Building a Transparent Intrusion Detection and Prevention System on SDN

Ognjen Joldzic, Zoran Djuric, Dijana Vukovic

Faculty of Electrical Engineering Banja Luka, Bosnia and Herzegovina

Email: {ognjen.joldzic, zoran.djuric, dijana.vukovic}@etfbl.net

Abstract

Network convergence, user mobility and various types of applications all contribute to the inhomogeneity of modern networks. The emergence of new technologies, unfortunately, increases the number of possible security threats to all parts of infrastructure. Therefore, network security protocols and mechanisms have to be able to respond to any security threat without affecting the performance of the network or degrading the quality of service. This paper presents an early stage concept of a transparent intrusion prevention system (TIPS) implemented using a combination of various technologies, most notably Software-Defined Networking (SDN) and poll-mode packet processing, which enables deep packet inspection in high-speed network environments.

1 Introduction

Modern networks have to be capable of carrying different classes of user traffic across the same physical connections (regardless of the traffics importance, type and technical requirements), and to still be able to provide each of the users with a satisfactory quality of service. This process, known as network convergence [1], at the same time introduced a number of side effects, not all positive, which had to be addressed in order for the primary goal of these networks to be accomplished. Positive aspects certainly include the reductions of costs (in both technical and administrative areas of service deployment), and a common development platform for future protocols and services [2]. However, the process of convergence puts an added strain on all segments of the network, starting with the processing devices required to transport the data to the end-users. Sending mixed content across general-purpose networks means that this traffic has to contend for the required bandwidth, and that additional measures must be taken to ensure its priority and low latency. This means that the network software and devices have to be aware of the content of the traffic, and contain special processing logic to perform their primary function without degrading performance.

A crucial aspect of computer networks that has to be covered in any modern network is security. Security threats warrant an implementation of a wide array of security protocols and solutions, which detect or eliminate any such threat without causing consequences to the normal operation of the network.

This paper was presented at the NIK-2014 conference; see http://www.nik.no/.

This paper proposes an approach for detecting and preventing malicious network activity, which will have minimal impact on regular network traffic. As the research is in its initial stages, most of the aspects of the proposed solution fall into the category of future work. The platform is based on transparent, adaptive and scalable network design in order to overcome the limitations of the currently standard approach to intrusion detection and prevention systems (IDS/IPS), and to leverage the advantages of several new technologies and concepts.

2 The Proposed Transparent Intrusion Prevention System (TIPS)

Ordinary means of packet capture are based on interrupts generated by the network interface card (NIC), which is serviced by a routine that performs the capture. Research published in [3] shows that for lower speed networks, this mode of operation is sufficient enough to provide a capturing framework that has an insignificant packet loss rate, and that no major performance gain is achieved by utilizing a different capturing software layer. However, the same research shows that the amount of time spent servicing the interrupt request in high speed environments is far too expensive for any application. The latency and the packet loss rate increases with the increase of speed, which leads to a conclusion that standard techniques for packet processing cannot yield satisfactory results in those conditions.

These effects can be mitigated by taking a different approach, which includes (partially or completely) eliminating interrupt requests and moving to a technology called device polling. Device polling has been explained in [3], and involves a more efficient mechanism in environments where a low latency (or high throughput) is required. Instead of spending long periods of time servicing interrupt requests originated by the NIC, the processor masks all further interrupts generated by the card, and allocates a task that polls the NIC in regular intervals. This results in a dramatic improvement in efficiency and speed of packet processing.

The use of technologies described in previous section enable this network security layer to function transparently to the rest of the network, including the devices directly connected to its interfaces. All traffic can be forwarded without altering any of the information within the header of any encapsulated PDU (Protocol Data Unit), providing the illusion of a direct physical connection between the devices that are on different sides of the security device. Even if a potential attacker is aware of the existence of TIPS, he would not be able to target it directly by an attack, which is an important advantage compared to other similar solutions.

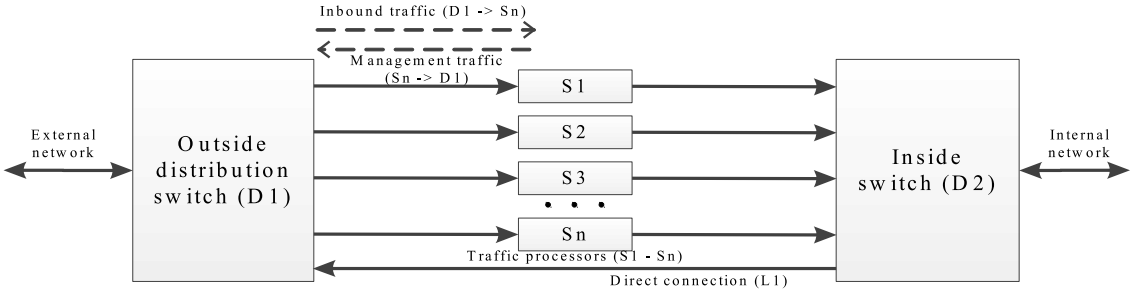

Figure 1: An Overview of TIPS Components

Figure 1 shows the basic components of TIPS. The middle layer of the diagram

(comprised of the nodes denoted in Figure 1 as S1, S2, etc.) presents an arbitrary number of hosts that perform the packet processing. One of the design goals of the entire proposed platform is to allow an easy expansion of the number of scanners and to quickly adapt to any potential change in configuration. This will be achieved by introducing another software layer between the processing hosts and the surrounding networks (denoted in Figure 1 as D1 and D2) that will be responsible for traffic distribution. This layer will be implemented by using SDN devices, which provide logically centralized network control for maintaining the rules for traffic forwarding.

During the operation of TIPS, the scanners communicate with the SDN switches by transmitting special, locally significant, link-layer frames. These frames determine the operation of the network, and affect the ways in which the traffic is distributed to the scanners. The switch creates a path to every link on which a scanner is detected and distributes the incoming traffic according to the number of currently active scanners, with the distribution algorithm depending on the type of the attack. With the inclusion of a new scanner, the distribution pattern is dynamically re-evaluated and reapplied in real time. The distribution algorithm is responsible for maintaining equal processing loads on all scanners, by adapting the distribution patterns in real-time according to the current load statistics. This alleviates the SDN switch of the added processing strain in high-speed network environments. Since the internal communication is limited only to nodes within TIPS, this protocol would be arbitrarily designed to minimize the amount of data transmitted between the nodes and the amount of processing required by the switches to respond to changes in configuration.

Upon detection of malicious traffic, the scanner that detected the activity instructs the SDN switch to discard all such traffic by installing one or more rules inside its forwarding database. For attacks such as DoS and DDoS, an entropy-based algorithm that is relatively common in literature could be implemented [4]. This implementation has to be executed in a way that will utilize the scalability of the platform and the variable number of scanners. The change in the number of scanners must not, in any way, affect the validity of the detection algorithm. After an arbitrary period of time, the discarding rule is aged out on the switch, and the entire process is repeated. Since the outside networks are designated as external and internal (i.e. the attacks are only expected for the external network), the routing within this transparent network is asymmetrical - the traffic originating from within the internal network is always sent through the direct connection between the switches, thus further increasing performance and reducing latency.

3 Related Work and Contribution

Most existing IPS solution are signature-based systems that require prior knowledge about the incoming attacks in order for a successful detection [6], [7], with only a smaller number dealing with anomaly detection [8], [9]. TIPS is a destination-based [5] IPS that offers the following contributions to the field. The use of SDN and poll-mode processing technologies enables the implementation of a transparent network security device, that should be able to adaptively respond to network threats based on anomalous network behaviour. The performance gain is expected from a flexible design with a variable number of processing devices and a traffic distribution algorithm that should be able to equally allocate the available resources and thus be efficient against Denial of Service attacks.

4 Conclusion

The main contribution of this paper is the initial step towards the implementation of a transparent intrusion detection and prevention system. The authors of this paper argue that the development of a transparent network layer mitigates one of the most important problems in deploying any security device attacks aimed directly at the device itself. The solution aims to combine several network technologies, primarily SDN and poll-mode packet processing, in order to create an adaptive platform that will be able to respond to most network threats within a very short period of time.

References

[1] J. Ellis, C. Pursell, J. Rahman, The Convergence of Voice, Video & Network Data, Academic Press, 2003,

[2] A. Umar, S. Moyer, The impact of network convergence on telecommunications software, IEEE Communications Magazine, Volume 39, issue 1, 2001, pp. 78-84,

[3] L. Deri, Improving Passive Packet Capture: Beyond Device Polling, Proceedings of SANE, 2004,

[4] K. Kumar, R.C. Joshi, K. Singh, "A Distributed Approach using Entropy to Detect DDoS Attacks in ISP Domain", International Conference on Signal Processing, Communications and Networking ICSCN '07, 2007, Chenai, pp. 331-337,

[5] S.T. Zargar, J.B.D. Joshi, D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", IEEE Communications Surveys & Tutorials, 2013, pp. 2064-2069

[6] U. Oktay, O.K. Sahingoz, "Proxy Network Intrusion Detection System for Cloud Computing", Proceedings of International Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE), 2013, pp. 98-104

[7] S. Garg, A. Garg, A. Kandpal, K. Joshi, R. Chauhan, R.H. Goudar, "Ontology and Specification-Based Intrusion Detection and Prevention System", Proceedings of Confluence 2013: The Next Generation Information Technology Summit (4th International Conference), 2013, pp. 154-159

[8] K. Giotis, C. Argyropoulos, G. Androulidakis, D. Kalogeras, V. Maglaris, "Combining OpenFlow and sFlow for an effective and scalable anomaly detection and mitigation mechanism on SDN environments", Computer Networks, Volume 62, 2014, pp. 122-136

[9] C. Xiuquing, Z. Yongping, G. Yu, "Adaptive Intrusion Prevention Algorithm Based on HMM Model", Proceedings of 2011 International Conference on E -Business and E -Government (ICEE), 2011, pp. 1-4