Ph.D. Pavlov I. (MITI SUT)
Nischenko V. (MITI SUT)
Tereshenko V. (MITI SUT)

THE TAXONOMY OF MAJOR CONTEMPORARY APPROACHES IN INTRUSION DETECTION SYSTEMS

Павлов І.М., Ніщенко В.І., Терещенко В.І. Аналіз таксономії систем виявлення атак в контексті сучасного рівня розвитку інформаційних систем. *Проаналізовані різні погляди на таксономію систем виявлення атак систем захисту інформації і представлена нова класифікація систем виявлення атак, у якій таксономічні ознаки підібрані таким чином, щоб максимально збільшити кількість характеристик для опису цих систем захисту інформації у відповідності з сучасними умовами розвитку інформаційних технологій.*

Павлов И.Н., Нищенко В.И., Терещенко В.И. Анализ таксономии систем обнаружения атак в контексте современного уровня развития информационных систем. *Проанализированы различные взгляды на таксономию систем обнаружения атак систем защиты информации и представлена новая классификация систем обнаружения атак, в которой таксономические признаки подобраны таким образом, чтобы максимально увеличить количество характеристик для описания данных систем для дальнейшего проектирования систем защиты информации в соответствии с современными условиями развития информационных технологий.*

The article analyzes different views on IDS taxonomy and presents new intrusion detection system classification, which taxonomy features are selected in order to maximize the number of characteristics that help to describe systems data for further design of information protection systems according to the current level of information systems development.

Key words: *Intrusion detection systems, taxonomy, feature, information security, attack, anomaly.*

Formulation of a problem.

Nowadays during the rapid development of network technologies and global IT development of the society, problems of providing high level of information systems protection take the first place. With an increasing number of computer incidents connected with security, the intrusion detection systems (IDS) are being developed rapidly. (IDS) is one of the most important decisions to protect systems and networks.

Traditionally IDS are classified according to two characteristics: the method of detection and system level that provides protection. And despite the fact that these two classification features are the most important while choosing intrusion detection system, there are other characteristics that also play an important role in designing IDS, whereas the safest solution can not be achieved while considering one or two aspects of taxonomy. All developers of intrusion detection systems and organizations that use IDS must understand and consider their classification to select the best solutions for information protection systems. During the study of various aspects of taxonomy and application of different options we can achieve higher level of information systems security.

In this regard, the authors systematized classification features of intrusion detection systems and developed classification of systems data that fully complies with all the current trends of communication networks development and challenges to the protection of information systems in general.

Analysis of recent researches and publications enables us to make conclusion that most of the existing classifications of IDS are very abstract, are not complete, and a great amount of important characteristics (elements) require additions and generalizations.

Considering the classification in the research [1] which is considered to be one of the first attempts to make classification of IDS, it is clear that the authors include security monitoring aspects such as vulnerability assessment. They classify IDS by five criteria: detection method, behaviour during identification, source of audit, detection paradigm and usage frequency. One year later, the authors of [2] added several new key classification features. However, in the course of time, [3] the authors show in their classification that IDS can run as a standalone centralized application or integrated application that creates a distributed system. But the most complete

classification according to the taxonomic characteristics is presented in [4] where the authors extend all efforts of their predecessors and include twelve classifications in the taxonomy, but not all of them can be accepted, some require full modernization and significant additions in accordance with today's realities.

In such a way the authors set a target to systematize classification features and provide current view of intrusion detection systems taxonomy.

The main part.

This article is modern opinion of IDS taxonomy with the short determination and explanation of each feature in systematization. To make this classification comprehensive and complete besides the usual features, such as monitoring environment, detection method, architecture, response type, the principle of work and time of reaction also were included the following characteristics: a source of audit, construction technology, detection paradigm and mode of data collection (Figure 1.).

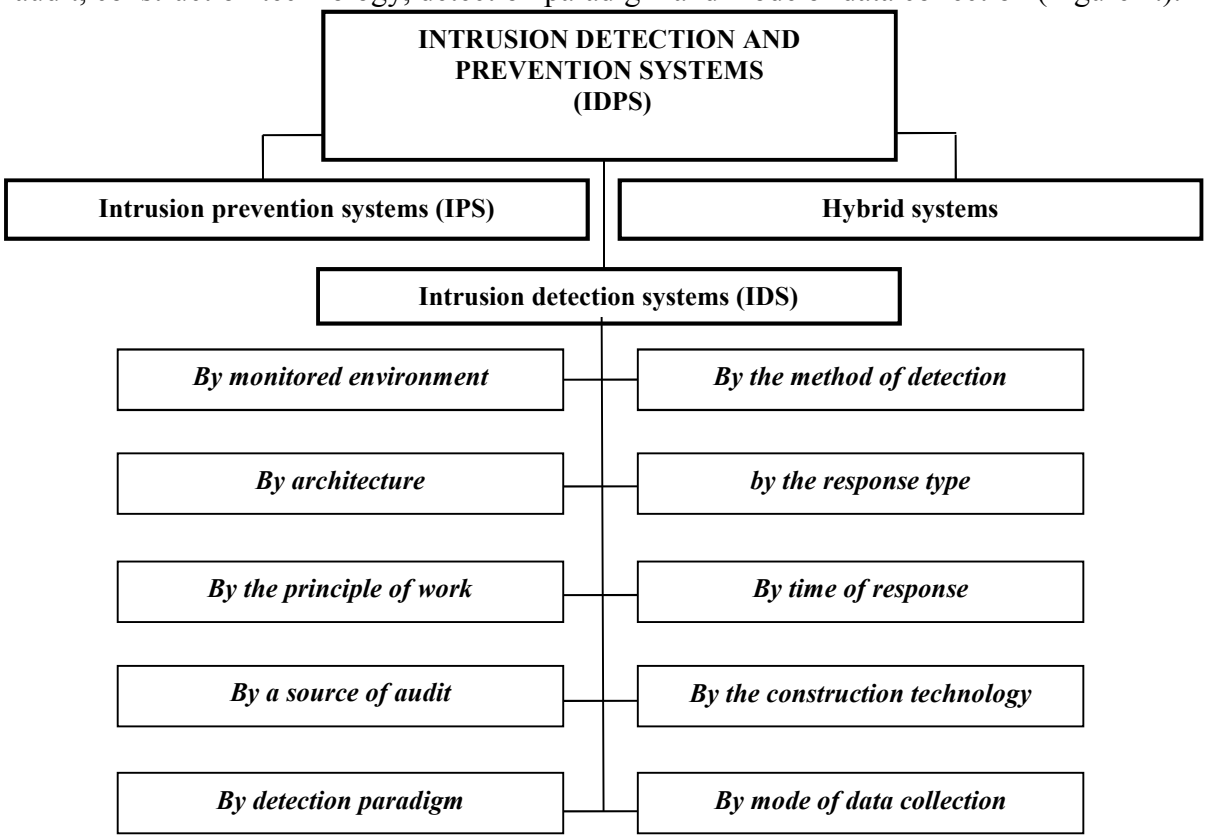

Figure 1. Classification features of the intrusion detection system taxonomy

The first classification feature of intrusion detection system is the classification **according to the monitoring environment**, depending on the source of information collecting: the network, particular computer or some applications running on the computer.

Most classifications presented in [1], [2], [3] divide IDS by this feature into two types: network-based IDS and host-based IDS. But nowadays , the presence of one type reduces its effectiveness because of absence of another one, that's why the development of hybrid and combined systems that operate successfully at both network-based and host-based systems, becomes very popular. The increase of the range of additional services and the emergence of such determination as an application created the necessity to monitor security at the application level. It is expedient to classify intrusion detection systems by monitoring environment into: network-based, host-based, hybrid (combined) and application based.

The second feature of IDS classification is the division **by method of threats detection**. Method of detection is also present in other classifications, as detection technique, principle or approach. However, regardless of feature determination, historically IDSs are divided into Signature

Based IDSs and Anomaly Based IDSs. Almost all scientists, who work with IDS classification, have the same point of view. But some differences appear when principles of the Anomaly Based IDSs are presented together with others, but it is incorrect. In turn, the most accurate IDS classification based on anomaly detection methods was presented in [6].

Today, anomaly detection methods are priority methods during IDS development. The most popular among them are four subgroups: statistical anomaly detection, data mining based detection, knowledge based detection, machine learning based detection.

Also, hybrid methods are absent in most classifications, but they are actively investigated nowadays and represent a synthesis of signature based IDS and anomaly based IDS.

Another classification criteria is the division **by architecture**.

There are host systems (with active software) and target systems (observed by others) depending on IDS architecture.

Earlier IDSs were active on the very same protected systems but with the appearance of workstations and personal computers the most IDS architectures provide IDS on the separate system, that is why there are host and target systems. This improves IDS functioning security

IDS are divided into active and passive **by the response type**.IDS can respond the intrusion actively or passively. Passive measures mostly mean IDS report, made for people whose further activity can be based on this report.

When IDS respond the intrusion actively, it can additionally change the condition of attacked object, it means the automatic intervention in some other system (eg. control switch, or firewall).

Another feature of IDSs classification is division **by the principle of work** into static and dynamic. Not each modern IDS classification has similar classification feature, the reason is that the most of scientists believe that static IDSs are obsolete. However, there are information systems that do not include a lot of important information and are not constantly attacked by intruders, that is why they do not require complicated mechanisms if dynamic IDSs realization.

Static systems make "snapshots», (snapshot) environment and provide their analysis, looking for vulnerable software, misconfigurations, check the versions of applications as for the presence of known vulnerabilities and weak passwords, check the content of special files in the user directory or check the configuration of open network services.

Dynamic IDSs monitor all the actions taking place in the system in real time, reviewing audit files or network packets transmitted over time. Dynamic IDSs implement analysis of in real time and allow constant monitoring of the security system.

Another feature of IDSs classification is division **by time of response**. Many early IDSs were packet type, it means that they were completely dependent on the accumulation of audit records in the operating system. IDSs of the Batch mode do not perform any action in response to the detected attack. This type was observed as only possible in [1], but a year later the real time IDSs were added in [2].

The real time IDSs process the continuous flow of information at once. Detection of attacks carried out by real time IDS leads to results very quickly, and it allows IDSs to perform certain responsive actions automatically.

It is also advisable to classify intrusion detection systems **by source of audit**. IDSs detect intrusion by analyzing data collected after usage of various audit types. The collected data represent a system, applications and network behavior. Successful intrusion detection depends on the completeness of data collected from sources of audit, speed of data acquisition and data processing.

Data from the hot log files of computer systems carry information about the user activity on a given machine. In case of successful attacks, they are vulnerable to changes, that is why they are topical only until the time of attack.

The analysis of network packets is popular for collecting information about the events coming from the network. Application level gateways or filtering routers can serve as interceptors. Packages analysis can be done quickly if it is held at a low level, for example, after the comparison with the model or after using a signature analysis.

Using of IDS sensors is a characteristic feature of a new generation of intrusion detection systems that detect attacks not directly, but are able to correlate information gathered from multiple intrusion detection tools (scanners). This method saves and reduces the number of events that must be processed. It is also beneficial when activity covers multiple users, computers or networks.

Data from application logs is good source of information, as they are more accurate and more complete, because the file contains all the necessary information and does not require re-assembly unlike the data from network packets.

IDSs that use system state analysis modulate the attack as a series of state transitions, starting from the initial state of security and ending with the state of security threat. These systems use diagrams to model critical events that must occur for successful penetration into the system.

Another important feature of IDS classification is distribution **by the construction technology**.

During the deployment of IDS, it is important to know that the technologies are used during the construction of information system. Wired networks in comparison with wireless use different and specific methods of safe transfer, such as encryption. That is why; the physical network of data transfer plays an important role in the design of IDSs.

It is known that the first classifications did not have this feature, it originated only with the appearance of wireless technologies, and the current tendency of rapid development and modernization of wireless technologies, requires increased attention to the taxonomy of wireless methods of information transmission.

The leading networks are generally faster and cheaper than wireless. Some of the networking functions, such as traffic behavior and network topology can be used for intrusion detection in leading communication networks.

Stationary wireless networks are situated in fixed locations. One of the advantages of using fixed wireless networks is the ability to connect with users in remote areas with no need to lay new cables. Mobile wireless networks form a collection of mobile nodes that are self-configured automatically without the help of a fixed infrastructure or centralized management. They are: hierarchical, mobile agents, autonomous also cooperative and separated.

Hierarchical IDSs are designed for multi-layer network infrastructures where the network is divided into clusters.

Mobile agent has the ability to move through a large network is designed to perform only one specific task, and applies online. Various agents are designed for different functions, this reduces energy consumption. If the network is damaged or some agents are destroyed, other agents can still work. Mobile agents are independent on the platform architecture.

Stand alone IDSs are installed on each host (node) independently. They base their decisions only on the information gathered on its own host, collaboration between nodes in the network is impossible. Hosts do not share information and do not aware of the security status of neighboring nodes.

Distributed and cooperative IDSs involve in their work all network nodes. It means that each node participates in intrusion detection, which is provided by usage of IDS agents. IDS agent discovers and collects information of local events and data to identify potential attacks.

According to the **detection paradigm** IDSs are divided into those that assess the condition and those that appreciate the transitions between states.

Detection paradigm describes IDS estimation of invasion and can be of two types. The first type assesses the state to know whether it is safe or vulnerable. The second type evaluates transition between states, namely the movement from secure state to unprotected one.

Assessment of state like the rating of transitions between states can be done in two ways:

• Without unbalancing of the system, means that the system performs monitoring and assesses vulnerability, requesting for necessary information, and comparing it with figures of known vulnerabilities.

• Proactive way means that the system performs an impact on the environment to determine the condition or make the transition. This method is actively used to determine the system state, because it is almost indistinguishable from real intrusions.

The last classification feature of intrusion detection systems is distribution **by mode of data collection**. Audit data can be collected in a distributed mode from several different locations or sources, or they can be collected centralized from a single source.

Thus, generalized classification of IDSs is presented on Figure 2.

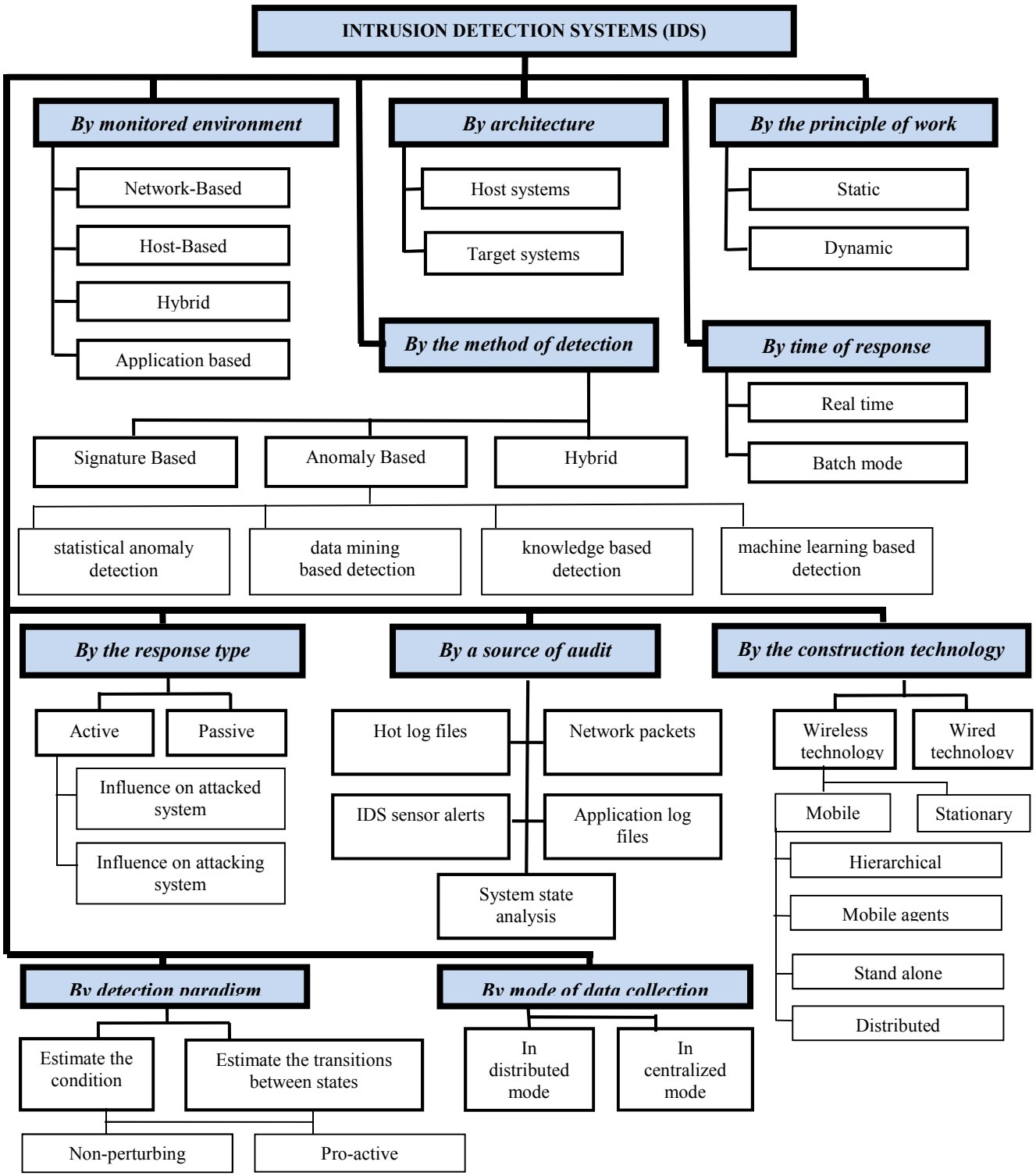

Figure 2. IDS classification in accordance with modern trends in information system

Conclusion. Most previous IDS classifications were very abstract, not completed, and they missed some important characteristics. The article developed IDS classification in which taxonomic features are selected in order to maximize the number of characteristics to describe IDS for further design of information security systems. Comprehensive classification allows organizations to have accurate information about IDS type, which should be used in accordance with established safety standards in organization and type of information system.

We believe that a complete set of classifications include: monitoring environment, method of detection, architecture, principle of work, reaction time, response type, audit source, construction technology, identification paradigm and data collection mode.

The presented classification can serve as a basis not only for establishment of protection system, but also to adapt organizations in accordance with IDS, it also meets their needs. For example, when the organization's budget is limited, this classification can help to identify the highest priority components which in complex decision will result a higher level of information security in modern information systems.

REFERENCES

1. Debar, H., Dacier, M., and Wespi, A. (1999), „Towards a Taxonomy of Intrusion Detection Systems," Computer Networks, vol. 31, 1999, pp. 805 – 22.

2. Debar, H., Dacier, M., and Wespi, A. (2000), „A Revised Taxonomy for Intrusion-Detection Systems," presented at Annales des Télécommunications, vol. 55, 2000, pp. 361 – 78.

3. Kabiri, P., and Ghorbani, A., A. (2005), „Research on Intrusion Detection and Response: A Survey", International Journal of Network Security, Vol.1, No.2, Sep. 2005, pp.84 – 102.

4. Amer, S.H., Hamilton, J.A., „Intrusion Detection Systems, (IDS) Taxonomy – A Short Review," DOD Software Tech News, vol. 13, no. 2, June 2010, DOD Data & Analysis Center for Software, Air Force Research Laboratory, Rome, N.Y., pp. 23 – 30.

5. Ali A. Ghorbani, Wei Lu, and Mahbod Tavallaee, Network Intrusion Detection and Prevention: concepts and techniques. London: Springer, 2010, p. 27 – 49.

6. Manasi G.; Rana; Yadav, „Taxonomy of Anomaly Based Intrusion Detection System: A Review" International Journal of Scientific and Research Publications, Vol. 2, Issue 12, Dec. 2012.

7. Бабенко Л.К. Разработка комплексной системы обнаружения атак / Л.К. Бабенко, О.Б. Макаревич, О.Ю. Пескова // Информационная безопасность: материалы V междунар. науч. – практ. конф. 2003. №4(33). С.235 – 239.

8. Остапенко А.Г., Иванкин М.П., Савенков Г.А. Обнаружение и нейтрализация вторжений в распределенных информационных системах: учеб. пособие. – Воронеж : ФГБОУ ВПО „Воронежский государственный технический университет", 2013.