Yadigar N. İmamverdiyev[1], Babek R. Nabiyev[2] DOI: 10.25045/jpis.v08.i1.09
[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]yadigar@lan.ab.az,[2]babek@iit.ab.az

CONCEPTUAL MODEL FOR THE INTELLIGENT NETWORK SECURITY MONITORING

This paper offers a fundamentally new and more effective conceptual model for the intelligent network security monitoring. It reviews the general intellectual architecture of the monitoring process, its functional blocks, processing and application trends. In addition, it explores the gaps and weak points of the monitoring system. To tackle the mentioned problems, the proposed model combines functional capabilities, such as the monitoring of problem-oriented information, initial processing of the gathered data, data indexation, data structuring, storing and managing collected data, selecting the data at the request of decision makers and generating readable and analyzable reports.

Keywords: *network security, monitoring, artificial intelligence, network traffic, conceptual model.*

Introduction

An intelligent monitoring of network security is the analysis of signs and warnings for detecting and responding to various intrusions causing threats for the computer network security. One of the main advantages of this system, as its name implies, is its intelligence. Intelligence indicates the use of artificial intelligence methods. Network security monitoring can also be carried out without the introduction of the artificial intelligence methods. However, it requires a lot of financial and human resources. Material resources and human labor can be reduced with the application of artificial intelligence methods by appropriately partially or completely automating this process. In particular, all the processes of the intelligent monitoring system of network security from sensors to decision-making should be implemented with the introduction of hardware and software based on artificial intelligence methods.

For the collection of the necessary data about the performance and safety of computer networks, their accurate analysis and making decisions on ensuring network security and the use of Data Mining technologies is of paramount importance in the course of the network security monitoring [1].

Numerous scientific and practical works have been done in this field. The approaches to the detection and removal of the threats may include: *security operations centers (SOC), security information and event management (SIEM) and Computer Security Incident Response Team (CSIRT).*

Network security management systems face the challenges in the course of the identification of abnormal events and the implementation large volumes of data processing. In this case, the completeness of the obtained data and decision is doubtful. The main objective of the conceptual model of the network security monitoring is to save computing resources and human labor by facilitating the process and assisting the decision-making. For this reason, various hardware, software and tools are used.

This case study offers a conceptual model for the intelligent monitoring of network security.

Network security systems

Intelligent monitoring of the network security is a complex system. Such systems work wider and large scale data, and therefore, ready solutions are very difficult to be found.

The systems combined for the network security have centralized, distributed or partially centralized structures. In the centralized systems, the data collected as per the segments are transmitted to the center for running analysis. The advantage of this structure is that it is possible to get more precise answer due to the complete transfer of data. The disadvantage is that the service denial may be unavoidable in the case of peak loading due to the centralized analysis apparatus.

The presence of only one denial point in these systems is unacceptable. On the other hand, there are distributed structures unattached to the unique center for the data analysis. Distributed system can be fully or partially centralized. In fully distributed structure, all segments and their function blocks are discretely equal. In other words, the failure of a segment has insignificant impact on the performance of the entire structure. However, constraints of the data and analysis processes in the local segment negatively affect the fullness of the results. In partially centralized structure, in certain circumstances, one or several segments are responsible on the analysis process. Nevertheless, in this case, the segment responsible for the process of analysis is loaded much more than others. For this reason, a balanced and partially centralized system should be established between the fully distributed and centralized systems.

[2] indicates that the local measures are no longer effective enough to ensure the network security. For example, it is known that the classic Intrusion detection systems (IDS) are no longer effective enough, and it is necessary to establish intrusion detection network. *DOMINO overlay* global intrusion detection network specified in [3] can be a good example. *DOMINO overlay* is a cooperation system for intrusion detection and responsible for the detection process of the intrusion in the large-scale and broadband Internet nodes. The system is geographically located in different places and has a hierarchical-heterogeneous structure. Nevertheless, there is an exchange of information between the network actors.

SIEM is another approach to the detection and removal of network security events. *SIEM* can have different functionality in accordance with the solutions offered by vendors. However, all *SIEM*s have something in common. Fundamental or key parts of *SIEM* are: collection, analysis/aggregation, and storage.

Safety operations centers are involved in organizational and technical security issues. Operational capacity of the system is realized on the basis of the following blocks: data generator sensors, data collection block for data storage, common format database, analysis of incidents, knowledge base, decision making and reporting.

*CSIRT*is a Computer Security Incident Response Team. Its main goal is to ensure the management of information security risks of corporate network at the adopted level. To this end, *CSIRT* performs the processes of detection and prevention of the actions aimed at the violation of information security and informs the users. *CSIRT* implements collection, storage and analysis of the statistical data related to the dissemination of malicious programs in the corporate network and network attacks [5]. To achieve the goals, *CSIRT* interacts with other organizations in the field of information security.

The organizational and practical systems to ensure the information security have been listed above. The main components of these systems include monitoring and resulting information. The conceptual model proposed in this article will ensure more rapid and substantial results.

Principles of building conceptual model

Intelligent monitoring of the network security is a complex system collecting the information about the network and directing the information about the analysis and its results to the concerned persons or systems, meeting modern requirements and consisting of software and hardware sets. The monitoring system provides the performance of numerous functions, which leads to the improvement of the network efficiency.

This system collects all necessary information via the sensors from computer network, computer systems, users and other sources. The data collection, storage, processing and visualization are separately difficult processes that require huge human labor. One of the issues, but not less important is correctly interpreting the data. As we mentioned above, a human factor here, of course, is also of paramount importance. In this case, intrusion detection system is required to properly interpret items according to what the threats are determined. Any error at this stage can lead to loss of control on the computer network security.

When it comes to the duties of the network security intelligent monitoring, the basic policy should be determined. This policy is also important for the information to be collected and analyzed ensuring the users with reliable and secure use of global and local network. This is very important for the prevention of the events to happen or to explore the happened incident.
Taking into account the abovementioned, first of all, it is important to establish the conceptual architecture of the system. This conceptual architecture specifies the requirements for each block and provides an easy transition into the implementation process.

The intelligence of the units is not limited to the separate introduction of artificial intelligence models. Conceptual architecture incorporates many local, regional and one global center, which creates the hierarchical structure. If the model units with the same rank are defined and a favorable condition is created for the exchange of information between them, the problem can be solved at lower levels. In other words, depending on the level of the problems, for their operational elimination and with minimal material damage, initially, they should be resolved at the local level.

The conceptual architecture of intelligent monitoring of the network security are set up with the duties and functions, processes and sensors, systems, including used modern technologies. As Figure 1 shows, the architecture generally consists of collection, analysis and decision units. Each unit consists of sub-units performing certain functions. They are explained below in details.

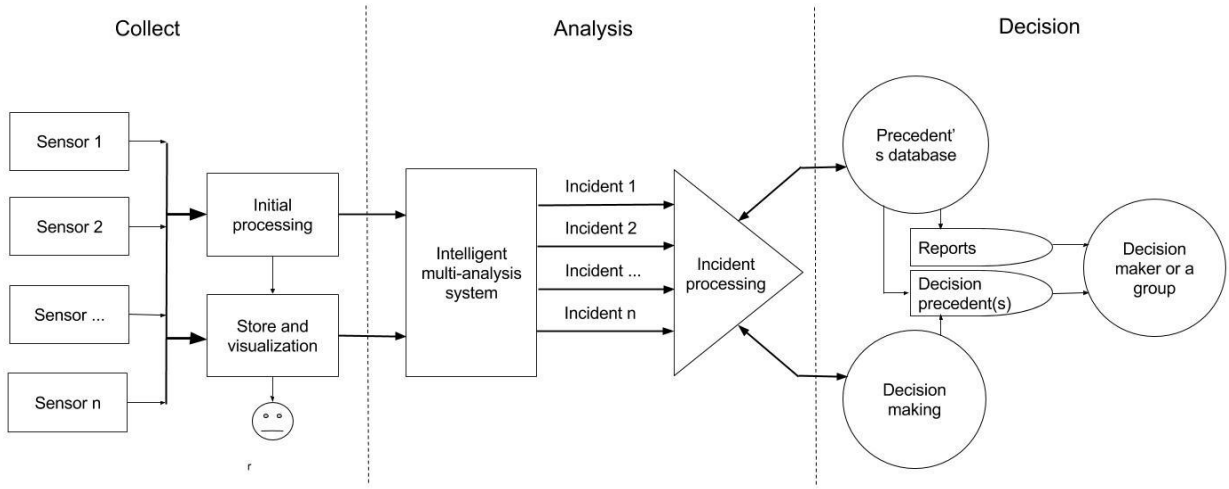

Figure 1. Conceptual architecture of the intelligent monitoring of the network security.

Collection unit

Collection (sensors) - Different types of sensors are used to collect information about the network. These sensors can run autonomously or be managed from a single center. The number and types of sensors may vary according to the profile and scope of the monitored network. The class of the sensors is determined by the nature of collected data. The sensors can generally be divided into 2 classes: hardware sensors and software sensors. However, these sensors are also divided into sub-classes according to the type of the collected information (traffic, process, user activity sensors, etc.). Hardware sensors may refer to generally accepted monitoring sensor as *SNMP, IPFIX, sFlow* and others. The manufacturer referred sensors are also available, such as *Cisco-netflow, Microsoft - Windows Network Card Sensor* and etc. Software sensors include *PRTG - Packet Sniffer Sensor, Core Health Sensor, Sensor Cluster State* etc. these sensors are designed for logging the activity generated from determined sources.

Collection and analysis of the traffic flow is one of the most common methods for the monitoring of the broadband networks. This approach is very relevant at the provider level. *NetFlow, IPFIX* and other protocols are used for the collection of the traffic flow. Monitoring

stages of the traffic flow are closely connected with one another, and each stage shall be carefully studied [6]. These stages realize the package observation, flow measurement and transmission, data collection and analysis.

The traffic can be analyzed at the package level through the sensors located in the network. Package-based monitoring is opposite tothe monitoring of larger scaled traffic flow and ensures to obtain more detailed information. However, the implementation of this process causes the danger for the personal data of a user and requires powerful processor and large RAM for the processing. [7] offers a monitoring method that mention only the first four bytes of the package and requires less resource.

Initial processing–since the data are generated from the various sensors and in various formats, initially, they are undergone the aggregation process, and as a rule, all data is converted to unique format. This process is called consolidation. Correlating the data undergone the aggregation process and gathering the different parts of the attack in thesame form, the detailed information can be obtained.

Storage - according to the corporate policy, the received information is stored for a certain period of time. Obviously, the information generated by the network structure, services and users is becoming a mass of information over time. Therefore, the data in which the anomalies are not detected and is in accordance with the current policies passing through classification mode for offline data storage, must be constantly stored.

Storing only the data with detected anomalies can lead to the lack of certain information in the course of re-analysis of the data, nevertheless, this will be useful for the proper use of resources, which are not unlimited at the end result.

Collection and storage of the network traffic data becomes more difficult due to the expansion and acceleration of the networks, whereas, solutions such as SQL database and custom binary format can not be extended in accordance with the increasing pace of incoming data. [8] shows an open source software generated with the synthesis of the network traffic collection tool *nProbe* and *FastBit* database. The network traffic flow until the *Gbit* speed can be collected and any information can be searched and found anytime through this method.

Visualization -the visual appearance form for the understanding of numerical data about the network traffic and the initial observation tool for operators. It may include *Cacti, Nagios* and other open code software. These tools generate line graphs collecting computer network traffic, status of counting nodes and statistical information about the equipment via *SNMP* in a certain time interval (Figure 2).

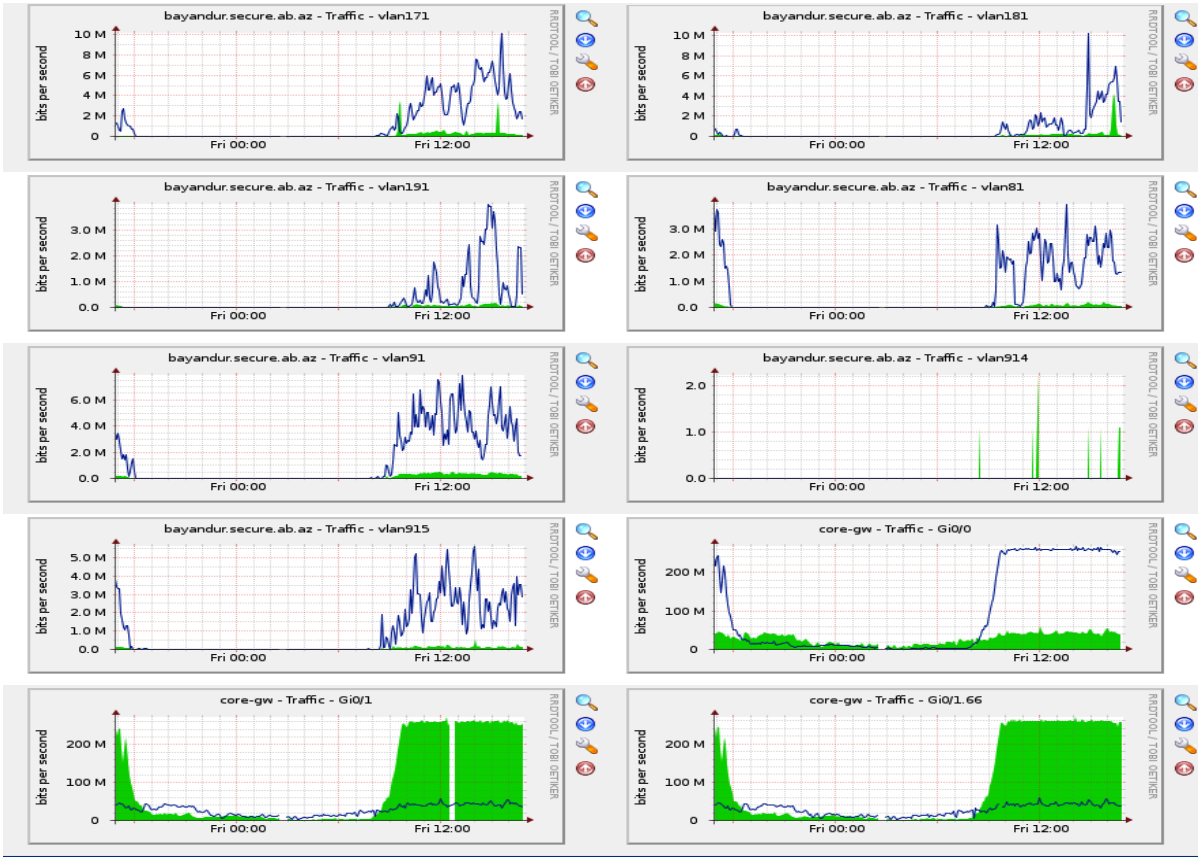

Figure 2. Diagram visualization of the network traffic

Analysis unit

Network traffic identification and categorization is one of the main elements of its management. It may include flow prioritization, traffic shaping and diagnostic monitoring.

Internet traffic measurements are often performed on the server, which has high computing power. The server collects and analyzes the traffic flow and packages. Given that in the course of the long-term, large volume and large-scale statistical data monitoring, *Tera* and *Peta* bytes of data are generated, it is not expedient to perform this processing on one server. Typically, discretization or aggregation methods are used for large-scale data compressing, in this case, certain data of the traffic flow is reduced. Recently, cloud computing technologies and cluster file systems are used to address this issue. For example, the use of cloud-based *MapReduce* software platform is offered for the analysis of Internet traffic [9]. The experiments based on open-source software *MapReduce* and *Hadoop* show that the statistical traffic calculation is achieved 72% faster than the single-server calculation tool.

The studies aimed at improving the efficiency of network management and network security widely use traffic classification and clustering. Moreover, the studies in the field of traffic analysis are also becoming relevant with the extensive use of the Internet and the development of the protocols and applications. Classification and clustering methods are widely used for the detection of information security incidents or anomalies. For instance, [10] offers two-stage sequenced classifier to improve the characteristics classification without reducing the efficiency or accuracy using *NaiveBayes* and neural network techniques.

It is known that one of the causes of the threats is the generation of anomalous traffic in the network, which is not in line with the thematic profile. Taking this into account, [11] has developed a tool to identify the behavior profile of the network traffic. Identifying the behavior profile the k-means clustering method is applied.

[12] offers the realization method for the real-time identification and classification of the network traffic. Six machine learning algorithms (*AdaboostM1, C4.5, Random Forest tree, MLP, RBF and SVM with Polykernel*) are applied for this purpose. This realization shows that the tree-type machine learning method is effective for traffic classification and identification, and the Internet traffic classification performs 99.76.16% accuracy.

Decision unit

Decisions–the decisions made regarding the processing of information security, in most cases, are based on the experience and previous decisions and adapt them to the new situation. Taking this into account, expert systems should be used in order to reduce the human factor and to improve the efficiency of the response. The architecture we propose uses the theory of precedents(Case-Based Reasoning, CBR)for managing this process.

The essence of the *CBR* methodology consists of the followings: In fact, the precedent is a <problem, solution method>pair. Over time, the occurred situations and their solutions are stored in the special database– precedents'base. When a new situation occurs, the similar one is searched and found in the database, and its solution is method is adapted to the reviewed situation. *CBR* methodology is used in diagnostics, forecasting, planning and projecting in many different subject fields, and in solving many classification problems. [13] explores various aspects of *CBR* information security and applies them in the risk assessment, intrusion detection, analysis of the network security situation.

Precedents database–solutions of the pre-identified incidents and for which appropriate measures are stored in the database. In other words, the precedents database is placed in the center as the ready solutions storage. If a new problem occurs, it is registered in the database with the signs vector function, which also provides a search for the problems in the precedents database. Obviously, the higher the level of the function similarity, the higher is the effectiveness of the search for precedents.

Decision maker or a group –when appropriate precedent is not found in the precedents' database the decision are made by the pre-defined experts.

Decision support system transfers the decision made in both cases –when the appropriate precedent is found and not found, to the processes to neutralize the threat, as well as to related persons in the form of report. After defining new incidents and their solutions, these solutions are transferred by the related persons entitled to make the final decision to the ready-made solutions' base.

Macro-architecture of the conceptual model

The coverage of the architecture of the above-mentioned conceptual model of the intelligent monitoring of network security is within a local network. Therefore, itis capable to control the processes that take place within a local network and to generate appropriate decisions. Taking into account the existence of different networks under a corporate network, we can appreciate the importance of the occurred incident or in general, the exchange of the Internetwork monitoring data about the situation from the information security point of view. Based on the foregoing, it is necessary to build the macro architecture of the conceptual model of the intelligent monitoring of hierarchical structured network security.

Figure 3 shows the hierarchical macro-architecture of the conceptual model and its two levels: corporate and local. The proposed conceptual model is applied separately for each level and its segments. Each block located in the local level represents a separate corporate network, and being in various sizes, they can locate in different regions and time zones. Notwithstanding the foregoing, each block and should separately be provided with autonomous mode and the ability to exchange information and should be integrated into the entire infrastructure. In other words, though, the blocks are separately an integral part of the local structure, each block should share

current information about itself and abnormality by actively exchanging information with the blocks, which have own analogues in the conceptual architecture.

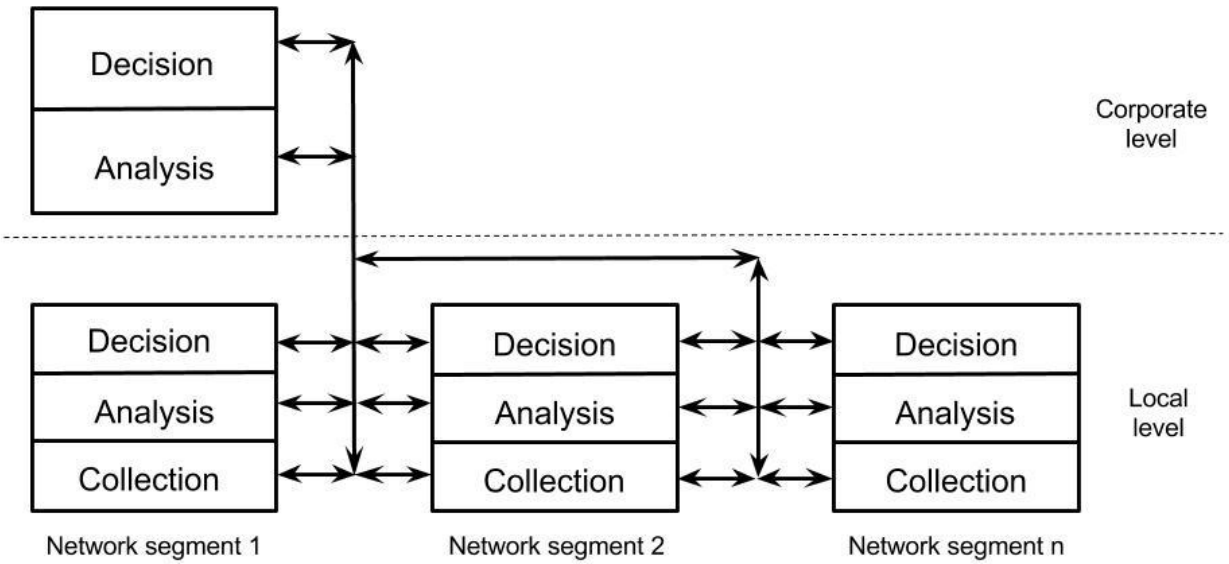

Figure 3. Conceptual macro-architecture of the intelligent monitoring of the network security

As can be seen from the Figure 3, the global level block does not have collection function. The main duties of the block is to monitor the performance of low-level blocks, and in special cases, to respond to incidents, which can not be processed by the blocks located in the local level, and to generation solutions.

Conclusion

This article proposed the conceptual model of the intelligent monitoring of the network security, which covers all the elements of the corporate network, users, technologies, and data and provides the detection of information security events. The main goal is to response to the incident, which may occur in any part of the network immediately and entirely, by covering entire corporate network and its subnets in real-time. The relevance is the ability to realize the processes of detection, processing and decision-making of the commercial products controlling the network security issues.

References

1. Alguliyev R.M., Imamverdiyev Y.N., Nabiyev B.R. // The analysis of the methods for information technology network security monitoring, 2014, No 1, pp. 60-68.
2. Fung C.J., Boutaba R. Design and management of collaborative intrusion detection networks / International Symposium on Integrated Network Management, 2013, pp. 955-961.
3. Yegneswaran V., Barford P., Jha S. Global Intrusion Detection in the DOMINO Overlay System / Proc.of the Network and Distributed System Security Symposium, 2004, pp.1-17.
4. Fataliyev Z., Imamverdiyev Y.N. Security Operation Center Architecture for E-government based on Big Data Analysis / Republican scientific-practical conference on the problems of building e-government. Baku, 2014. pp. 140-144.
5. Hofstede R., Celeda P., Trammell B., Drago I., Sadre R., Sperotto A., Pras A. Flow Monitoring Explained: From Packet Capture to Data Analysis with NetFlow and IPFIX // IEEE Communications Surveys & Tutorials, 2014, vol. 16, pp. 2037-2064.

6. Deri L., Lorenzetti V., Mortimer S., Collection and Exploration of Large Data Monitoring Sets Using Bitmap Databases / Second International Workshop Traffic Monitoring and Analysis, 2010, pp 73-86.
7. Giura P., Memon N., NetStore: An Efficient Storage Infrastructure for Network Forensics and Monitoring /Proc.of the International Symposium on Recent Advances in Intrusion Detection, 2010, pp. 277-296.
8. Lee Y., KangW., Son H., An Internet Traffic Analysis Method with MapReduce // Proc. of the IEEE/IFIP Network Operations and Management Symposium Workshops (NOMS Wksps), 2010, pp. 357 – 361.
9. Imamverdiyev Y.N., Nabiyev B.R. Multi-classifier model for the network traffic // Problems of Information Technology, 2014, No 2, pp. 60-68.
10. Nabiyev B.R. Method for the network traffic clustering / Second Republic scientific-practical conference on the multidisciplinary issues of information security dedicated to the 150th anniversary of the International Telecommunication Union, Baku, 2015, pp. 213-215.
11. Jaiswal R. C., Lokhande S. D. Machine learning based internet traffic recognition with statistical approach /Proc.of the Annual IEEE India Conference, 2013, pp. 1-16.
12. Imamverdiyev YN., Nabiyev B.R. Precedents theory-based of decision-making method for the network security monitoring // Problems of Information Technology, 2012, No 2, pp. 53-58.