Memory 24GB

We use virtualization to implements controllers, SDNs nodes and our security module under the management of an Open source virtualization platform XEN server [18].

We implement tree Open Daylight Controller on Linux operating system Ubuntu 16.04 64bits with 4 GB of RAM. We construct a network hierarchy model by devising our topology into 3 domains; each network domain 1, 2 and 3 is managed by a different controller.

Each area is composed from 3 open flow switches and its constructed using Mininet Emulator [19] version 2.2.1 on a different Linux operating system Ubuntu 16.04 64 bits with 2 GB of RAM.

Table II: Security Plan Implementation Results

Security Plane Modules	Flows	Flux analysis (packets/s)	Incident Detection	Incident Analysis	Action	Controller performance (%)
Firewall and NIPS modules	Normal Flow	100	-	-	Allow	9.02%
		150	-	-	Allow	9.54%
		200	-	-	Allow	10.15%
	Infected Flow	100	42	224	Drop	10.12%
		150	97	375	Drop	12.06%
		200	142	438	Drop	12.94%
Anomaly detection modules	Normal Flow	100	-	-	Allow	8.05%
		150	-	-	Allow	9.94%
		200	-	-	Allow	10.75%
	Infected Flow	100	321	-	Alert	16.49%
		150	412	-	Alert	18.73%
		200	675	-	Alert	23.81%

TABLE III: DDOS DETECTOR IMPLEMENTATION RESULTS

	ICMP			UDP			TCP		
	Connection requests (packets/s)	Detection (ms)	Mitigation (ms)	Connection requests (packets/s)	Detection (ms)	Mitigation (ms)	Connection requests (packets/s)	Detection (ms)	Mitigation (ms)
Area 1	1423	127	429	845	72	312	2047	168	689
Area 2	1548	246	517	1720	247	534	1069	175	527

To perform a forensics analysis on controllers we use GRR server on Linux operating system Ubuntu 16.04 64bits with 4 GB of RAM. We also download and install his agents on each controller.

To filter packet on our network and on each controller, we use a stateful firewall Netfilter on Linux operating system Ubuntu 16.04 64 bits with 2 GB of RAM.

B. Experiment Results

In this part we will implement the security measures and modules that we proposed and discuss in this work. For this we have launched several types of attacks on an open source and virtualized SDN environment.

We have launched several types of attacks (Dynamics Tunneling Attack, Spoofing Attack, Malware attack) at the level of control and data planes. It should also be noted that the attacker's goal is to access and infect the server within the network. So, we have configured our firewall in advance to ban any external connection to the server. Table II shows the results of our implementation.

The results of the test demonstrate in the first place that our security plane is very reactive and that it was able to detect and stop all kinds of infections even in the case of a dynamic flow tunneling attacks which change the flows rule to bypass firewalls.

DoS attack and the distributed Denial-of-Service attacks (DDoS) are considered as one of the most dangerous security problems in IT networks. In our case we will launch a simple DDoS attack lunched from our two testing area using the hacking application tool H3ping. We will also use several types of packets (ICMP, UDP and TCP) during this attack.

As shown in table 3, we have launched several DDoS attack from our two areas (Area1 and Area2) to infect and put down the controllers. The results show that our DDoS detector was able to detect and stop this type of attack. It is mentioned that some of these infected packets were redirected to the honey controller to determine the source of this attack and for further analysis.

V. CONCLUSION

In this paper we propose a security framework in Hybrid distributed Software defined networks environment. Security is one of the major concerns of experts when deploying SDN architectures. So, we implement a centralized modular security plane to detect and mitigate different threats and security incident in SDN environment. So, we develop an adaptive statefull firewall to filter malicious connections, an adaptive network intrusion detection server to inspect infected packets and an anomaly detection module to detect DDoS and zero day attacks. In addition, the firewall processes packets from SDNs nodes (reactive flow, proactive flow) and from standard network equipment (NON-SDN flows).

Regarding our future work, we project to make our security framework more secure and more performant and we would like to develop a model that could integrate more security models to increase safety in SDN environment. In our testbed, we used a simple virtual SDN architecture. So, it is expected to develop more suitable model adapted to a real deployment of SDN.

ACKNOWLEDGMENT

The author would like to thank everyone who has contributed to the progress of this research.

REFERENCES

[1] R. Masoudi and A. Ghaffari, "Software defined networks: A survey," *Journal of Network and Computer Applications*, 2016.

[2] T. D. Nadeau and K. Gray, "SDN: Software defined networks," O'REILY, 2013.

[3] Sandhya, Y. Sinha, and K Haribabu, "A survey: Hybrid SDN," *Journal of Network and Computer Applications*, 2013.

[4] O. Blial, M. B. Mamoun, and R. Benaini, "An overview on SDN architectures with multiple controllers," *Journal of Computer Networks and Communications*, p. 8, 2016.

[5] I. Ahmad, S. Namaly, M. Ylianttilaz, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Communications Surveys and Tutorials*, pp. 2317-2346, 2015.

[6] C. Yoon, T. Park, S. Lee, H. Kang, S. Shin, and Z. Zhang, "Enabling security functions with SDN: A feasibility study," *Computer Networks*, 2015.

[7] K. Zkik, T. Tachihante, G. Orhanou, and S. El Hajji, "A modular secure framework based on SDMN for mobile core cloud," in *Proc. International Conference on Mobile, Secure and Programmable Networking*, 2016, pp. 137-152.

[8] X. Qiu, K. Zhang, and Q. Ren, "Global flow table: A convincing mechanism for security operations in SDN," *Computer Networks*, vol. 120, pp. 56-70, 2017.

[9] S. Jantila and K. Chaipah, "A security analysis of a hybrid mechanism to defend DDoS attacks in SDN," *Procedia Computer Science*, vol. 86, pp. 437-440, 2016.

[10] J. Okwuibe, M. Liyanage, and M. Ylianttila, "Performance analysis of open-source linux-based HIP implementations," in *Proc. 10th IEEE International*

Conference on Industrial & Information Systems, At Peradeniya, Sri Lanka, 2015.
[11] A. Lara and B. Ramamurthy, "OpenSec: A framework for implementing security policies using OpenFlow," in *Proc. CSE Conference and Workshop Papers*, 2014, pp. 781-786.
[12] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "AVANT-GUARD: Scalable and vigilant switch flow management in software-defined networks," in *Proc. ACM SIGSAC Conference on Computer & Communications Security*, 2014, pp. 413-424.
[13] M. Liyanage, I. Ahmad, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, A. Valtierra, and C. Jimenez, "Security for future software defined mobile networks," in *Proc. 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2015.
[14] S. Zhu, J. Bi, and C. Sun, "SFA: Stateful forwarding abstraction in SDN data plane," *Proceedings of the ONS Research Track*, 2014.
[15] G. Yao, J. Bi, and L. Guo, "On the cascading failures of multicontrollers in software defined networks," in *Proc. 21st IEEE International Conference Network Protocols*, 2013.
[16] R. Braga, E. Mota, and A. Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow," in *Proc. 35th Annual IEEE Conference on Local Computer Networks*, 2010.
[17] A. J. Pinheiroa, E. B. Gondimb, and D. R. Campelo, "An efficient architecture for dynamic middlebox policy enforcement in SDN networks," *Computer Networks*, vol. 122, pp. 153–162, 2017.
[18] "XenServer 6.x Best Practices," Dell Compellent Storage Center (2013)
[19] Introduction to Mininet. [Online]. Available: https://github.com/mininet/mininet/wiki/Introduction-to-Mininet

Karim Zkik received his Engineering degree (2013) in Networks and Telecommunication Sciences at the National School of Applied Sciences of Safi, Morocco (ENSAS).
Working towards PhD degree in Computer Science at the Mohammed V University in Rabat, Faculty of Sciences, Rabat, Morocco.
His research interests are in the areas of network security, with current focus on authentication and confidentiality of data and the security of networks on the mobile cloud computing environment and software defined networks.

Said EL Hajji is Professor in the Computing Sciences Department, Faculty of Sciences, Mohammed V University in Rabat, Morocco.
His main research interests include mathematics, cryptography, networked and Information systems security.

Ghizlane Orhanou is an Associate Professor in the Computing Sciences Department, Faculty of Sciences, Mohammed V University in Rabat, Morocco.
She received his PhD degree in Computer Sciences from the Mohammed V University in Rabat, Morocco in 2011. She received in 2001, a Telecommunication Engineer Diploma from Telecommunication Engineering Institute (INPT Morocco). Her main research interests include networked and Information systems security.