Proceedings of TEAM 2015

7th International Scientific and Expert Conference
of the International TEAM Society

15–16th October 2015,
Belgrade, Serbia

Organizers of TEAM 2015 Conference:

- Faculty of Mechanical Engineering, University of Belgrade, Serbia
- Innovation Center of the Faculty of Mechanical Engineering, I.I.d. Belgrade, Serbia
- Structural integrity and Life Society “Prof. Dr Stojan Sedmak”
- International TEAM Society

The conference is organized under the auspices of the International TEAM Society:

Founder Institutions:

- College of Slavonski Brod, Croatia
- Mechanical Engineering Faculty in Slavonski Brod, University Josip Juraj Strossmayer in Osijek, Slavonski Brod, Croatia
- College of Mechanical Engineering and Automation, Kecskemét College, Kecskemét, Hungary

Member Institutions:

- Faculty of Materials Science and Technology in Trnava, Slovak University of Technology, Slovakia
- Faculty of Manufacturing Technologies with seat in Prešov, Technical University of Košice, Slovakia
- Faculty of Agriculture, University Josip Juraj Strossmayer in Osijek, Croatia
- Faculty of Mechanical Engineering, University of Belgrade, Serbia

Proceedings of TEAM 2015

7th International Scientific and Expert Conference of the International TEAM Society

15–16th October 2015,
Belgrade, Serbia

Publisher: Faculty of Mechanical Engineering, University of Belgrade

Editor in Chief: Prof. Aleksandar Sedmak

Editors: Zoran Radakovic, Simon Sedmak, Snezana Kirin

ISBN **978 – 86 -7083 – 877 – 2**

Circulation: 200 copies

Copied by Faculty of Technology and Metallurgy, Research and Development Centre of Printing Tehnology, Karnegijeva 4, Belgrade, Serbia

All papers are reviewed

The authors are only responsible for the accuracy and contents of all published material.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

62(082)(0.034.2)

INTERNATIONAL TEAM Society. International Scientific and Expert Conference (7 ; 2015 ; Beograd)
Proceedings of TEAM 2015 [Elektronski izvor] / 7th International
Scientific and Expert Conference of the International TEAM Society, 15/16th October 2015, Belgrade, Serbia ; [Editor in Chief Aleksandar Sedmak]. - Belgrade : Faculty of Mechanical Engineering, 2015 (Belgrade : Faculty of Technology and Metallurgy, Research and Development Centre of Printing Technology). - 1 elektronski optički disk (CD-ROM) ; 12 cm

Sistemski zahtevi: Nisu navedeni. - Nasl. sa naslovne strane dokumenta. - Tiraž 200. - Bibliografija uz svaki rad.

ISBN 978-86-7083-877-2

a) Техника - Зборници
COBISS.SR-ID 218229516

Scientific Reviewing Committee

SEDMAK, Aleksandar, University of Belgrade, RS, chairman
AILER, Piroska, Kecskemét College, HU
BÉRES Gábor, Kecskemét College, HU
CHATTOPADHYAYA, Somnath, Indian School of Mines, Dhanbad, IN
CRISTEA Anişoara-Gabriela, University in Galaţi, RO
JOHANYÁK, Zsolt Csaba, Kecskemét College, HU
KOLEDA, Peter, Technical University in Zvolen, SK
KOZAK, Dražan, MEFSB - University of Osijek, HR
KIRIN, Snežana, University of Belgrade, Serbia
LÍSKA, János, Kecskemét College, HU
MARKOVIĆ, Monika, Faculty of agriculture, University of Osijek, HR
MIROSAVLJEVIĆ, Krunoslav, VUSB Slavonski Brod, HR
MONKA, Peter, FVT TUKE, SK
MONKOVÁ, Katarína, FVT TUKE, SK
PALADE Florentina, University in Gala□i, RO
RAOS, Pero, MEFSB - University of Osijek, HR
ŠIMUNOVIĆ, Katica, MEFSB - University of Osijek, HR
ŠUGÁR, Peter, FMST in Trnava, SK
SURZENKOV, Andrei, Tallinn University of Technology, EE
ŽIVIĆ, Marija, MEFSB - University of Osijek, HR

Organizing Committee

Aleksandar Sedmak, (chairman)
Miloš Milošević, (co-chairman)
Nenad Mitrović
Snežana Kirin
Branislav Đorđević
Dragana Perović
Igor Svetel
Simon Sedmak
Miloš Đukić
Gordana Bakić
Uroš Tatić
Zorana Golubović
Dražan Kozak
Sergej Hloch
Ivan Samardžić
Antun Stoić
Josip Jukić
Krunoslav Mirosavljević
Piroska Ailer
Lóránt Kovács
Jozef Peterka
Milan Maronek
Jozef Zajac
Vladimír Modrák
Vlado Guberac
Sonja Marić
Milorad Milovančević
Branko Burgarski
Marko Rakin
Katarina Čolić
Goran Sofronić

CONTENT

SURVEY ON INTRUSION DETECTION SYSTEMS

László Göcs[1*], Zsolt Csaba Johanyák[1]

[1]Kecskemét College, Faculty of Mechanical Engineering and Automation, Hungary, H-6000 Kecskemét,
gocs.laszlo@gamf.kefo.hu

Abstract

Intrusion detection systems (IDSs) play an important role in the defense of the companies' IT systems. These systems provide automated protection against a variety of attacks and intrusions. Without them in several cases system administrators are not able to recognize in time high degree attacks and thus effective defense and intervention actions cannot be taken. IDSs use sensors to detect potential attacks and they either inform system administrators or intervene automatically when an attack signature is recognized. In this paper, we do a survey on the main families of IDSs presenting their classification and the advantages and disadvantages of the different approaches.

Keywords: IT security, IDS systems, corporate security, intrusion detection system, data security

1. Introduction

Intrusion-detection systems analyze network traffic and software behavior looking for special events and traces, which could be signs of malicious activities or attacks. When comparing them to firewalls one can state that while a firewall is blocking unconditionally the traffic that is considered unnecessary and is enabling traffic types considered as safe, the task of IDS is to recognize attack traces and in some cases to effectuate counter-actions as well [1].

An IDS consists of the following elements (Fig. 1):

- *Sensors*: monitor and record activities that are processed by the IDS;
- *Analytical Engine*: analyzes the collected data and compares it to the known malicious activity patterns stored in the database;
- *Signature Database*: the collection of known and suspected harmful activities.
- *Report Generator*: alarms system administrators and logs IDS activity [2].

Practice unambiguously shows that creating an automated environment is indispensable for a corporate IT system, where there are many workstations and the communication is multidirectional.

Without its support the administrators would not be able to monitor intrusions and their consequences. The main goal of this paper is to give a comprehensive picture of the IDS families, their key ideas, their advantages and disadvantages.

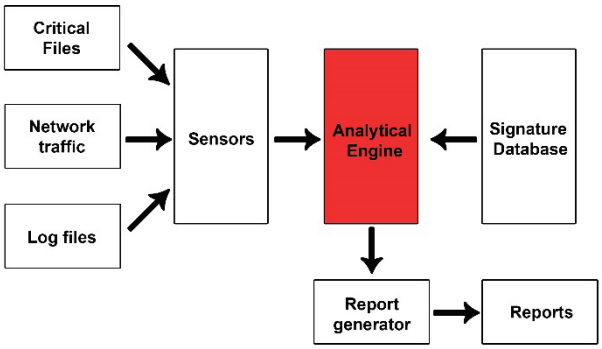

Figure 1. IDS System

2. IDS Categorization

Intrusion detection systems can be categorized in several ways. In this paper, six main aspects are used based on [10] for the definition of main IDS classes (see Fig. 2). They are the applied intrusion detection approach, the type of the protected system, the structure of the IDS, the source of the data used for the analysis, the level of the services offered after the recognition of an attack, as well as the timing of the analysis.

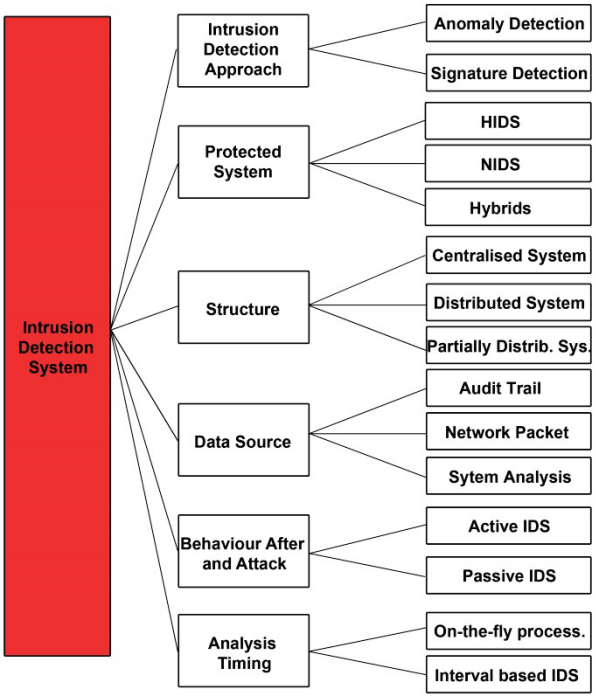

Figure 2. Types of IDS systems [10]

The first aspect we take into consideration for the categorization of IDSs is the applied intrusion detection approach. Conform to it one can identify anomaly detection and signature detection based IDSs [9].

Anomaly detection based IDSs (also called Behavior based IDSs - BIDSs) work on statistical basis. They learn the normal behaviors of both the system and the users. Based on the acquired knowledge they determine whether the analyzed activity is harmful to the system or not. BIDS create statistics for the logon time, the time a user was logged in, the usually accessed files, as well as for the frequency of the modification and movement of these files.

The advantage of the anomaly based approach is its fast and dynamic adaptation capability to unknown attack types. The disadvantage of BIDS is that it alerts the administrator and takes counter measures more often than knowledge-based IDSs due to their high rate of false alarms [9]. Additionally, a BIDS is less efficient in case of systems whose behavior pattern is not static enough for the creation of statistics or in case of systems where user activity is not monotonous, [4]. One has to take extra precautions in course of the learning period to avoid the possibility of “learning” an actual intrusion as a normal behavior.

Signature based IDSs use a database with samples of previous attacks. They are also called Knowledge-based IDSs (KIDS) or misuse detection based IDSs (MIDS). Based on the stored patterns the IDS decides whether the observed activity is a potential attack attempt or not. It is currently the most widely used IDS model. Its advantage is that owing to the stored samples significantly less traffic is blacklisted than in case of BIDS as well as its alarm signals are standardized and easily interpreted by administrators. The disadvantage of KIDSs is that its database requires constant updates and maintenance, as well as it does not recognize new attack types [3], [9]. Thus it may allow access to the system for a new, previously unknown attack types (high rate of false negative decisions) [9]. Moreover, a KIDS could put a new attack type on the white list of activities.

Based on the subject of the protection one can distinguish three kinds of IDSs, the host-based, the network based, and the hybrid systems [2], [7].

The HIDS [19] is used to monitor a stand-alone computer. It has to be installed to and configured for the protected system. A HIDS also requires small testing mechanisms built into it that collect the necessary information for the intrusion attempt recognition from the monitored system's log files. It is able to indicate and prevent threats and physical attacks to the system.

The NIDS usually includes a network monitoring tool, which is supported by a network interface card. This type of IDS is located in a segment of the network or at its borders and examines network traffic. It is able to observe and protect against attacks one or more systems and devices in the network.

Recently it has become a new trend to combine two types of IDSs, the host-based and network-based ones. It is called hybrid intrusion detection system (HYDS). It is more flexible than previous solutions and it increases the level of security. HYDSs combine IDS sensors, reports, and counterattacks to protect a segment or the entire network [4].

3. Structure

Big companies often face the problem it is hard to establish a proper IDS. The biggest challenge is that the individual detection systems can be situated geographically spread at far distances. First, one has to decide about the type of the connection between them and the hierarchical structure to be built. Next, the information and command flow has to be defined, and the final question is whether the IDS infrastructure is controlled centralized, distributed, or a combined approach is chosen.

The structure of an intrusion detection system can also be used as a distinctive characteristic of the categorization. Based on it conform to the above described aspects one can identify centralized, distributed, and partially distributed IDSs.

The IDSs usually utilize agent applications that are installed on some nodes of the computer network. These nodes are called monitor nodes. A monitor node examines the network traffic. It can listen in two modes, i.e. normal and promiscuous. In normal listening mode, the monitor node interprets and forwards data packages that were sent to a given internal subnet after processing (evaluating) them. In promiscuous listening mode, the monitor node examines all messages independently from their destination.

Centralized IDSs (CIDSs) have a central software on a server of the network, which application is responsible for the analysis, detection, classification, and action [5].

The advantage of the centralized approach is the reduced cost compared to the case of a distributed system. Besides, the maintenance and administration costs are also lower. Furthermore, the whole network architecture becomes more simplified and thus the number of vulnerabilities in the security infrastructure of the organization is also reduced. In addition, the managers of CIDSs being able to monitor and evaluate the systems and the networks of the company as a whole unit can easier identify a large scale attack [11].

A Distributed IDS (DIDS) contains several intrusion detection systems. They form a network and communicate with each other or with a central server. This solution has several advantages compared to the centralized one.

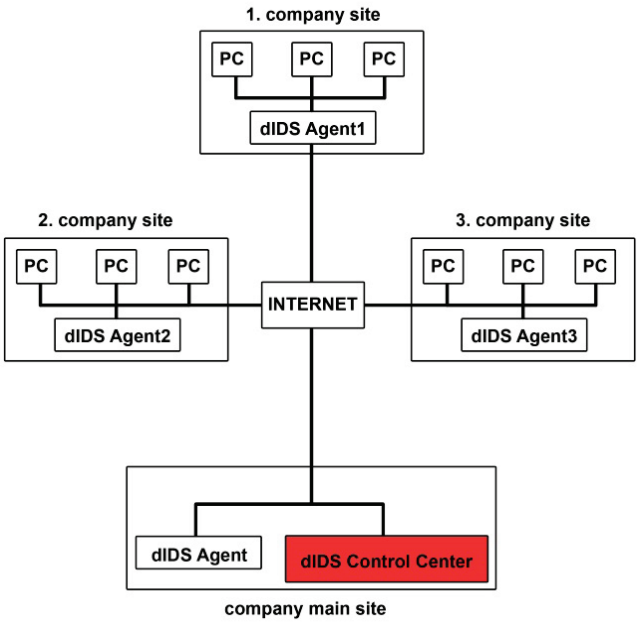

Figure 3. Distributed IDS structure [16]

Firstly, the monitoring, analysis, and processing of attack data is easier. Moreover, a DIDS is able to recognize attack signatures on the whole network of the company where individual segments can be situated geographically far from each other or even in different time zones. DIDS make possible an early intrusion detection that can result in blocking incoming traffic into the whole network from specific IP addresses.

In addition, if a worm gets into the company's network a DIDS can successfully prevent its further propagation. Furthermore, if a threat is identified in one segment it will not be necessary its further analysis on other segments. A DIDS can easily recognize and trace back an internal attack as well using the data logged by DHCP and RADIUS servers [16].

In order to avoid the complexity of using an additional specialized routing protocol (required for a centralized IDS) and limit the overall energy consumption of sensor nodes distributed IDSs consist of agents being able to do the job partially or fully on their own [5].

The partially distributed IDSs combine the centralized and distributed control strategies. The local agents – characteristic to distributed systems – identify locally the hostile activity and take counter actions. Besides, they also send a report to the center. The advantage of the combined approach is that is makes possible the recognition of a coordinated attack that happens at several entry points of the company network at the same time.

Data analysis plays an important role in the protection of IT systems. The data can come from various sources like audit logs, network traffic sniffing, or system analysis. Thus based on the origination of the data they are working with one can define three groups of IDSs being presented in the following subsections.

Audit trails contain information about system activity both by system and application processes as well as data about user activity related to systems and applications. Based on audit trails known intrusion attempts are modelled as sequences of user behavior. These behaviors are then modelled as events in an audit trail. The IDS is responsible for determining how identified user behavior is manifested in an audit trail [6].

A firewall typically does not examine the entire packet and not permitted packet types are simply dropped. Unfortunately this approach cannot stop all malicious packets from getting into the protected system.

An IDS can do a deep examination of packets from the network traffic, and based on the results can permit or prohibit their pass, all of this doing in real-time. Thus all suspicious events/packets are immediately blocked. Therefore the advantage of a network packet based IDS is that owing to the check of the whole package one can block even new attacks against which the original configuration of the firewall would not be able to give protection. Thus network packet based IDS is able to stop attacks that cannot be stopped by the firewall.

A system attack can influence the functioning of the system by deploying malicious software. Therefore the presence of non-desired processes/tasks can also be a sign of hostile activities and thus provide information for IDSs. The limits of this approach are given by the fact that advanced malicious programs are developed to work hidden in the background being difficult to recognize.

Intrusion detection systems also can be categorized based on their behavior after an attack. There are two basic approaches. After recognizing the hostile activity the IDS either creates only a report/alert (passive) or it blocks the attack (active) in order to prevent further malicious activities.

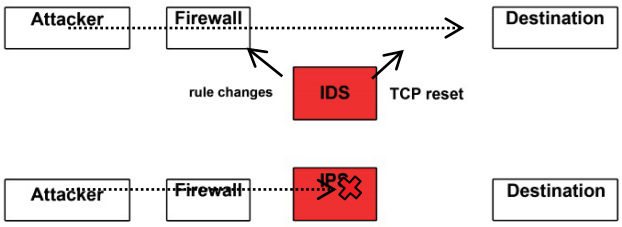

Figure 4. IDS and IPS operation

An active IDS is an intrusion prevention system (IPS). It works without need for human intervention by automatically blocking suspicious system access attempts. The IPS should be placed at the network boundary. However, owing to its position the IPS itself could become vulnerable to attacks. Furthermore, it could even happen that the activities of the IPS are identified as unauthorized access. Its disadvantage is that without proper configuration an IPS often disables users and applications that otherwise would be authorized to use the system.

A passive IDS does not take preventive actions. It runs background scans and in case of potential attacks or suspicious behaviors it alerts the system administrator. The advantage of this approach is that as a passive observer in the network, it does not become the target of attacks, and there is no risk of identifying its own activities as an attack. The disadvantage is that by the time the administrator receives the notice, analyzes it and decides on the proper response, most likely the attack had taken place and the damage is done.

Intrusion detection systems can work continuously while others must be run periodically [18].

Most of the IT systems work continuously around the clock. They need real time protection in order to ensure maximum uptime. Most of the IDSs belonging to this category are based on network traffic analysis. Usually the header of the transport layer packets is monitored, which can include the IP addresses, TCP/IP flags, etc. Another approach analyzes the application layer communication (FTP, HTTP, etc.). Here an important aspect is whether the content of the packets is conform to the protocol.

The advantage of the on-the-fly processing based IDSs is that they can offer a continuous protection and a higher level of availability of the IT system compared to the interval based ones. Their drawback is that they can require huge computational capacity and working memory. Sometimes the applied algorithms are not fast and efficient enough which can result in packet losses.

Interval based IDSs are not working continuously, they are run periodically when a prescribed amount of time is elapsed. There are IT systems that operate only in certain time intervals periodically. They do not need to be monitored and protected continuously. In their case a periodically activated interval based IDSs can provide a proper protection. The advantage of the interval based approach could be that the computational load generated by the IDS is less than in the case of the on-the-fly approach. However, the IDSs belonging to this category can offer only a reduced protection for continuously operating IT systems.

4. Conclusions

IT systems have become part of each section of the everyday life of a company. Their security and availability is a priority for all concerned personnel. Although most likely it is not possible to ensure a full protection but there are several tools that can contribute to the enhanced security when they are properly configured and tuned.

Intrusion detection systems play an important role in the defending mechanism of each professional IT system. They appeared in the late 80s and their evolution continuously followed the growth of IT systems. This paper gives a comprehensive review of the categories of intrusion detection systems showing their advantages and drawbacks as well.

There is no overall optimal solution, one should carefully examine the actual situation, infrastructure available computational power and of course the cost factor which was only implicitly included in this survey.

5. Acknowledgement

The Project is supported by the Hungarian Government and co-financed by the European Social Fund.

6. References

[1] MTA SZTAKI: Az informatika ihálózat iinfrastruktúra biztonságikockázataiés kontrolljai, Budapest 2006, p. 265.

[2] KiranDhangar, Deepak Kulhare, Arif Khan: A Proposed Intrusion Detection System, International Journal of Computer Applications (0975 – 8887), Volume 65– No.23, March 2013

[3] John McHugh, Alan Christie, and Julia Allen: The Role of Intrusion Detection Systems, IEEE SOFTWARE September/October 2000,

[4] Christopher Krügel, Thomas Toth, EnginKirda: Service Specific Anomaly Detection for Network Intrusion Detection, SAC '02 Proceedings of the 2002 ACM symposium on Applied computing ACM New York, NY, USA,2002 pp. 201-208.

[5] A.H. Farooqi and F.A. Khan: Intrusion Detection Systems for Wireless Sensor Networks: A Survey, D. Ślęzak et al. (Eds.): FGCN/ACN 2009, CCIS 56, pp. 234–241, 2009.

[6] E. Biermann, E.Cloete, L.M. Venter: A comparison of Intrusion Detection systems, Computers & Security, 20 (2001) 676-683

[7] Marina Bykova, Shawn Ostermann, Brett Tjaden: Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics, CERIAS Tech Report 2001-75

[8] V. Jaiganesh, S. Mangayarkarasi, Dr. P. Sumathi: Intrusion Detection Systems: A Survey and Analysis of Classification Techniques,International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 4, April 2013

[9] LiberiosVokorokos, Anton BALÁŽ, Martin Chovanec: Intrusion Detection System Usig Self Organizing Map, ActaElectrotechnica et Informatica No. 1, Vol. 6, 2006

[10] Qutaiba Ibrahim and SaharLazim: Applying an Efficient Searching Algorithm for Intrusion Detection on Ubicom Network Processor, International Arab Journal of e-Technology, Vol. 2, No. 2, June 2011

[11] D.Y. Yeung, Y. Ding: Host-based intrusion detection using dynamic and static behavioral models, Pattern Recognition, 36 (2003), pp. 229-243.