An InfoSec Based Software Defined Networks (SDNs) over Insider and Outsider Attacks in Business Process

R.Raja[1] Dr.V.Dhanakoti[2]
[1]M.E Student [2]Associate Professor
[1,2]Department of Computer Science and Engineering
[1,2]Valliammai Engineering College, Chennai,

Abstract— The objective of the project work is to propose a Software Defined Networks (SDN) architecture which enables network control to become directly programmable and underlying infrastructure to be abstracted from application and network services. SDN approach is done by decoupling the system that makes decisions about authorized user data provenance. Here the internal attackers are monitored through four different layers to avoid internal leakage. Evaluation analysis, Complaints are the most important layer which is implemented to monitor authorized users abnormal behaviour. Here an algorithm for information security management system based on data provenance is considered and implemented in a prototype called Software Defined Networks, which is used for processing and decision making.

Key words: Software-defined networking, SDN, network virtualization, Open Flow

I. Introduction

A basic properties of the software defined network architecture is the physical separation of the control plane from forwarding plane. The process of data plane is processing and delivery of packets based on state of the routers and endpoints. Control plane process is to establishing the states in routers to determine how and where packets are forwarded, such as routing, traffic engineering, and firewall state. In 1980's central network control is developed. Follow of central network control, active networks in developed in 1990s to introduce programmability into the network. Open flow is the open standard developed by Stanford university clean state project. The ultimate goal of the project was to provide a base or platform to run experiments in functional networks. SDN architecture provides high end security. Traffic analysis in the network can be regularly transferred to the central controller. SDN to analyse the network and correlate the feedback from the network. The above provides a new security policies to prevent an attack can propagated across the network.

A. Purpose of the project:

Open Flow is the innovative technology allows users to easily setup new innovative routing and switching protocols in network. It is used in the following applications such as, High security application networks, virtual mobility and next generation internet protocol based mobile networks. It provides a powerful and simple way of design and associate (or merges) complex network security applications into bigger networks. Open flow gives benefits of researchers with an unheard-of unique point of control over network flow routing decisions across the data planes of all Open flow enabled network components. The necessary advantage of the developed approach is the possibility of getting statistics collection from directly on the switch, this gives the opportunity to analyse the traffic and perform actions closer to the source of malicious activity or destination simplifies development of rule sets for traffic filtering and redirecting. A network operating system provides a specialized set of functions for an efficient network security application operation. The set of activities to work with the flow rules: - Identifying the source of the rules (security application or the regular application), and given a method for signing rules;

– Detection of mismatch occurred between rules, for example, same rules portrait different way in various applications;
– Mismatch or different resolution based on the priorities of the sources of the rules and their signatures;

The important goal of the information security management system is to find a malicious or abnormal activity on the criteria of a set of input variables. Usually, gathered characteristics have a simple distribution and can be well approximated by fuzzy membership functions; decision-making and training algorithms are software level tasks and can be implemented as applications for the network operating system or as modules for the specialized framework.

B. Overview of the Project:

Software defined network (SDN) is totally different from previous network infrastructure, due to relationship between the control plane and data plane of the network device. Open flow control plane rules define flows of forwarding, changing or dropping packets that enter the open flow switch. Open flow controller is having the logic for updating, defining and adapting the flow rules. The open flow controller improve the efficient of traffic management through communicate the multiple switches consequently by direct routing or optimize tunnelling. It can be easily handle the complex logic processing flows and their prohibition and permission. Open flow controller provides an application programming interface (API) to implement the flow rules.

II. Architectural Diagram

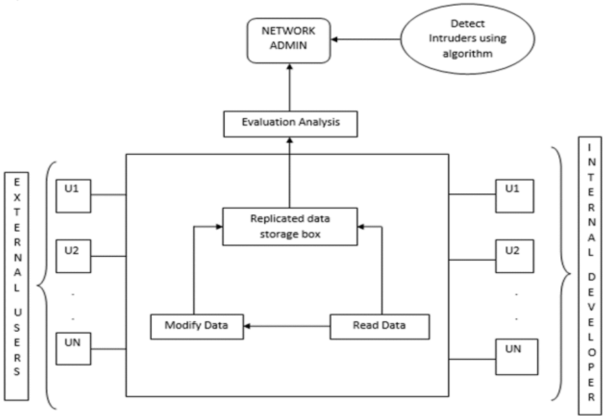


Fig. 1: System Architecture Diagram

III. System implementation

The system after careful analysis has been identified to be presented with the following modules:

- Ambiguous Reasoning
- Event creation
- Admin Authentication
- Bidding Portal
- Approval and Decision making

A. Ambiguous reasoning:

Ambiguous reason is a form of many-valued logic, a form of knowledge Representation Suitable for notions that cannot be defined precisely, but which depend upon their contexts Efficiency. In this module, data can be predicted and collected in a storage. The user data's are analysed and comparing with already stored data's for providing the security to the Open Flow Network. After providing the security to the open flow network, the intruders has been prevented by using this ambiguous reason

B. Event creation:

Event means a certain action that has been completed in an instance of time period. In this module, an event can be created in the Open network. The user of the Open Flow network only have the access to create the event. After Creation of the Event, the user may waiting for the approval for the concern authority(admin).The admin only have the rights to give the approval for all the events created by the user.

C. Admin authentication:

Authentication is the process of giving access to the members who are registered in an Open Network. The above module user can create some event and waiting for the access of the authority. In this module, the authority can give the authentication for the user based on verify some details regarding their event. After verifying the event details and then only the authority giving access to participate their event in bidding.

D. Bidding portal:

Bidding is an offer of setting price one who willing to pay for something. A price offer is called bid. In this module bidding can be started by the authority that means already some events were created that events have some products for sale. The User has the rights to ask for the bid based on the quality of the product that participated in the event. Lots of user's can quote for the same price for the same product and there must be heavy competition among the users. There also some intruders involve in the bidding. This can be provided by using Ambiguous Reason.

E. Approval and decision making:

The complete event can be monitored by the authority, they have make some good decision based on the user's response. The User can bid the same amount for the same product and the authority can have the rights to take some good decision about their bid price for the product. Finally the authority approving and finalizing the product based on their higher bid by the User.

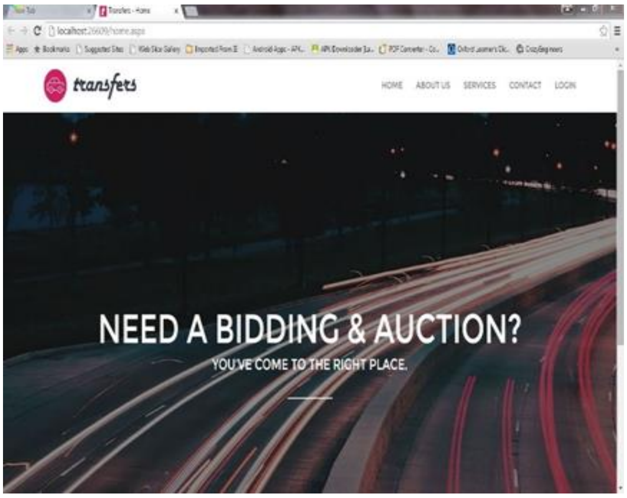
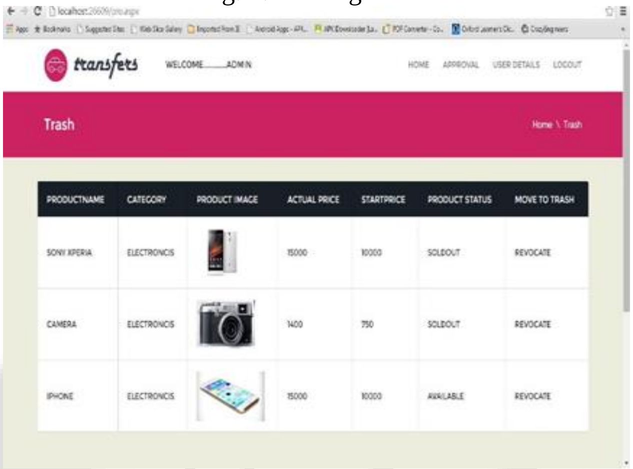


Fig. 2: Bidding Portal



PRODUCTNAME	CATEGORY	PRODUCT IMAGE	ACTUAL PRICE	STARTPRICE	PRODUCT STATUS	MOVE TO TRASH
SONY XPERIA	ELECTRONCIS		15000	10000	SOLDOUT	REVOCATE
CAMERA	ELECTRONCIS		1400	750	SOLDOUT	REVOCATE
IPHONE	ELECTRONCIS		15000	10000	AVAILABLE	REVOCATE

Fig. 3: Products

IV. Conclusion and future work

Software-defined networks is provide an opportunity for efficient and effective detection and solving of network security problems, allowing the integration of complex network security applications in large networks. For data security and privacy protection issues, the fundamental challenges are separated of sensitive data and access control. This model making access control for flexible and dynamic by applying different risk mitigation actions to different information flows, depending on the level of perceived risk. To implement a prototype of a secure network operating system based on the ambiguous security model, where an access control decision is based on the perception of the level of potential risk associated with the requested access.

References

[1] Sandra Scott-Hayward, Sriram Natarajan, Sakir Sezer , "A Survey of Security in Software Defined Networks", IEEE Communications Surveys and Tutorials,PP.623-654, 2016.

[2] Sergei Dotcenko, Andrei Vladyko, Ivan Letenko , "A Fuzzy Logic- Based Information Security Management for Software - Defined Networks" The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, Russian Federation, 2014.

[3] Dotsenko S.M., Vladyko A.G., Letenko I.D. "Intrusion detection systems based on embedded microprocessor

systems” Telekommunikatsii (Telecommunications), PP.15-18, 2013.

[4] Shin, Seugwon, et al. "FRESCO: Modular composable security services for software-defined networks." Proceedings of Network and Distributed Security Symposium. 2013.

[5] Mehdi, Syed Akbar, Junaid Khalid, and Syed Ali Khayam. "Revisiting traffic anomaly detection using software defined networking." Recent Advances in Intrusion Detection. Springer Berlin Heidelberg, 2011.

[6] Cingolani, Pablo, and Jesus Alcala-Fdez. "jFuzzyLogic: a robust and flexible Fuzzy-Logic inference system language implementation." Fuzzy Systems (FUZZ-IEEE), 2012 IEEE International Conference on. IEEE, 2012.