Journal of Engineering and Applied Sciences 13 (Special Issue 9): 6961-6966, 2018
ISSN: 1816-949X

Smart Network Probes for Campus Network Incident Analysis

Ladislav Balik, Ondrej Hornig and Vladimir Sobeslav
Department of Information Technologies, Faculty of Informatics and Management,
University of Hradec Kralove, Hradec Kralove, Czech Republic

Abstract: The aim of this study is to present a security system proposal based on the integration of smart network probes with a focus on the creation of complex solution which was implemented during the project of smart network probes at University of Hradec Kralove. This study presents a system designed for academic research environments where it serves as a tool for extended security in protection of sensitive data used in research and development against the local and remote threads.

Key words: Firewall, honey pot, network monitoring, network probe, packet inspection, real-time analysis, security

INTRODUCTION

Network security threats and vulnerabilities such as distributed attacks, exploits, viruses, phishing, etc. are arising gradually in time. According to the cyber security index which aggregates the views of information security industry professionals as expressed through a monthly survey, security problems rose up nearly 50% over last 12 months (Cyber Security, 2017). The ways the attackers infiltrate various electronic systems are becoming more and more sophisticated. This attack complexity is represented by the distributed characteristics, layered network approach and also with the utilization of social engineering techniques. Local policies may be hardened by a distributed firewall with the smart network probes which protect local end devices from the remote and local attackers at the same time. In general, the use of multiple, highly specialized and single purpose devices can produce far better results than the versatile one.

The more sophisticated attack is being held, the more intelligent security systems action has to be taken. Every local network perimeter must be secured by at least one border network element such as router, firewall or IPS. One solution may not successfully solve all the possible problems. Combination of more firewalling approaches brings together more methods for threats detection while the complexity of such system increases significantly.

Yet, another important topic in the area of networking security is the incident reaction time. This problem is arelatively complicated task to achieve and it touches several problems from the networking and security area. The amount of data is growing continuously, data has to be gathered, analyzed, parsed, stored in adequate period of time, otherwise the consequent reaction made by the security system might be useless. Therefore, the intelligent security system which can handle the huge amount of data, consist of specialized hardware, intelligent parsing techniques, fast databases and efficient security system.

For the previously mentioned reasons, the main goal of this article is to present a security system proposal based on the integration of smart network probes with a focus on the creation of complex solution which was implemented during the project of smart network probes at University of Hradec Kralove, granted and supported by the CESNET, Organization for e-Infrastructure for Science, Research and Education, Czech Republic. Firstly, the basics facts of network security monitoring are stated, secondly, the architecture of proposed system is presented and finally, the results of pilot project are discussed and analyzed.

MATERIALS AND METHODS

Network security monitoring: Network security monitoring is the key approach to proactively secure any enterprise network including the specifics of campus topologies. To face the network security challenges from distributed network attacks, combined social engineering techniques and other sophisticated methods, real time network flow analysis is very important and an integral part of any security system which is able to gain improved network security visibility (Cyber Security, 2017). This research area is relatively wide and it is also, represented by many research teams and vendor technologies such as CISO NetFlow or IPFIX. This area can be divided into the main categories:

Corresponding Author: Ladislav Balik, Department of Information Technologies, Faculty of Informatics and Management, University of Hradec Kralove, Hradec Kralove, Czech Republic

- Real time data flow gathering
- Data parsing a storing
- Intelligent security data flow analysis

Notwithstanding this scientific categorization and the research teams interest, the basic principles of modern network security monitoring of data networks lies on the inspection of communication elements, detection and prevention system and last but not least, the specialized hardware which is able to collect huge amount data in real time. We will devote the most important issues in the next section which discusses the smart network probes project.

Packet inspection: Recent computer networks, including the internet are built upon the TCP/IP Model which is de facto standard for any other networks, even in the industry (Brida *et al*., 2014; Horalek *et al*., 2015). The basic element at network layer is the packet, datagram respectively. Stateful packet inspection is an evolution of original packet filtering method, the difference between stateful inspection and packet filtering is the ability to monitor firewall or a state of connections. Packets belonging to these connections can be forwarded or dropped based on the information, whether it belongs to apreviously established traffic flow. Stateful Packet Inspection (SPI) denies all new incoming connections from an untrusted zone (or interface) by default. Connections from a trusted zone (e.g., local network) are matched to afirewall rules and only connections belonging to these flows are permitted from an outside network. This mechanism simplifies the rule creation, because it is necessary to define rules only in one direction. Rules for packets from an outside network are created dynamically (Mishra *et al*., 2011).

Application firewall, sometimes called as proxy firewall, provides similar functionality as a packet filter but adds additional capabilities in traffic inspection. Application firewall is able to analyze header information from first up to the seventh layer of ISO/OSI reference model. This method inspects largely deployed protocols such as HTTP, FTP, POP3, SMTP where application firewall is able to filter traffic based on URI information (Greenwald *et al*., 1996).

Prevention and detection systems: More complex but also, more resource-demanding approach is to inspect those packets that belong together in to the same data stream. Larger caching and better protocol knowledge are necessary. It is common that network attackers use the sequences of packets that can itself act as legitimate traffic but together present a security threat to vulnerable systems. Monitoring and analyzing of such packet streams enables to identify even segmented types of attacks. This method is used by IDS, IPS and some advanced firewall applications. This approach as written above is highly source-demanding and its utilization is usually planned on separate hardware-accelerated devices on the border of local network segment (Rehak *et al*., 2006).

Such sophisticated system, also, brings a new type of risk. As it is made up of many components and modules which may be manufactured by many different vendors, security risk of single component failure is therefore, ameliorated. Critical errors of a single module may significantly affect the whole system and generate new types of vulnerabilities. In this example, one software component failure (multiplied by number of components in every system) may open new security hole for potential attacker.

Specialized network probes: Network probe is a program or specialized device located in the middle of network. The main propose is the network activity data monitoring or collecting. The main reason for the implementation of specialized probe is the growing number of network data that must be analyzed in real time. At the rate of tens or hundreds of gigabits per second, the network flow must be evaluated using hardware accelerated probes. Net-Flow is a feature that was introduced on Cisco routers that provides the ability to collect IP network traffic as it enters or exits an interface.

Network flow agents are able to analyze the number of bytes, packets, flag fields, duration of flow. NetFlow technology helps to optimize the network infrastructure (Wang *et al*., 2011). The gathered data are then consequently used in security application for further decisions about the data flow legitimacy and other reaction can be performed. A common flow monitoring setup consists of three main parts:

- Flow exporter: aggregates packets into flows and exports flow records towards flow collectors
- Flow collector: responsible for reception, storage and pre-processing of flow data
- Analysis application: analyzes received data in the context of intrusion detection or traffic profiling

Another categorization of high speed network probes can be done on the basis of the data analysis, first method is the protocol payload analysis (Chen *et al*., 2014) which is limited mainly in encrypted data communication and the second is behavioral traffic analysis (Cyber Security, 2017).

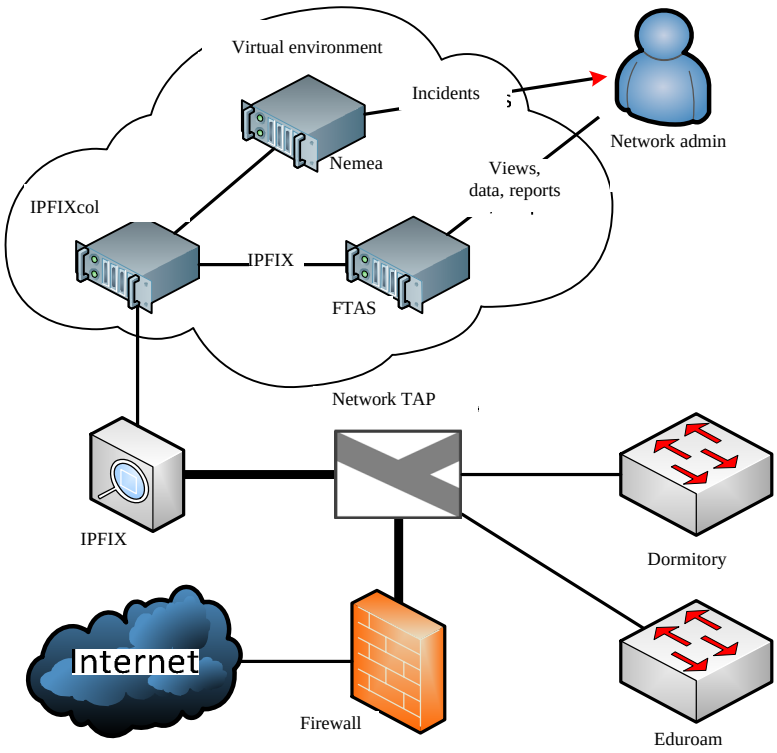

Fig. 1: Network flow monitoring-system architecture

Smart network probes application in campus network: Local network protection and their separation from the Internet network can be handled with commonly available technologies such as specialized firewall with strictly set rules and IDS/IPS penetration detection systems. Most networks are well-protected against security threats from the outside (Horalek *et al*., 2015). On the other hand, traffic monitoring in the local networks is often ignored and the inner perimeter of the network usually has lower protection. One of the main problems is the huge amount of data that flows between the local networks at high speed (Rehak *et al*., 2009). This data must be captured, analyzed, processed, saved and passed to the security systems that will subsequently identify any threats.

Before the realization of the project, protection options of local networks in the campus network were limited as no suitable solution could be found. During the project realization, specialized safety technologies developed by CESNET (e.g., high-speed network probes, FTAS system and Warden) were used (Rehak *et al*., 2009). These technologies operate in "Security monitoring as a service" mode and in cooperation with the CESNET-CERTS security team.

Thanks to the STaaS service, utilities developed or used by CESNET are available to the associated organizations. From this set of utilities, a selection has been made. This selection allows global monitoring of the local network and identifies potential problems in the network. The monitoring of the Eduroam network and the dormitory network are the priority. For this purpose, we have chosen the technology of network monitoring based on IP flow. To realize this monitoring, we have used the following utilities provided by CESNET.

Probe with the IP flow data exporter. The probe consists of commonly available hardware (server bought for this project's purposes) and IP flow logger dedicated software. The probe allows monitoring and exporting the network and transporting layer data as well as the application of layer data. Thanks to the plugin concept, the probe can be easily upgraded.

To gather and store the data from the probe, IPFIXcol collector has been chosen as it allows to process data in various formats. The collector can process data from the application layer as well.

Data analysis. For the purposes of data analysis, Nemea system has been used as it contains various suspicious event detection modules. Nemea has the advantages of modularity, possibility to expand the module toolbox and an ability to process the incoming data. At the same time it is possible to export the data directly from the FastBit database and to perform additional statistical inspection which was addressed in this project as well.

FTAS collector. Along with the IPFIXcol collector, FTAS collector has been utilized as well. It serves to access the information about IP traffic. FTAS, also, allows setting up of automatic detection of network attacks and anomalies.

Honeypot. In some networks, both in private and in public range, a honeypot has been installed. It is set up to send warning reports to the people responsible for the campus security. The data about the incidents are sent to the Warden system as well as it allows share of this information with CESNET.

According to, the needs of monitoring of UHK's local networks, architecture from the instruments shown above has been assembled; it is pictured in Fig. 1. The probe is monitoring the online traffic and exports the expired IP flow records. The records are being saved to the IPFIXcol collector and at the same time forwarded to the Nemea system where their concurrent analysis is performed. At the same time, the records are being saved to the FTAS collector where the reports are continuously being counted, anomalies detected and data stored for their potential later manual analysis. The anomalies detected by the FTAS system and by the honeypot system are being sent by email to the people responsible for the computer network security. Given the low number of the authorized individuals, this solution is currently sufficient. Should the number of administrators responsible for these matters be increased, report sending to an autonomous ticketing system will be considered.

RESULTS AND DISCUSSION

Deploying a very restrictive firewall rules may help to suppress some types of threats but it certainly cannot solve the complexity of local area network security. Additionally in accordance with the principle of academic freedom, university networks, users and project should not be restricted more than necessary. The only way is therefore to monitor the actual operations which are generated from the user work or system operations, this important information can be used for the suppression or prevention of security threats. Due to the previous mentioned presumptions it was thus necessary to equip the local network perimeter with appropriate probes that will monitor network traffic and provide data evaluation on the collector. These operating figures exclude the content of network traffic and therefore do not affect the privacy of users. Another yet important asset of proposed solution is the use of open standards such as IPFIX or NETCONF without proprietary extensions. This makes them suitable for integration with the existing systems and technologies. With regard to emerging threats, software can be used to innovate probes and probes updated regularly.

The main contribution of the project is the incorporation of the monitoring component to the campus's local network interface. Before this project's initiation, no way of this thorough central monitoring of the network traffic was available. Another significant merit of this project is the periodic report generation. These reports can be provided for auditing or even proving in case of any inadequate user behavior in the network that would contradict the campus computer network usage policies.

Tested solution adaptation: Based on the experience from the testing deployment, a few adjustment measures have been carried out. The initial plan reflected the experience with the deployment in CESNET2 WAN network. As the new solution was deployed at a local network's border, the amount of actual data traffic was substantially lower than expected.

Time granularity for file generation from the received data was modified. The time interval was changed from 5-30 min. This change helps to prevent too high number of files to be created on the drive which yields two main advantages: the first advantage is that it economizes file system's i-nodes and the other one is that the data is processed more effectively during the analysis.

The monitored data is subsequently inspected. Besides common information from network and transport layers, information about the flows from some protocol's application layer is collected as well. Those protocols are SMTP, DNS, HTTP, HTTPS and SIP. The performance characteristics are as follows:

At the probe's input, the average data traffic was measured to be 7k/sec packets. The amount of data was on average 61MB/sec. At the probe's output, on average 186/sec flows were measured while the minimum number of flows exported was 7/sec and the maximum was 707/sec flows.

Data evaluation methods: To store the information about the received data, FastBit database is used. It is a column-based NoSQL database that offers a basic set of search functions based on the technology of compressed bitmap indexes. This approach allows faster searching than a typical SQL database. However, its modifications are more difficult.

The data is stored in common files that are identified by their name and path. Such a file can be loaded quickly as its path corresponds to the timestamp of its creation. Every particular record in the FastBit database contains the information about the corresponding data flow. The basic information is the start and the end of the data flow which can be found in Data flow start and Data flow end columns. Depending on the communication type in the third (network) layer, the source and destination IPv4 and

IPv6 addresses can be tracked. For socket structure and communication identification, the port (source and destination) must be tracked as well. Additional parameters that allow detection of the deployed probes are various headers of the monitored protocols (HTTP, SMTP, etc.).

To export data from the database, fbitdump application is used. It allows use of many variables and attributes for exported data filtration and their view. The data can be presented either directly in lines or as aggregated data using custom key metrics. FastBit can also, make data accessible in the CSV format which can be easily redirected to the file using an operand. The data obtained this way can be imported into a large number of other databases (e.g., SQL) spreadsheets or specialized statistical analysis software.

The most important analytical outputs are Nemea system reports. These reports are generated every week during Monday night. The output contains transfer statistics for individual protocols and at the same time possible safety issues identified in the data flows (based on spamlists and blacklists). The generated report documentation is divided into four main parts. The first part contains TOP-N statistics based on the number of bytes transferred and the number of connections opened from the perspective of various IP addresses or IP address segments (the third layer information is used). The second part analyzes the data flows using the identification of communicating protocols and it assigns those amounts of transferred bytes and packets and total established connections. All the protocols are inspected from the perspective of the source and destination IP addresses (or subnets).

The third part analyzes suspicious data flows using behavioral analysis and rates their suspiciousness. The administrator is to make the final decision whether the activity is indeed defective, or whether it was only incorrectly identified. Among the employed measures there were also, techniques for detection of brute-force attacks trying to crack SSH, RDP or Telnet protocol passwords. Another measure was IP blacklist filter that monitored communication of the local addresses with the addresses listed on defined blacklists (e.g., Malware, ZeuS, SpamHaus, PhishTank).

Using the mechanisms described above and periodically generated outputs, the traffic in the local network can be well documented and IPS/IDS mechanisms implemented in the central firewall can be adjusted. As for future expansion of these measures, the implementation of data collection using NetFlow protocol in multiple devices (e.g., in the future planned Cisco Catalyst 6500 L3 network switches) as well as in other university networks used by e.g., employees can be considered.

Incident types: In settings of firewalls at the border of the local network and the Internet, restrictive protection is applied. Traffic is allowed only in explicitly specified ports. For these reasons, both in TCP and UDP it was reasonable to expect the user's attempts to avoid the given safety policies.

One way to avoid the policies of forbidden ports is masking data traffic in VPN connections. Ports in the table above that are directly permitted are OpenVPN, L2TP and PPTP. Another way is to use SSL VPN which uses port 443 or to use a port of a different protocol.

In the network, devices communicating from the addresses outside the local subnet were detected and therefore, from the perspective of LAN, they were communicating from non-existent networks. These devices are usually incorrectly configured or connected they are assigning their ranges to local networks managed by the university via. DHCP servers or trying to communicate with the remembered addresses of the networks they were connected to before (e.g., laptops with printers). In worse cases it could imply searching for the networking devices in default settings and attempts to attack them have been made. However, no such case has been detected.

Using Nemea framework, incidents regarding communication with the blacklisted IP addresses have been detected. The events with the highest intensity have been detected for the SpamHaus blacklist. Given the strict filtering policies that block all the email communication, we can assume those were falsely positive events. Events for the command and control blacklists regarding ZeuS and Feodo botnets have been detected as well. These were mostly communications of multiple private addresses with one external address. These events have been investigated more in depth. The last type of the events detected was use of the Tor anonymity network. In case of the Tor network, the traffic does not necessarily have to be unwanted but given the Tor network's qualities it is appropriate to monitor such events. In case of investigation of the incident it is appropriate to consider whether the IP address initiated connection or whether it was contacted by the Tor node.

CONCLUSION

The main aim of this project was to ensure better control over the state of the network services via continuous surveillance over the traffic in the networks where it is not possible to fully monitor the connected user's devices. Thanks to this monitoring it is possible to uncover anomalous states and to respond to them adequately. Simultaneously it is necessary to maintain the quality of the current university network's traffic. In the future the expansion of the system to all the university

network subparts is planned and so, information is being gathered about the safety incidents in the local networks with the development of new reports and collected data analyses.

ACKNOWLEDGEMENTS

The researchers would like to thank the CESNET organization and the CESNET-CERTS security team for the funding and the technological solution which has been implemented as a pilot project. This work and the contribution were also supported by project "Smart Solutions for Ubiquitous Computing Environments" FIM, University of Hradec Kralove, Czech Republic (under ID: UHK-FIM-SP-2016-2102).

REFERENCES

Brida, P., J. Machaj and J. Benikovsky, 2014. A modular localization system as a positioning service for road transport. Sensors, 14: 20274-20296.

Chen, Z., Y. Wu, J. Ge and E. Yuepeng, 2014. A new lookup model for multiple flow tables of open flow with implementation and optimization considerations. Proceedings of the IEEE International Conference on Computer and Information Technology (CIT), September 11-13, 2014, IEEE, Beijing, China, ISBN: 978-1-4799-6240-2, pp: 528-532.

Cyber Security, 2017. Index of Cyber Security. Cyber Security. http://www.cybersecurityindex.org/.

Greenwald, M., S.K. Singhal, J.R. Stone and D.R. Cheriton, 1996. Designing an academic firewall: Policy, practice and experience with surf. Procedings of the Symposium on Network and Distributed System Security, February 22-23, 1996, IEEE, California, USA., ISBN:0-8186-7222-6, pp: 79-92.

Horalek, J., S. Karamazov, F. Holik and T. Svoboda, 2015. Analysis of the Use of Cloud Services and their Effects on the Efficient Functioning of a Company. In: Computational Collective Intelligence, Manuel, N., N.T. Nguyen, D. Camacho and B. Trawinski, (Eds.). Springer, Berlin, Germany, ISBN: 978-3-319-24305-4, pp: 336-345.

Horalek, J., S. Neradova, S. Karamazov, F. Holik and O. Marik *et al*., 2015. Proposal to Centralize Operational Data Outputs of Airport Facilities. In: Computational Collective Intelligence, Nunez, M., N.T. Nguyen, D. Camacho and B. Trawinski (Eds.). Springer, Berlin, Germany, ISBN: 978-3-319-24305-4, pp: 346-354.

Mishra, A., A. Agrawal and R. Ranjan, 2011. Artificial intelligent firewall. Proceedings of the International Conference on Advances in Computing and Artificial Intelligence, July 21-22, 2011, ACM, New York, USA., ISBN: 978-1-4503-0635-5, pp: 204-207.

Rehak, M., M. Pechoucek, M. Grill, K., Bartos and V. Krmicek *et al*., 2009. Collaborative approach to network behaviour analysis based on hardware-accelerated FlowMon probes. Intl. J. Electron. Secur. Digital Forensics, 2: 35-48.

Wang, D., Y. Xue and Y. Dong, 2011. Memory-efficient hypercube flow table for packet processing on multi-cores. Proceedings of the Conference on Global Telecommunications (GLOBECOM 2011), December 5-9, 2011, IEEE, Honolulu, Hawaii, ISBN: 978-1-4244-9266-4, pp: 1-6.