Oleh HARASYMCHUK[1], Olha BLOSHCHENKO[2], Vasyl RAMSH[3]

Opiekun naukowy: Oleh HARASYMCHUK[1]

ANALYSIS OF PRINCIPLES AND SYSTEMS FOR DETECTING REMOTE ATTACKS THROUGH THE INTERNET

Summary: In the paper, we analyze modern technologies and functionality of intrusion detection systems. Moreover, there were considered the main types of tasks that such systems should solve. The classification of the intrusion detection systems on various grounds has been carried out.

Key words: network attack, information system, intrusion detection system, intrusion, anomalous behavior, signature, network.

ANALIZA ZASAD I SYSTEMÓW WYKRYWANIA ZDALNYCH ATAKÓW PRZEZ INTERNET

Streszczenie: W artykule przeanalizowano nowoczesne technologie i funkcjonalność systemów wykrywania ataków oraz rozważane są podstawowe typy zadań, które powinny być rozwiązane przez takie systemy. Dokonano klasyfikacji systemów wykrywania ataków na różnych podstawach.

Słowa kluczowe: atak sieciowy, system informacyjny, system wykrywania ataków, włamanie, nietypowe zachowanie, sygnatura, sieć

1. Introduction

At this time, the issue of providing information systems (IS) security is extremely important. New principles of network construction, that based on mutual exchange of packets, have allowed to significantly increased the level of flexibility and

[1] PhD, Lviv Polytechnic National University, Associated Professor of Information Protection Department, oleh.harasymchuk@gmail.com

[2] Lviv Polytechnic National University, student of Information Protection Department, olhabloshchenko@ukr.net

[3] PhD, Separated Subdivision of National University of Life and Environmental Sciences of Ukraine Berezhany agrotechnical institute, Associated Professor of Energy and Automatics Department, ramsh_v@ukr.net

survivability of systems. During the past twenty years we see the extraordinary development of the Internet and its rethinking in a new quality.

But, with the spread of the networks, have begun to appear the facts of committing using the Internet. One of the dangerous types of malicious activity on the World Wide Web is a variety attacks, that are constantly improving.

A network attack (web-attack) is an action, aimed at seizing of control (privilege escalation) of a wide/local area network, or its destabilization, or denial of service, and as well an obtaining data from users, who use this wide/local area network.

For now, distinguish the following types of attacks: mailbombing, buffer overflow, use of specialized programs (viruses, packet sniffers, Trojan horses, email-worms, rootkits, etc.), digital network intelligence (DNI), IP-spoofing, man-in-the-middle, injection (SQL-injection, PHP-injection, cross-site scripting or XSS-attack, XPath-injection), denial of service (DoS- and DdoS- attacks), phishing-attacks [1].

Recent trends indicate about constant emergence of new types of attacks – hidden attacks. In this case, the computers, controlled by the attacker, gain access to the target service quite on legal grounds (for example, visit the company's website) and overload the channel with resource-intensive operations (quality reduction attack) or at some point "explodes" by empty traffic, which puts before security systems new non-trivial tasks of detection and counteraction. To date, it has necessary to state that there is no reliable comprehensive tool of counteracting these attacks. However, the role of modern intrusion detection systems (IDS) is gradually growing [2-4].

Intrusion detection system, unlike a firewall, can protect not only from an external attack, but also from an internal one, which can be even more dangerous.

Currently, the theory of IDS went far ahead. Mathematicians develop statistical models to be able to distinguish suspicious network activity from acceptable, but in practice the "pattern model" ("signature") is more popular. That is, the intrusion detection system is the stronger, the more signatures (patterns) of known attacks it knows. The working principle of such a system is in analyzing network traffic in real time and logging of events, which are based on the knowledge of this system fall into the category of unauthorized.

The purpose of this work is to analyze the technology and functionality of intrusion detection system, the range of tasks they must solve and the implementation of the classification of these systems on various grounds.

1.1. Basic information about intrusion detection systems

Intrusion detection – is the monitoring of events in a computer network or system and their analysis for security policy violations.

To date, the attack detection technology, on the one hand, is still very immature, and on the other - is constantly attracting new producers and developers, the number of which is growing rapidly. Constantly emerging the firms, that offer their services in this area, but, they are also quickly disappearing or being absorbed by more powerful rivals and competitors. However, despite the lack of theoretical foundations of attack detection technology, there are quite effective methods that are used today.

The basic mean of protection of information and telecommunications systems and networks from information-destructive influences (interventions) in the form of cyber-attacks are *intrusion detection and/or prevention systems*, the main goal of which is to operational them identification (establishing a compliance between the object and its identifier (unique attribute) and, ideally, the initiation of an effective protection script to stop the fact of violation of confidentiality, availability and integrity of information resources or services.

Attack detection – is a process of assessing the events of an information system and its information flows, which is implemented through analyzing the event logs of operating systems (OS) and applications or network traffic.

Intrusion detection systems should not be used if access to the corporate network from the Internet is not blocked by any other mean of protection (firewall, etc.) and anybody can enter the network. Detection of attacks should be a logical complement to existing security means, and should to enhance their capabilities for security management of IS. IDS also allows you to control the effectiveness of other security systems, such as firewalls, identification and authentication systems, access mediation systems, tools for building virtual private networks, cryptographic information security systems and antivirus systems. Due to that, they are the main goals of offenders attacks. Given the fact that these systems are created and operated by common people, they are also tending to human errors, like all other components of the IS.

The existence of attacks is closely linked with their detection. If it could not be possible to detect the attacks, it would be a disaster in terms of security, and vice versa, if all attacks would be detected, there would be nothing to explore and would not be nothing to defend from.

In practice, to protect from attacks used not only software products but also specialized hardware-software tools. The use of a hardware component introduces a new features of functioning, and it is also necessary for reduce the cost of existing solutions with the required of more productivity and security.

IDS constitute a separate class of software, which included programs, procedures, rules, and also, if that provided, supporting documentation and data, which relating to the functioning of the information processing system [5]. The full name of IDS is intrusion detection and prevention systems, because it is automated counteraction are one of the main advantages of such systems, compared to, for example, tools that based on human factor.

The use of IDS makes it possible to solve a number of tasks, that ensure the achieve of information security goals:

- monitoring and analysis of user, network and system activity;
- audit of system configuration and detection of vulnerabilities;
- recognition of known and, if it possible, unknown attacks and warning the staff responsible for providing of information security (IS);
- "understanding" of mainly obscure sources of information about attacks (network traffic, event logs, system calls, etc.);
- statistical analysis of anomalous actions patterns;
- control of the integrity of files and other resources of the information system (IS);
- installation and work support of honeypot to capture information about intruders;
- burden reduction on the staff (or exemption from it) which are responsible for information security (IS), from the current routine operations of control over users, systems and networks that are the components of the information system (IS);
- control of all actions of the subjects of the information system (users, programs, processes, etc.), including those, who have an administrative privileges;

- providing the opportunity to management security functions to non-specialists in the area of information security.

Some of these tasks are solved by mechanisms that built into operating systems or applications. But the process of such analysis is labor-intensive and requires to perform a large number of routine operations, which can lead to omission of some violations.

Many classes of attacks include each other, therefore software products that have different functions of prevention and protection against attacks can be divided into the following categories:

1. *Firewalls* - tools that filter packets based on their headers and/or other criteria.
2. *Antivirus programs* that search for viruses and suspicions on viruses in files or information flows.
3. *Sniffers* - programs that intercept all traffic in the segment for its further analysis manually or automatically.
4. *Means of detecting attacks/intrusions* - similarly as sniffers, carries out interception all or part of the traffic and search for suspicious events. Different search methods are used, most often the signature method.
5. *Means of Integrity Control of file systems* periodically check file systems, on which operating systems are installed, which can be compromised on the fact of changing or deleting of "unchangeable" files, emergence of new. Verification most often is carried out with using cryptography tools with a view to increase reliability.
6. *Honeypot* - mimic the work of one or the other service/host of network. All appeals to them are controlled and recorded. Is a class that is evolving to date. Are promising in terms of gathering evidence of malicious intent of the attacker, in this without exposing the real systems to danger.

1.2. Technologies and functionality of intrusion detection systems

Intrusion detection systems, like most of modern software products, shall comply with a number of requirements: modern development technologies, focus on the features of modern information networks, compatibility with other programs.

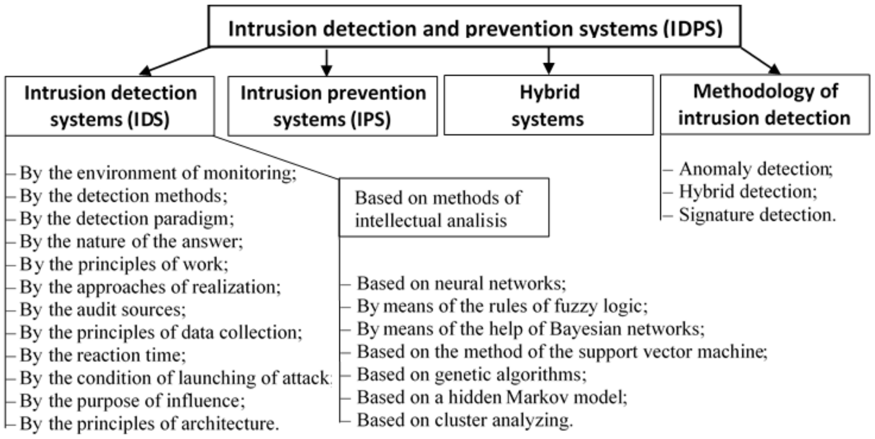
Intrusion detection and prevention systems (IDPS)
Intrusion detection systems (IDS)
Intrusion prevention systems (IPS)
Hybrid systems
Methodology of intrusion detection
- By the environment of monitoring;
- By the detection methods;
- By the detection paradigm;
- By the nature of the answer;
- By the principles of work;
- By the approaches of realization;
- By the audit sources;
- By the principles of data collection;
- By the reaction time;
- By the condition of launching of attack
- By the purpose of influence;
- By the principles of architecture.
Based on methods of intellectual analisis
- Based on neural networks;
- By means of the rules of fuzzy logic;
- By means of the help of Bayesian networks;
- Based on the method of the support vector machine;
- Based on genetic algorithms;
- Based on a hidden Markov model;
- Based on cluster analyzing.
- Anomaly detection;
- Hybrid detection;
- Signature detection.

Figure 1. Classification features of intrusion detection and prevention systems

Current intrusion detection systems are modern multifunctional complexes that solve a wide *range of tasks*:

– Monitoring the effectiveness of firewalls. For example, installing an intrusion detection system after a firewall (within the corporate network) allows you to detect attacks that were missed by the firewall and, thus, to determine the missing rules on the firewall.

– Monitoring of network nodes with uninstalled patches or nodes with outdated software.

– Blocking and access control to individual Internet nodes. This is necessary when the organization doesn't have the money to acquire a firewall and IDS, and the functions of the firewall are spread between the intrusion detection system, router and proxy server.

– Access control of employees to servers based on keywords.

– Monitoring email. Some systems can detect viruses in e-mail messages.

– Backup coping of firewall functions. Very often, attackers incapacitates the firewall in order to further uncontrolled intrusion into the corporate network. To reduce the likelihood of intrusion, can be used intrusion detection systems that operate on network level, to temporarily backup firewall functions. This will enable to filter a network traffic by different fields of the IP-packet header, and organize powerful enough filter of packet, which not much inferior to the capabilities of a real firewall.

– Temporary replacement of the firewall during maintenance for update the firewall software or testing its settings.

– File access control. Mainly for this purpose information protection systems from unauthorized access are used. However, in some cases, these systems cannot be used to control access to files that contain important and critical information (for example, password files or databases). Thus can be used IDS that operates on individual nodes (so-called host-based IDS). In doing so can be used both systems that analyze event logs and those that analyze system calls.

– Analysis of information flows. Using of IDS can be controlled all protocols and services that used in the network, as well as the frequency of their using, which allows to build an information flows diagram in the organization and a network map, which is the key to a successful creation of information security infrastructure in the organization.

– Gathering of evidence and investigation of the incidents. IDS can and should be used to gather evidence of unauthorized activity through the following *such opportunities*:

a) recording of events occurring during the attack, for further analysis and research;

b) imitation of non-existent applications in order to misleading the attacker (the so-called mode of deceptive system);

c) advanced analysis of event logs of application and system software, database servers and Web-servers, etc.;

d) the ability to investigate security events before execution any action;

e) receiving DNS-, MAC-, NetBIOS- and IP- addresses of the attacker's computer.

– Network map construction. Very often, some IT-departments of the organization or their employees gain unlimited and uncontrolled power over the system and its components, which gives rise to vulnerabilities in the software and hardware that are not eliminated for a long time. Offended or disgruntled administrators of IT-departments may also unauthorized and uncontrollably change the configuration of networking hardware, critical servers, and other devices to harm their organization or blackmail their leadership. Intrusion detection systems are an effective, and often the only, means of controlling employees and departments that have great power over an organization's information system.

An effective way to prevent unauthorized using of information systems and network resources is to support multilevel security, when shares firewalls, intrusion detection systems, audit systems, security policy and other means of security.

The most overall structure of the intrusion detection system developed by a group of CIDF researchers (Common Intrusion Detection Framework) [6], fig. 2.

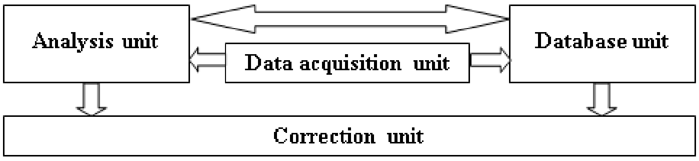

Figure 2. The overall structure of the intrusion detection system

Data acquisition unit (*sensor, Event-box*) – analyzes the data for processing and decision making by the analyzer. This data may contain the names of the controlled parameters, their features and values. The sensor can perform data conversion to the requested format or for curtailment the scope of data which are transmitted.

Analysis unit (*Analyzer-box*) – decides on the presence or absence of signs of attack or anomaly based on data from sensors. As part of the analysis, this block can perform the functions of filtering, normalization, conversion and correlation of data. When an attack is detected, the analyzer block may add a description of the detected attack to the input data. Can have a multilevel system.

Database unit (*data warehouse, Database-box*) – the block contains sets of decisive rules and semantic descriptions of attacks, as well as cumulative information from sensors. Data can be in text files, databases, etc.

Correction unit (*Response-box*) – informs the administrator about the recorded attack, and in the case of an intrusion prevention system, forms an active response.

Intrusion prevention systems monitor activity in real time and quickly implement actions to prevent attacks. Possible measures: blocking traffic flows in the network, resetting connections, issuing signals to the operator. Intrusion prevention systems can also carry out packet defragmentation, ordering of TCP packets to protect against packets with changed sequence numbers, and confirmations.

1.3. Classification of intrusion detection systems

There are different ways to classify intrusion detection systems based on different characteristics. The type of IDS should be defined based on the *following characteristics*:

– Method of system control. According to the methods of system control are divided into network-based, host-based and application-based.

– Method of analysis. It is part of an intrusion detection system that analyzes events from an information source and decides if intrusion occurs. Methods of analysis are misuse detection and anomaly detection.

– A time delay between receiving information from the source and its analysis and decision making. Depending on the time delay, intrusion detection systems are divided into interval-based (or batch mode) and real-time. Most of commercial IDS are real-time network-based systems.

Detection of attacks requires an execution one of the two conditions: either understanding the expected behavior of the controlled object of the system, or knowledge of all possible attacks and their modifications. Historically, the technologies on which IDS are built, are conditionally divided into two categories:

1. *Detection of anomalous behavior* (anomaly detection):

a) is based on the model of normal behavior;

b) identifies anomaly occurrences at the flow of events.

2. *Detection of misuse* (misuse detection):

a) is based on a model of behavior with criminal intent;

b) compares models with the flow of events.

Detection of anomalous behavior, uses a well-proven apparatus of mathematical statistics. The approach is used in detecting DoS-attacks that use sending a large number of traffic over a short period of time, etc. This approach tries to apply in controlling user's behavior in the information system. Typical user actions are described in the pattern, deviations from which are recognized as an anomaly and that requires the intervention of relevant services.

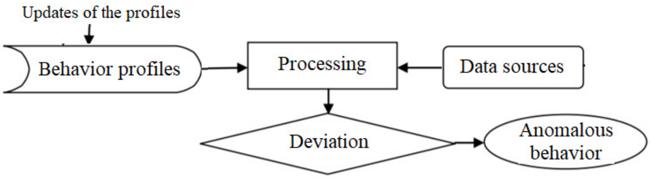

Figure 3. Scheme for detecting anomalous behavior

To date, the technology of anomalies detection is not widespread. This is due to the fact that this technology looks beautiful in theory, but it is very difficult to realizing in practice.

Another approach to detecting attacks is the misuse detection, which is in description the attack in the form of a pattern or signature and search for this pattern in a controlled space (in network traffic or log). Antivirus systems are a prime example of an intrusion detection system that works with this technology.

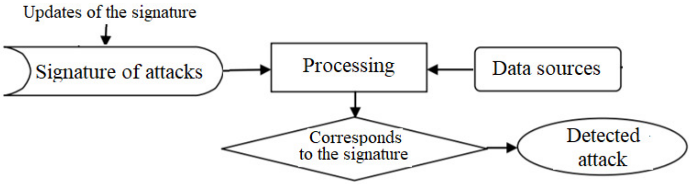

Figure 4. Signature-based intrusion detection system

It is difficult to single out one better method to using it in the IDS. Each of these classes has its advantages and disadvantages, its scope, its attacks, for which detect it is designed to. Experts note that these methods are used in modern systems in proportions of 70/30 in favor of a signature method.

But, in practical activities, can be applied an another classification, which takes into account the principles of practical realization of such systems:

– *detection of attacks at the network level* (network-based) – systems analyze network traffic;
– *detection of attacks at the host level* (host-based) – systems analyze event logs of operating system or programs.

A principal advantage of network-based intrusion detection systems is that they identify the attack before those reach the node which is attacked. These systems are easier for deployment in large networks because they don’t require installation on different platforms that used in the organization. Besides, such systems almost don’t reduce productivity of network.

Host-based intrusion detection systems are designed for work under the direction of specific operating system, but this imposes certain restrictions on them. Using the knowledge of how an operating system should "behave", tools built by this approach sometimes can detect intrusions that missed by network attack detection tools. Using the knowledge of how an operating system should "behave", tools built by this approach sometimes can detect intrusions that missed by network-based attack detection tools. But most frequently this is achieved at a high cost, because the permanent registration which is required to perform this kind of detection significantly reduces productivity of the host which protected. Such systems heavily load the CPU and require large amounts of disk space to store event logs and, in principle, are not apply to highly critical systems that work in real time. If there is a need to protect one or more nodes, then host-based intrusion detection systems can be a good choice. But if need to protect most of network nodes, network-based intrusion detection systems are likely to be the best choice, because increasing the number of nodes in the network will not affect the level of security which is achieved with an IDS. It will be able to protect additional nodes without advanced settings, while in the case of using a host-based system, it will be need to install it and configured for each protected host. An ideal solution would be an intrusion detection system that combines both of these approaches.

Commercial intrusion detection systems (IDS) that available on the market today use a network or system approach to detect and repel attacks. In any case, these products search for attack signatures, specific patterns that usually indicate on hostile or suspicious actions. In case of search for these patterns in network traffic, IDS works at the network level. If the system looks for attack signatures in operating system event logs or in application, this is the system level. Each approach has its advantages and disadvantages, but they both complement each other.

There are several ways for detect, block, and prevent security policy breaches. The first and most common way is recognizing already implemented attacks. This method is used in "classic" intrusion detection systems, information protection systems against unauthorized access, etc. But, the "disadvantage" of tools of this class is that the attacks can be re-implemented. They are also re-detected and blocked. And so on, to infinity, what, of course, inefficient, because it leads to impermissible time losses, human and material resources. It is better to prevent attacks even before their realization. This is the second way. It is implemented by finding vulnerabilities (in other words, it is the detection of potential attacks) which can be used to realization an attack. The third way is to detect already committed attacks and prevent their recurrence in the future. By virtue of the above, security policy detection systems may be classified according to the stages of attack development, as described below.

Systems that operating in the first stage of the attack realization allow to detect vulnerabilities of the information system which are used by intruder. In other words, these are intrusion prevention systems. Otherwise, the tools of this category are called security assessment systems or security scanners.

Systems that operating in the second stage of the attack realization and allow to detect attacks in the process of their implementation, that is in real (or close to real) time. It is these tools and are considered to be intrusion detection systems in the classical sense. In addition, new classes of tools of intrusion detection have recently emerged – *deception systems* and *intrusion prevention systems*.

Systems that operating in the third stage of the attack realization detect already committed attacks. These systems are divided into two classes – *integrity control systems*, which track changes in controlled resources, and *logbook analysis systems*.

Unfortunately, a single terminology in this area still not produced. Each producer, wishing to show that its system is unique and superior to other solutions, creates a new class of IDS.

This is how the *following classes of intrusion detection systems* have appeared:

– virtual intrusion detection systems,
– hybrid intrusion detection systems (for example, Prelude IDS),
– gateway intrusion detection systems,
– multi-tiered intrusion detection systems,
– state-controlled intrusion detection systems,
– specification-based [7] or stack-based intrusion detection systems, etc.

As a result of the analysis of the most common tools of detection and counteraction to attacks, we proposed the following classification (Fig. 5):

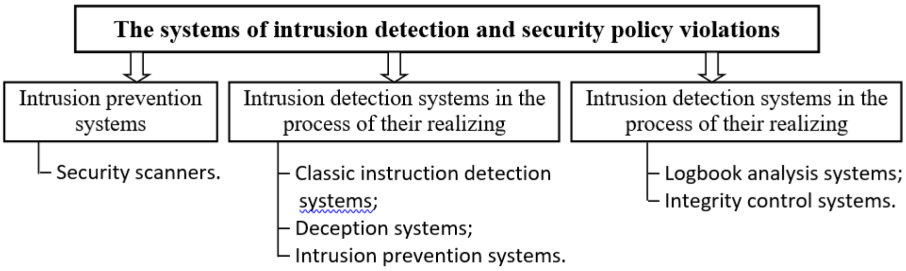
The systems of intrusion detection and security policy violations
Intrusion prevention systems
Intrusion detection systems in the process of their realizing
Intrusion detection systems in the process of their realizing
Security scanners.
Classic instruction detection systems;
Deception systems;
Intrusion prevention systems.
Logbook analysis systems;
Integrity control systems.

Figure 5. Classification of intrusion detection systems

2. Conclusions

In summary the above, we can draw the following conclusions:

1. To solve the problems of protection against attacks over the Internet requires a concept that defines the objects of protection, goals, tasks and basic principles of protection, and also the composition and sequence of work to prevent, detect and respond to attacks.

2. Sufficiently simple and effective approach for providing a protection is using a list of the most commonly vulnerabilities used for attack, which used by hackers to carry out a network attacks, and ways to resolve them. In fact, these vulnerabilities are exploited in more than 80% of all attacks that occur. Modern network scanners are

able to detect these vulnerabilities. Currently, the list of most commonly used vulnerabilities is constantly expanding.

3. Administrative methods of protection of corporate networks are suitable for use in small networks, since they involve a significant amount of manual work.

4. To protect corporate networks from distributed attacks, most appropriate to used full-featured protection methods which based on the principles of detection, reorientation, verification and forwarding, using of which guarantees full protection.

5. Good results are obtained by the use of specialized architecture, which includes the abiliting of detecting more and more refined, complex attacks of a particular type, and counter them, and should to prevent offenders to causing a serious damage to valuable network resources.

REFERENCES

1. Мережеві атаки, можливості та недоліки мережевих екранів [Електронний ресурс]. – Режим доступу: *https://ukrbukva.net/page,2,91957-Setevye-ataki-vozmozhnosti-i-nedostatki-setevyhekranov.html*, 28.08.2020. .
2. AXELSSON S.:, Research in Intrusion-Detection Systems: A Survey, Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, 1999.
3. Webpage www.ic3.gov [Електронний ресурс]. – Режим доступу до матеріалу сайту: *http:// www.ic3.gov/ media/IC3-Poster.pdf*, 21.09.2020.
4. WU S.X., BANZHAF W.: The Use of Computational Intelligence in Intrusion Detection Systems: A Review, Applied Soft Computing, 10(2010)1, 1–35.
5. ЗОРІНА Т.І.: Системи виявлення і запобігання атак в комп’ютерних мережах. Вісник східноукраїнського національного університету імені Володимира Даля № 15 (204) ч.1 2013. – с. 48-54.
7. ДОВБЕШКО С.В., ТОЛЮПА С.В., ШЕСТАК Я.В.: Застосування методів інтелектуального аналізу даних для побудови систем виявлення атак. Сучасний захист інформації, 37(2019).
8. BERTHIER R., SANDERS W.H.: Specification-based Intrusion Detection for Advanced Metering Infrastructures. Conference: 17th IEEE Pacific Rim International Symposium on Dependable Computing, PRDC 2011, Pasadena, CA, USA, December 12-14, 2011.