Towards an SDN-Enabled IDS Environment

Sebastian Seeber
Research Center CODE
Department of Computer Science
Universität der Bundeswehr München
Neubiberg, 85577, Germany
sebastian.seeber@unibw.de

Lars Stiemert
Research Center CODE
Department of Computer Science
Universität der Bundeswehr München
Neubiberg, 85577, Germany
lars.stiemert@unibw.de

Gabi Dreo Rodosek
Research Center CODE
Department of Computer Science
Universität der Bundeswehr München
Neubiberg, 85577, Germany
gabi.dreo@unibw.de

***Abstract*—Security related monitoring in high speed backbone networks is still a challenging task, since the amounts of data to process increases continuously. Thus, new approaches need to be investigated to detect and handle attacks in high-speed environments to protect the underlying access lines. Therefore, we introduce a new approach for redirecting suspicious traffic taking advantage of properties of OpenFlow in an SDN environment. Using this, we are able to redirect identified suspicious traffic to various IDSs for further inspection in a dynamic and adaptive way. Our solution is able to drop bogus traffic as well as forwarding DDoS related traffic to a DDoS WASHING MACHINE. Furthermore, it is able to cope with privacy concerns, because only traffic marked as suspicious which can not be processed on-site is redirected to cloud security providers.**

I. Introduction

Security at network level states an important research area since consumers and companies push their data continuously into cloud environments [1] and more data is transferred over large distances, e.g. between branch offices. A reason for this evolution is the increasing popularity of cloud services as well as simplicity and fast dynamic expandability of resources on demand. Furthermore, the fact that people are connected everywhere with any device fosters the exchange of personal data.

From the network security and availability perspective, there exists an increasing amount of distributed denial-of-service (DDoS) attacks during the last years [2]. A recent report from Akamai [3] shows 90 % growth of DDoS attacks in the last 12 month, whereby the motivation ranges from political or social - including hacktivism and cyber warfare - to self-enrichment or revenge [4], [5].

To raise the attractiveness of security solutions, new approaches that reduce false-positive rates in the detection process and act without the need of human interaction, have to be developed. Furthermore, a positive trade-off is mandatory for a widespread adoption, e.g. maintaining an own probing infrastructure or hiring additional technical support is not a choice for most businesses [6], [7]. Considering this, the advent of software defined networking (SDN) promises a large variety of possibilities to improve network monitoring and traffic steering. Nevertheless, widespread deployments using SDN principles are still rare and mostly static (proactive) configured [8], [9].

Following this principle companies get an incentive to deploy such solutions, since in particular costly reconfiguration of network devices and attached IDSs is no longer required. In addition, companies are able to reuse existing solution with our integrative approach. Furthermore, using vendor-independent protocols like OpenFlow, which are not depending on special vendor working groups, fosters the adoption and modularity of our solution and helps companies to get away from strong vendor dependencies. Besides this, NETCONF is designed to change the configuration itself of a device, in contrast OpenFlow is creating forwarding table entries which is much more flexible and adaptive.

II. Approach

Existing security function implementations are deployed in a static fashion, which does not include changes of the network itself much less being able to cope with high sophisticated network enabled attacks. Therefore, our solution provides security functions in a dynamic and free composable manner - based on immediate detection results - concatenating adaptive programmable security functions. This approach is primarily based on the overall idea of [10]. OpenFlow is a well-established protocol in SDN deployments, hence the most suitable enabler for our approach. In the following the concept of our approach is briefly illustrated: Incoming traffic reaches an OpenFlow enabled switch (OF-switch). This switch is equipped with a base rule set in the forwarding tables. This base rule set acts as a light IDS that maintains a history of recurring events including involved IP addresses as well as information from external sources. These sources include public available black-lists, white-lists, geolocation data and their severities. Further developments of these lists include the correlation of IP-to-location mappings to support the suspiciousness value of an event and additional consumer triggered event lists. This value is calculated based on the Common Vulnerability Scoring System (CVSS), which includes amongst other how unlikely a vulnerability is exploited and the source of an attack based on the IP address. That's what we call severity in our case.

Based on this database of events, lists and previous observed incidents, forwarding rules inside the OF-switch are modified to adapt the functionality of the overall monitoring and detection process. Therefore, the steering entity (SDN controller) maintains a rule set per consumer that includes basic knowledge about the capabilities on the consumer site to detect security related behaviour (e.g. IDS) and preferred DDoS WASHING MACHINES [11]. This knowledge is essential to forward the suspicious traffic to the consumer for reducing false-positives on the one hand and on the other hand to redirect only the attack traffic in case of a DDoS attack to the WASHING MACHINE the consumer has a contract with. As a DDoS WASHING MACHINES we consider cloud services

978-1-4673-7876-5/15/$31.00 ©2015 IEEE

that are able to cope with huge amounts of attack traffic (e.g. CloudFlare, Fortinet). Based on the on-site detection results of the consumer, the steering entity is able to adapt the forwarding behavior of the OF-switch (iterative rule refinement). To collect all the results our solution is based on existing standards and interfaces to exchange security events via message protocols like IDMEF and TAXII. These protocols are commonly used for incident exchange between multiple vendor solutions [12].

Our approach follows the overall goal to reduce false-positives and improve the quality of the forwarding rule set progressively. In coincidence, our solution claims to immediately redirect attack traffic that would cause an overload of the on-site network to a cloud security provider that is able to cope with this amount of traffic, having in mind privacy concerns of the consumer. Following this, our solution redirects only attack traffic to a cloud security provider leaving the trustworthy part untouched.

III. Initial Results

To evaluate our approach we use the opportunity of our participation in the FLAMINGO Joint Security Lab (FJSL), where we get access to traffic traces from partners including detected and identified malicious traffic. Our proof of concept is running in a dedicated environment including three HP 2920 OpenFlow-enabled SDN switches, a traffic steering entity (Ryu SDN controller supporting OpenFlow Version 1.3) and three Open-Source Intrusion Detection Systems (Snort, Suricata, Bro) running on Dell 2950 server hardware and one dedicated Cisco IDS.

As a knowledge base for our steering entity we collected black-lists from Spamhaus (SBL XBL, PBL, DBL), OpenBL, APEWS and PSBL. To correlate the traffic with geolocation information we used a self build geolocation database. This database consisted of different weighted sources like MaxMind Geolite, whois and BGP. Using this we outperformed pure MaxMind or whois by up to three percent accuracy on country level for IPv4 and four percent for IPv6 [13].

Within our evaluation we replayed the traffic from the FJSL and included further malicious content using simulated BlackEnergy Botnet [14] traffic with hard coded IP addresses of our lab. The continuous observation of our Proof of Concept lab environment showed a reaction as expected. In the first step we grounded our detection results on the events generated by our IDSs. These are fed into our steering entity via common known security incident protocols like IDMEF or TAXII respectively, depending on the capabilities of the IDSs. Subsequently, our steering entity pushed flow rules to support further detection cycles in order to reduce false-positive rates. In the second step we took advantage of the BlackEnergy Bot simulation in our lab. Therefore, we removed relevant rules within the IDSs that are able to detect BlackEnergy Bot directly. In the following, we observed that a set of IP addresses is still repeatedly identified with a low severity by our IDSs (recurring behavior). Combined with our geolocation database and due to the recurring observation of these IP addresses our approach was able to reidentify BlackEnergy Bot and as a consequence pushing modified forwarding rules.

IV. Conclusion & Future Work

As current security threat reports constitute more and more sophisticated and high volumetric attacks our approach supports defense and detection mechanism by combining existing solutions in a highly dynamic and decomposable manner. In addition, our solution maintains an attack history directly in the steering entity enhanced by existing up-to-date black-lists and our self build geolocation database. We pointed out our results and proved our approach with a Proof of Concept in a lab environment, where we used real traffic traces collected from our partners in the FJSL. As a next step we will investigate possibilities to prove our solution in a real network environment and further experiments with attack traffic from labeled traffic data sets.

Acknowledgment

This work was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Programme.
Additional thanks for supporting us goes to RUAG Schweiz AG, Division RUAG Defence concentrating its network enabled operations activities in a business unit designated NEO Services.

References

[1] Franklin Morris, Infographic: SMB Cloud Adoption Trends in 2014;. Last accessed on 2015-01-28. Available from: http://www.pcworld.com/article/2685792/infographic-smb-cloud-adoption-trends-in-2014.html.

[2] Arbor Networks - Worldwide Infrastructure Security Report 2014;. Available from: http://pages.arbornetworks.com/rs/arbor/images/WISR2014.pdf.

[3] Akamai - Q4 2014 State of the Internet Security Report;. Last accessed on 2015-01-28. Available from: http://www.stateoftheinternet.com/resources-web-security-2014-q4-internet-security-report.html.

[4] Passeri P. Cyber Attacks Timeline Master Indexes;. Last seen: 2015-05-14. Available from: http://hackmageddon.com/cyber-attacks-timeline-master-indexes/.

[5] Inc CS. Cisco 2015 Annual Security Report;. Last seen: 2015-05-14. Available from: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.

[6] PwC. The Global State of Information Security Survey 2014. PwC;. Last seen: 2015-05-19. Available from: http://www.pwc.com/gx/en/consulting-services/information-security-survey/giss.jhtml.

[7] Symantec N. National Small Business Study. Symantec;. Last seen: 2015-05-19. Available from: http://www.staysafeonline.org/download/datasets/4389/2012_ncsa_symantec_small_business_study.pdf.

[8] Vissicchio S, Vanbever L, Bonaventure O. Opportunities and research challenges of hybrid software defined networks. ACM SIGCOMM Computer Communication Review. 2014;44(2):70–75.

[9] Maturing of OpenFlow and Software-defined Networking through deployments. Computer Networks. 2014;61:151 – 175.

[10] Seeber S, Rodosek GD. Towards an Adaptive and Effective IDS Using OpenFlow. In: Intelligent Mechanisms for Network Configuration and Security. Springer; 2015. p. 134–139.

[11] KROPÁČOVÁ A. CESNET-CERTS Computer Security Incident Response Team CESNET Zikova 4, Prague;.

[12] Steinberger J, Sperotto A, Golling M, Baier H. How to exchange security events? Overview and evaluation of formats and protocols. In: Integrated Network Management (IM), 2015 IFIP/IEEE International Symposium on. IEEE; 2015. p. 261–269.

[13] Koch R, Golling M, Stiemert L, Rodosek GD. Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis. Systems Journal, IEEE. 2015;.

[14] Nazario J. Blackenergy ddos bot analysis. Arbor Networks. 2007;.