Network Systems Intrusion: Concept, Detection, Decision, and Prevention

Pleskonjic, Dragan; Omerovic, Sanida; and Tomazic, Saso

Abstract — ***This paper analyzes concepts for intrusion detection processes; building decision making (DM) criteria on the bases of intrusion detection, and prevention based on DM as a last level of protection in computer systems and networks. The second part of the paper discusses a practical implementation for Intrusion Detection and Prevention Systems (IDPS), based on Wireless technology (WIDPS). Basically paper concentrates on the problems/answers of how to differentiate between legal and illegal access, i.e. intrusion and what are the key and root causes of this difference. Two issues are differenced: finding the set of concepts needed for detection and a set of criteria for DM in IDPS. Paper concludes with achieved results and future goals related to automated DM process in wireless technology.***

Index Terms — ***agent, artificial intelligence, concept, decision making, detection, intrusion, prevention, sensor, server, system, wireless network.***

1. INTRODUCTION

THE problem of intrusion in computer systems and networks has been around for decades. Unfortunately, that problem is growing as the variety of different threats is increasing every day, especially with the massive usage of computers, distributed systems and the Internet. Wireless and mobile networks give us new challenges with respect to IDPS, as their nature is to spread their network signals around without known exact boundaries. Wireless systems, which are competitive by their price/performance ratio, provide an ability of anytime, anywhere connectivity. At the same time, this means that intrusion can happen anytime, anywhere in the network.

Since the phases for both attack and response are layered processes (later explained in Section 2.2), paper presents the IDPS as a DM System in a form of hierarchical set of the following six layers: Unstructured data, Data Retrieval, Data Modeling and Analysis, Concept Layer, Decision Making, and Decision [23].

Manuscript received February 25, 2007.

Dragan Pleskonjic is with the Finsoft Ltd, UK (e-mail: dragan.pleskonjic@finsoft.com). Sanida Omerovic and Saso Tomazic are with the Faculty of Electrical Engineering, University of Ljubljana, Slovenia (e-mails: sanida.omerovic@lkn1.fe.uni-lj.si, saso.tomazic@fe.uni-lj.si).

In order to populate all six layers with useful data that will lead to automatic intrusion prevention, one needs to answer the following 7 W's questions [26]:

- Why? - Why does one need an IDPS in one's computer system/network?
- Who? - Who sets the rules for IDPS criteria (the owner of the computer, the network, the programs, the processed data, or services offered on the network)?
- When? - When to react if detection of an intrusion is established (processing time for detection or prevention and corrective action)?
- Where? - Where are the places where computer systems, network, programs, data, and services are most vulnerable?
- What action/state? - What are we protecting and from whom? What are the necessary actions to be taken when detection of intrusion happens?
- (W)How? - How we can differentiate between attack and legal access? How to build a model an ideal IDPS (what are the necessary concepts)? How to implement such a system? At the end of the paper, a proposition of a practical implementation for WIDPS is given.
- Which? - Which ones are the possible implementations of IDPS, based on the 7 W's criteria?

Related to answering the first W's question "Why" one can consider WIDPS as a superset of traditional IDPS designed for wired networks. This is a consequence of the fact that the sets of threats, attacks and vulnerabilities of wired networks are only a subset of those for wireless networks. In other words, wireless networks are vulnerable to all intrusion types possible in wired networks, but, in addition, there are numerous possible intrusions that are wireless specific.

"Wired" means that the user's computer is physically attached and that wire concentration exists; an intruder/attacker needs to plug directly into the network. In wired networks there is network security perimeter. On the other hand, in wireless a network the intruder can stay anywhere in an area covered by the signal and intrudes, and remains unseen. There is no exact "border" between an internal and an external network. This causes a loss of the exact

classification between insider and outsider attacks which is one of the important concepts in classic IDPSs.

Sometimes people assume that host based systems prevent insider attacks and network based systems prevent outsider tasks. Authors may not agree with this in practice, but it is the case that, as soon as one adds a Wi-Fi signal, the border of defense becomes unclear and is not sharply defined.

The problem one has is the case of classic IDPS is that they cannot provide an adequate and satisfying level of protection for wireless networks. One needs WIDPS or at least necessary extensions to current systems in order to cover wireless based threats, attacks and vulnerabilities.

The answers for the rest of the W's questions are structured in the shape of DM layers as follows: Intrusion Detection, Decision Support, and Prevention. Then follows a proposal for WIDS, based on those DM layers and Artificial Intelligence (AI). Paper concludes with future challenges for WIDPS and IDPS in general.

The aim of this paper is to stress the various possibilities of WIDPS, since wireless technology is increasingly present in today's networks and therefore in people's life in general. Only the overview of WIDPS solution is presented. Full documentation is possible on request from the authors.

2. *Decision Making System in IDPS*

In this section, foundations of our IDPS solution are established, through the layers of a DM System. Our main goal is to determine where the weak spots of IDPS are and how to improve them.

The observation of processes in layers is not a new thing in science. One can take a look in a Six Dimensional Information World [29], OSI Network model, TCP/IP model, Semantic Web layered model [24], Layered Mobile Agent Architecture [36] etc, and see that different processes can be distinguished into several different hierarchical layers.

What is the process of DM in general and can it be applied to IDPS? In [23], [30] the authors presented the idea that every process which has Unstructured data and some Question as Input, and Decision on the output, can be seen as DM Process, as shown at Figure 1.

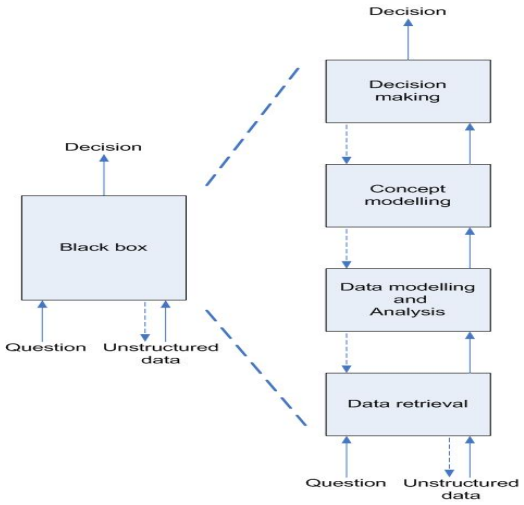

Figure 1. DM System Layers

Now let's discuss whether this model can be used for IDPS.

Generally speaking, the first step in IDPS is monitoring communications and/or behavior and collecting data. At the beginning of the process one has Unstructured Data. There is no exact method to differentiate the data of interest for IDPS. The majorities of data are, at first, not of interest and can be treated as noise in terms of their importance for IDPS. Usually that data represent regular use of the system; only small amounts of data and behavior can be part of illegal actions and intrusions (actually in real systems, on occasions this can be much more than a couple of percent, but still not a major part of communications).

The next layer in DM is Data Retrieval. Applied in IDPS, retrieval should be done in such a way as to extract the data of interest and not to overload the processor or to consume too many other resources, as that can be problem for itself. Also, efficient and reliable algorithms are necessary for this part. Moreover, in real time systems (which IDPS is considered to be) this problem can be very significant.

Usually IDPS deals with huge amounts of data. One of the first and most important questions is how to effectively do Data Modeling and Analysis, which also represents the next layer in a DM system. This should help one to understand and differentiate the data that are important for detection and appropriate prevention and what data are not useful for further analysis.

After the data are modeled and analyzed, one must construct concepts and build them into the Concept Layer. The concept layer in a DM system represents data structured in a way of conceptual hierarchy, where it is possible to add new concepts in the course of a simulation of process of learning, and also delete concepts which are no longer valid. Data are stored as concepts, so that that previously learned

knowledge (stored in some form of concept hierarchy) can be used to prepare for significant points and mimic human thinking, coupled with fast data analysis and processing to support the next stage – the DM process. One needs the Concept layer in IDPS in order to automate the detection and prevention processes with maximum possible accuracy.

Usually, it is hard to make all parts of a DM process clear. What is certain is that one must conform to the DM criteria, based both on the concepts and applications using the DM System.

This analogy with human DM (which is based on both previously learned knowledge and everyday perception) has been an important topic in science for many years now. Among possible mechanisms to achieve an automated process of DM are: Neural Networks, Expert Systems, Fuzzy logic [31] [32] [33] [34], etc.

IDPS is observed as a layered architecture made of three components: Intrusion detection, Decision support, and Prevention. It is possible to present IDPS and DM layers in parallel, as shown at Figure 2. Intrusion detection consists of the first four layers of DM, and Decision support consists out of last two layers of DM. Prevention depends both on the Decision support layer and the present technology available.

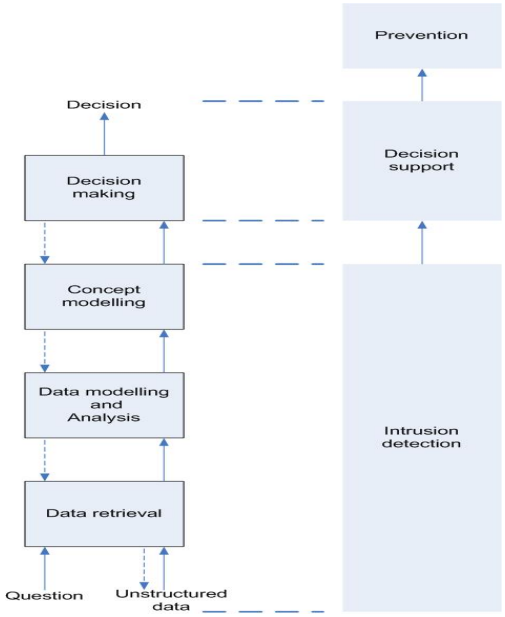

Figure 2. Parallel presentation DM and IDPS layers

In the next section, all three IDPS layers are explained in greater detail. The system proposed in this and some of other papers intend to employ mechanisms of automated DM as much as possible in order to make IDPS more human-aware and less like rigid computer-aware processes.

2.1 Intrusion Detection: Definition and Concepts

The potential threats to networks are numerous. Denial of Service (DoS), session hijacking, and sniffing are just a small sample of the potential attacks. While many of the attacks against wireless networks are similar to those against wired networks, 802.11 networks are generally subject to more threats.

Another problem is related to the open nature of Wireless Local Area Network (WLANs). Due to the propagation characteristics of wireless networks, there is limited control from where a signal can be accessed. This leads to a situation where, unlike wired networks, a hacker can manipulate or eavesdrop on the network from uncontrolled locations or geographical areas which were not intended to be served when the network was implemented.

Problems with network and especially WLAN security are well known, but solutions for those problems have not been coming quickly. That is especially the case with standardization. In order to satisfy market needs, some vendors started their own developments and proprietary standards. But this approach has not satisfied a wide base of customers. Work has also been directed toward confidentiality and authentication problems. On the other hand, problems with respect to some threats and resulting intrusions to corporate and organization networks, using wireless have not yet been addressed properly for a long time. There are some solutions existing but they are not directed to toward this area. At present in the area of intrusion protection there is an extension of Snort IDS named Snort Wireless [http://www.snort-wireless.org/], which is an open source solution. There are also vendors who are addressing different aspects of security, including wireless networks. But there are very few solutions specifically directed to WIDS. Namely, those solutions that are coming from: Airdefense, Enterasys, Network Chemistry, IBM, Cisco and WIDZ (rather waggish on first glance, but actually a serious approach). There are also other partial solutions.

WLANs can also create backdoors to wired networks. Many organizations spend a great deal of money on wired network security with extensive investments in firewalls, Virtual Private Networks (VPNs), and other security-enhancing technologies. A single unauthorized (rogue) wireless access point (WAP) connected to a wired network has the potential to create a backdoor to the wired network, circumventing the wired network security and thereby allowing a hacker to effortlessly gain access to a closed network. A wireless policy can help combat these threats. Fortunately, it is never too late to develop a policy, although an early adoption approach is mostly highly effective.

2.1.1. Intrusion definition

Before defining the intrusion, a list of specific attacks and vulnerabilities in Wireless Systems is presented. In order to be protected from the intruder, one must be fully aware of these two issues.

Wireless specific attacks and vulnerabilities:

- Easy access to 802.11 networks
- Unauthorized ("rogue") access points
- Unauthorized use of service
- Denial-of-service vulnerability
- MAC address spoofing and session hijacking
- Relatively easy traffic analysis and eavesdropping.

Various kinds of threats and actions of malicious people:

- Employing unauthorized access points (APs) – "rogue" or bogus APs that are designed to steal the association and login credentials
- War Driving - Probe requests which do not have the ESSID field set in the probe
- Flooding - attempts to flood the AP with associations
- Monkey / Hacker jacks
- Null probes
- Null associations
- Floods etc.

In the early 1980s Jim Anderson [35] was responsible for some of the starts in intrusion detection. Anderson defines an intrusion as any unauthorized attempt to access, manipulate, modify, or destroy information, or to render a system unreliable or unusable. This rather classic definition is accepted across the community and successfully covers important aspects of intrusion detection.

The definition of an intrusion depends upon the perspective from which it is seen (if one is attacker, the owner of the data, or an administrator, etc). It is very hard to differentiate WHAT an intrusion can be, especially because one can not predict the future intrusions and give them an irregular access label, before they have happened.

That is why is important to set the concepts of the intrusion, so one can define IDPS, no matter what is situation arises.

2.1.2. Intrusion concepts (IC)

In order to create an IDPS, various approaches can be taken. In this paper, IDPS is presented through the layers of a DM System, since authors believe this is the most efficient method to model a real life situation from the perspective of a network security environment.

An IDPS can be classified (according to various criteria) into different concepts: detection model, scope of the protection, time of attack, and type of response. The cases of IDPS concepts are given below.

As a detection model i.e. what is detected:

- Misuse detection i.e. signature based approaches
- Anomaly detection.

Scope of the protection (or by deployment) i.e. where detected:

- Network Based
- Host Based
- Application Based.

When an attack is detected:

- Real time
- After the fact i.e. after attack happened.

Type of response:

- Active
- Passive.

Based on these concepts, input data from an IDPS can be quite varied: traffic network parameters, application time, data transfer rate, etc., depending which concept is applied. After doing Data Retrieval, one proceeds to Data Modeling and Analysis are processed next. Basically system is doing filtering through all parameters that user receives from the network. Data which are crucial for the IC are further modeled in such a way from which concepts out of them. The rest of these data, which are not correlated with the IC, are discarded. A full description of how concepts are defined, built, populated and updated is given in the practical example of WIDS in Section 3.

2.2 Decision support in IDPS: Detection and Decision

After building the IC filtered from retrieved data next step in IDPS is Decision Support, namely Detection and Decision.

2.2.1. Intrusion definition

Detection in the IDPS is based on the IC. If one is able to detect the IC, then one is also able to detect the attack. For efficient detection of the intruder, one must analyze the attack anatomy. One approach is:

- Reconnaissance
- Exploitation
- Reinforcement
- Covering Tracks.

After the successful Detection of the intrusion, a proper Decision must be made.

2.2.2. Decision

In an IDPS Decision Support can be fully automatically or include human interaction. After the user has been recognized as an attacker, the system should be able to decide the following:

- Close the connection between the user and the system, so there is no dataflow
- Locate the physical resources of the intruder
- Learn how the attack happened and take self-learning steps so that a future attack of a similar kind can be blocked.

As stated earlier, after Decision Support, the next layer in IDPS is Prevention. This layer depends upon both the Decision support layer and the present technology available.

2.2.3. Prevention

Most of today's IDS systems will prevent an attack by alerting, dropping the offending packets, terminating the session for TCP and UDP based attacks, and dynamically establishing firewall rules that can keep the source of the threat off the network indefinitely or for a configurable period of time. Known sources of attacks can be stopped from even entering the network by enabling "Black Lists," while key corporate resources or trusted networks are always allowed to pass via "White Lists."

The phases for the response/attack prevention [27] are:

- Preparation
- Identification
- Containment
- Eradication
- Recovery
- Follow up and
- A loop for network self learning.

In general, the essence of Prevention is to protect individual/company data and provide Confidentiality, Integrity and Availability (the so called "CIA triad"). Viewing Prevention as a layered process (like Intrusion Detection and Decision Support) helps to better differentiate Intrusion weak spots and to builds a strong foundation of Prevention actions.

3. WIDPS

This section presents a full technical overview of our WIDPS solution based on the idea of DM layers. The letter W is used here to denote wireless, which is one of the growing network infrastructures at the present time.

It has been known that wireless networks suffer from all known wired intrusion types as well as some new intrusion types that are not specific for wired networks. In order to prevent these, a new approach is proposed, so one can detect and prevent intrusions of this type of network automatically.

3.1. The new idea and solution

When it comes to WIDPS, two problems arise:

- Wireless networks intrusions
- The kind of solutions which are intended to address typical problems in currently available IDPSs categories, which are briefly described above (misuse/anomaly detection, host/network, etc.) and which offer the resolution of such problems.

The idea is to create a WIPDS with a high degree of autonomy in tracking suspicious activity, detecting intrusions, making conclusions/decisions, and launching protective action (prevention) against the intruder.

Today's IDPS are mostly directed toward for wired networks. These systems are used in fixed and stable networks with "traffic concentration" units and their function is based on intrusion signs and rules. What the above mentioned systems lack are:

- What should be done about new attacks (different from the ones for which one know rules/signs)?
- How should the situation be handled where node is not based on a fixed physical place – which is case with wireless networks?

There is no "traffic concentration" in wireless networks (especially ad-hoc ones, but also in those with infrastructure too). In another words, there are no dedicated places where one can put IDPS agents (An agent is a program that performs some information gathering or processing task in the background). One needs a system that will support:

- IDPS agents in clients (wireless clients) for joint and local detection
- Cooperation between IDPS agents
- Self-learning capabilities
- Self-decision and alerts
- Self-defense against intrusion attempts (network administrators are not always present in the moment of intrusion).

This can be very complex in multidimensional and distributed system. Parties that will benefit from increased wireless security are:

- End user using wireless and mobile networks with increased freedom of work
- WISP (Wireless Internet Service Providers)
- Wireless software and hardware vendors, also where including in other wireless software and hardware products are included in other products
- The IT community in general (in this way one will encourage the average user to have more confidence in using wireless networks).

The use of Neural Network and Fuzzy logic in DM Systems (and also in WIDPS) has been considered as the Holy Grail for long time. With current developments in both areas possibility arises to consider their unity again and to create feasible system that combines them in order to give a more powerful solutions for the protection of wireless networks.

3.2. Architecture

The core of our WIDS proposed solutions are Agents [20]. In WIDS, agents are responsible for:

- Intrusion detection
- Decision support
- Prevention.

The architecture of our WIDPS solution is shown in Figure 3. WIDPS agents are connected (through secure channels) to each other and also through Access points. In that way Agents can efficiently exchange information and respond synchrously when an intrusion happens.

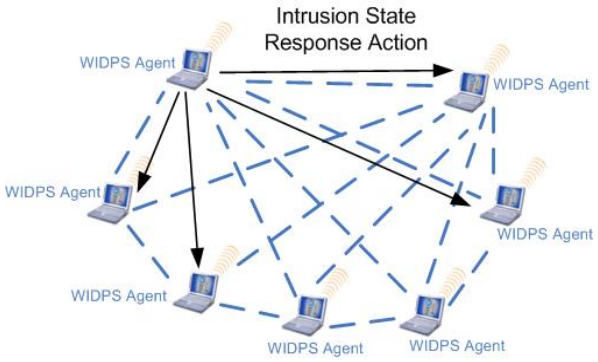

Figure 3. WIDPS Agents in ad-hoc wireless network [20]

This kind of solution is proposed for ad-hoc networks but not for the infrastructure mode. Some of this approach could be used to create basic principles for building a WIDS.

In order to protect any type of networks, the most important two concepts that need to be considered are:

- Intrusion Detection and Decision Concepts – A reactive approach
- Intrusion Prevention Concepts - Proactive action.

These two are quite different approaches, but should be very tightly coupled.

First, Intrusion Detection and Decision Concepts are discussed. The follow-up section is dedicated to Intrusion Prevention Concepts.

3.3. Intrusion Detection and Decision Support in WIDPS

For the WIDPS solution presented in this section, the following scenario related to Intrusion Detection Concepts is considered.

If one says that 0 is a proven intrusion, and 1 is a proven legal access, one can form limits in the following way:

- A is highest limit of decision where access is automatically classified as an intrusion
- B is lowest limit of decision where access is automatically classified as a legal access.

So, one can say that the scope is as shown at Figure 4:

- [0-A] is to deny access
- [A-B] requires human or artificial intelligence intervention
- [B-1] is to allow access

A and B are movable, where A ≤ B.

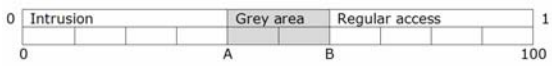

Figure 4. Example of the decision scale

One approach to making automated decisions is to define a scale with a range [0% – 100%] with thresholds at 40% and 60%. The system will consider as an intrusion everything in the range [0%-40%] and deny access. Also, the system will allow access for [61%-100%]. In the "grey area" which is, in this case in interval of [41%-60%], it will ask for assistance.

If one is talking about a WIDS Agent, assistance can be required from:

- A WIDS Sensor
- A WIDS Server
- Neighboring WIDS Agents
- And also from humans (for example from system administrator or response center personal). In that case it is not an automated, but a semi automated DM.

If assistance is required, suspicious activity will be held until an answer is received or a certain amount of time has passed. A good visual presentation of this is a slider with two movable notches representing low and high thresholds.

In [20], a mechanism has been proposed as shown at Figure 5 (slightly modified to fit also infrastructure mode also):

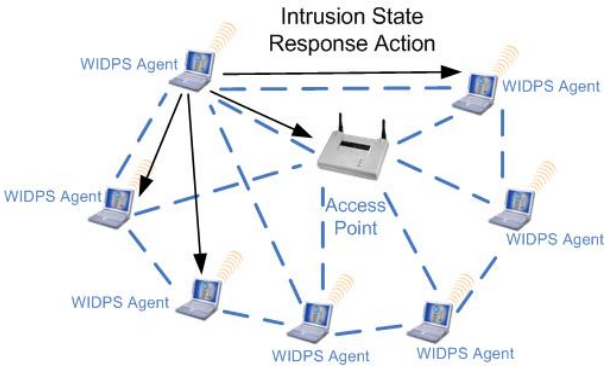

Figure 5. WIDS Agents in mixed (ad-hoc and infrastructure mode) wireless network

This mechanism considers:

- Data collection
- Detection (local and cooperative)
- Intrusion Response (local and global).

The DM processes in a WIDPS can be through the Conceptual Model WIDS Agent, as shown in Figure 6.

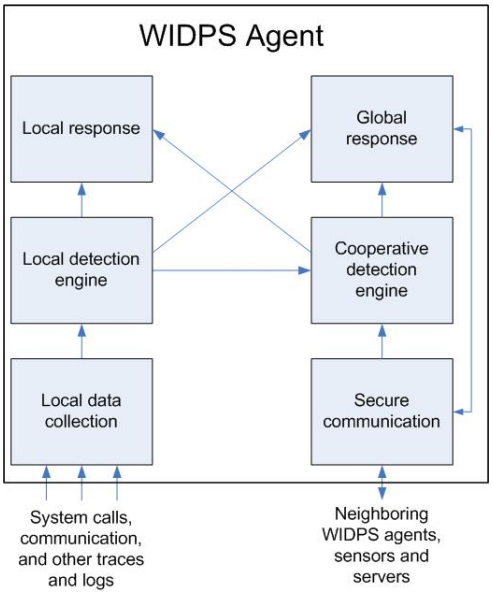

Figure 6. Conceptual model for a WIDPS Agent in an ad-hoc network [14]

The basic input in the Conceptual Model for a WIDS Agents is data that comes from an outside system and data that comes from the neighboring WIDS agents. These two types of data are processed in parallel inside the WIDS Agents. System data are gathered in the local data collection. Further, they are processed with a local detection engine and sent both to a cooperative detective engine and a local support medium.

Data from the neighboring WIDS agents are gathered through secure communications (and vice versa, specific WIDS agents also send data that they collect to other WIDS agents). Further, neighboring data are processed into the cooperative detection engine. The cooperative detection engine sends processed data to the local response medium and to the global response medium.

In several papers related to the WIDPS area [6] [8][9] authors propose an implementation of multiple layer and multiple dimensional systems, which consist of several key elements of IDS and IPS. These kinds of systems have been widely implemented at several levels in wireless and mobile networks. The essence of multilayer and multidimensional systems is the local response of particular system elements, as well as the existence of a global system response (in the case when attack happens). This multilayer system would have components such as:

- Intelligent agents and sensors (intrusion detection)
- Servers (central points for gathering and intelligent data processing, data exchange among other servers, agents, and sensors).

all with the purpose for generating proper prevention actions before any damage in the system occurs.

One of the purposes in the proposed the WIDPS is cross network connections and mutual accessing of distributed data bases. This way of organizing a WIDPS increases the partitioning of database and decreases the so called “zero time” (time counted after first appearance of new type of intrusion until the time when system is ready to protect its data). Having this property, a system is also resistant to a variety of new types of attacks.

The following a section is dedicated to a second type of Concepts which are necessary for the WIDPS solution presented, namely Intrusion Prevention Concepts.

3.4. Prevention in WIDPS

When suspicious activity is detected or an activity is classified as an intrusion, action should be launched. This action is classified as a local response meaning protecting the local host where the WIDS Agents are based or offering even wider protection in the network (if possible). Preventive action can also be defined as action to protect network(s) i.e. other neighboring parts of a network. Further, action can be extended to a wider network area and a higher level of security measures initiated.

In order to differentiate more precisely what intrusion is and what it is not, sensitivity and specificity definitions related to the WIDPS solution are presented next.

3.4.1 Sensitivity, specificity, and accuracy

In a WIDPS sensitivity is observed according to [25]. Therefore, one has four possible cases of attack detection: Intrusion Correctly Detected, False Alarm, Intrusion Missed, and Integrity Correctly Detected. One can make a table of all four states, and define them as: True Positive, False Positive, False Negative, and True Negative, as shown at Table 1.

		Intrusion	
		+	**-**
IDPS	**+**	**TP**	**FP**
Response	**-**	**FN**	**TN**

TP = True Positive = “Intrusion Correctly Detected”

FP = False Positive = “False Alarm”

FN = False Negative = “Intrusion Missed”

TN = True Negative = “Integrity Correctly Detected”

Table 1. Matrix of intrusions and detection

3.4.1.1. Sensitivity

Sensitivity is defined as the true positive rate (for example, the fraction of intrusions that are detected by the IDPS) [25]. Mathematically, sensitivity is expressed as follows:

True Positives / (True Positives + False Negatives)

The false negative rate is equal to 1 minus the sensitivity. The more sensitive an WIDPS is, the less likely it is to miss actual intrusions.

Sensitive WIDPSs are useful for identifying attacks on areas of the network that are easy to fix or should never be missed. Sensitive tests are more useful for "screening"; that is, when you need to rule out anything that might even remotely represent an intrusion. Among sensitive WIDPSs, negative results have more inherent value than positive results do.

3.4.1.2. Specificity

Mathematically, specificity is expressed as follows [25]:

True Negatives / (True Negatives + False Positives)

True negatives represent a WIDPS that is correctly reporting that there are no intrusions. False positives occur when an IDPS mistakenly reports an intrusion when there actually is none. The false positive rate is equal to 1 minus the specificity.

Specific IDPSs offer the greatest utility to the network administrator. For these programs, positive results are more useful than negative results. Specific tests are useful when consequences for false positive results are serious.

3.4.1.3. Accuracy

Often, a trade-off occurs between sensitivity and specificity that varies on a continuum dependent on an arbitrary cutoff point. A cutoff for abnormality can be chosen liberally or conservatively.

However, there are situations when one needs to spend the extra money to achieve both a high sensitivity and a high specificity. Accuracy is a term that encompasses both specificity and sensitivity. Accuracy is the proportion of all WIDPS results (positive and negative) that are correct.

For example, you might need a high-accuracy WIDPS in an area of the network such as the HTTP (Web) Server in Figure 7, which represents a typical corporate network and its protection.

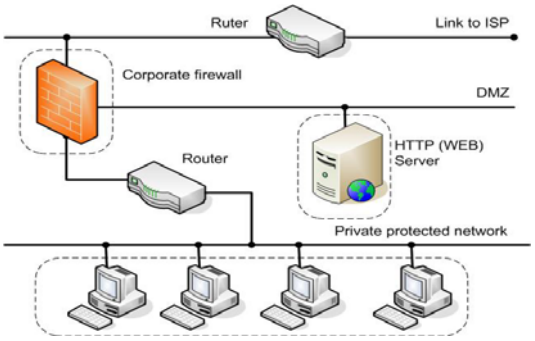

Figure 7. Typical corporate network and its simple layered protection

In this case, the Web server is under constant attack, and it would also cause the most immediate embarrassment and financial loss if compromised. In order to prevent this, the system needs to process any slight anomaly in an automatic manner because of the high traffic volume. In fact, to achieve the highest sensitivity and specificity here, one might need to combine layers of different WIDPS proposed.

3.5. WIDPS and artificial intelligence

As stated earlier, AI systems (Neural Networks, Expert Systems, Fuzzy Logic) can help mimic the way humans think. Human thinking, more precisely, a human DM process is what one wants to achieve in our WIDPS model automatically, so it is appropriate to implement this property of an AI system.

Two types of this AI are clearly distinguished in [28]:

- Strong AI - claims that computers can be made in a way to “think” as humans.
- Weak AI - claims that computers are an important tool in modeling simulations of human behavior.

Systems with AI have greater autonomy in data processing than “classical” computer systems, and also the ability to make an automatic response based on an implemented DM algorithm. An idea of a WIDPS based on a Neural Network model is presented next.

The main focus of Neural Networks usage is to achieve a desirable output to a corresponding input (in other words, train the network to “think” properly). Once the network is trained for n cases (with defined input and output), for n+1 input, it will give the correct (but for network unknown) output. This is achieved by varying the weights on the branches that are entering and exiting neural nodes in the network. Startup weights are changed over the training time, until the network output matches the correct (desirable) output. The core of the Neural Network model is presented at Figure 8.

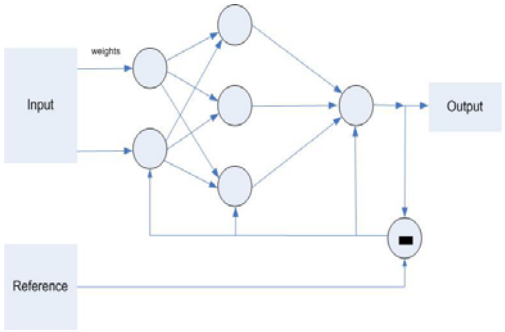

Figure 8. Neural network model

Building WIDPS based on Neural Networks for a particular computer system consists of the following three phases:

- Collecting training data - Data Retrieval in the DM System (i.e. obtain the audit logs for each user for a period of several days. For each day and particular user, form a vector that represents how often the user executed each command).
- Training - Data Modeling and Analysis, Concept Modeling in the DM System (i.e. train the neural network to build the user profile based on these command distribution vectors).
- Performance – Decision in the DM System (i.e., let the network identify the user for each new command distribution vector. If the network's suggestion is different from the actual user, or if the network does not have a clear suggestion, signal an anomaly, and take prevention actions).

These steps, also presented in Figure 9, can be reused over time in future WIDPS systems and the knowledge base can be shared among many servers (used in various networks). As result, one will a have fast growing base and systems with better efficiency and performances.

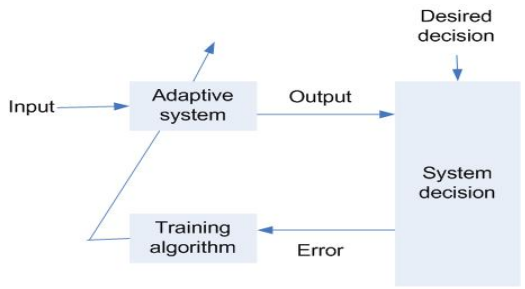

Figure 9. WIDPS solution based on Neural Networks

4. ACHIEVED RESULTS AND FUTURE WORK

Modern systems for intrusion detection and prevention demand greater data processing abilities, because they need to analyze, in a shortest period of time, all of the activities and traffic in the system (and system surroundings) in order to make a proper decision for intrusion detection and prevention. After that, in so called "real time", a system must activate its prevention procedures i.e. its response to attack. The impact of the human intervention in complex computer systems, where one has high data flow and a number of events and activities, is usually much slower (often late, or in worst case impossible) than what the system parameters demand. These facts leads to the conclusion that there is a need for automated DM systems, for which systems like Neural Networks, Fuzzy logic, Expert System, and similar AI systems, can offer automatic reasoning support.

This paper brought together basic approach and criteria for an IDPS (WIDPS specifically), including theory, methodology and measurement to examine and assess the value of Intrusion. Also, it introduces another view that is untraditional and subject to further analysis, changes and improvements. In order to assess the value of a real life network system based on this approach, it is necessary to design all parts of system, develop it, and put it into a real environment. This system environment involves a significant effort which must be taken in next stages of research as follows:

- Analysis of the simulated model in a laboratory environment using tools for simulation.
- Real development of a prototype and work in a controlled environment
- A real system in real environment based on DM System layers on the conceptual level, and artificial intelligence on the operational level.

5. CONCLUSION

In general, the DM mechanism to better differentiate whether something is or is not a legal access/intrusion is a similar problem to many other systems where it is necessary to make a decision based support on a limited set of known details and in limited time. Using DM System layers for the purpose of analyzing and designing efficient automated IDPS offers another opportunity to come up with better solutions. At the beginning, this approach appeared interesting and the first results have demonstrated the basic nature of the problem: introducing DM layers which can also be applied in a human way to bring about a decision. An important possibility is the use of experience with mechanisms that have been introduced in other similar systems where automated DM is also necessary. This is a new way of thinking about IDPS and requires that the work be continued. The next steps are related to building a prototype that will support IDPS concepts in wireless technology and logistic support based on Artificial intelligence.

It can be concluded that IDPS related research, development and usage will be expanded rapidly in the near future. This will occur because, on the one hand, the importance of computers networks and distributed systems (especially including wireless and mobile

networks) grows every day exponentially, and on the other hand, the level of the attacks by malicious people/groups is increasing over time, proportionally to the importance of these systems.

Generally speaking, although theoretical approaches to IDPS have been presented for a long time in scientific circles, their implementation is still not making the necessary progress demanded by companies, industry and everyday computer users. The special emphasis on a WIDPS is because of exponential usage growth of wireless and mobile networks. These types of networks which have unclear borders make it easier for malicious people/groups to perform eavesdropping, jamming, obstructions, and various kinds of new attack types, as well as some new methods of network intrusion.

ACKNOWLEDGMENT

The authors would like to thank to Prof. William Robertson, Dalhousie University, Canada and Prof. Tom Lincoln, University of Southern California, USA, for constructive feedback on this paper.

REFERENCES

[1] Paul Proctor, “The Practical Intrusion Detection Handbook”, Prentice Hall PTR, 2001
[2] Stephen Northcutt, Judy Novak, “Network Intrusion Detection”, New Riders, 2002
[3] Stephen Northcutt, “Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks, Routers and Network Intrusion Detection”, New Riders, July 2002
[4] Randall K. Nichols, Pannos C. Lekkas, “Wireless Security: Models, Threats, and Solutions”, McGraw-Hill, 2002
[5] Merritt Maxim, David Pollino, “Wireless Security”, Osborne McGraw-Hill, 2002
[6] Dragan Pleskonjic, “Wireless Intrusion Detection Systems (WIDS)”, 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, December 8-12, 2003
[7] Dragan Pleskonjic, Veljko Milutinovic, Nemanja Macek, Borislav Djordjevic, Marko Caric: “Psychological profile of network intruder”, IPSI 2006, Amalfi, Italy, March 23-26, 2006
[8] Dragan Pleskonjic, "Wireless Intrusion Detection and Prevention Systems", Invited speaker at IDC IT Security Roadshow 2006, Belgrade, March 16, 2006.
[9] Dragan Pleskonjic: “Protecting wireless computer networks by using intrusion detection agents”, IPSI 2005, Venice, Italy, November 10-13, 2005
[10] Dragan Pleskonjić, Borislav Đorđević, Nemanja Maček, Marko Carić: “Sigurnost računarskih mreža”, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5
[11] Dragan Pleskonjić, Borislav Đorđević, Nemanja Maček, Marko Carić: “Sigurnost računarskih mreža - priručnik za laboratorijske vežbe”, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
[12] Dragan Pleskonjić, Borislav Đorđević, Nemanja Maček, Marko Carić: “Sigurnost računarskih mreža – zbirka rešenih zadataka”, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6
[13] Joshua Wright, “Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection”, [Online document], 2002 Nov 8, Available at: http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf
[14] Yu-Xi Lim, Tim Schmoyer, John Levine, Henry L. Owen. Wireless Intrusion Detection and Response, Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003
[15] IEEE 802.11a/b/g is the set of Institute of Electronics and Electrical Engineers' standards for wireless computer communications. http://standards.ieee.org/getieee802/802.11.html
[16] Berkeley WEP Security Analysis Presentation http://www.drizzle.com/~aboba/IEEE/wep-draft.zip
[17] Yu-Xi Lim, Tim Schmoyer, John Levine, Henry L. Owen, “Wireless Intrusion Detection and Response”, Proceedings of the 2003 IEEE, Workshop on Information Assurance, United States Military Academy, West Point, NY June 2003
[18] Anup K. Ghosh, Aaron Schwartzbard, „A Study in Using Neural Networks for Anomaly and Misuse Detection“, Proceedings of the 8th USENIX Security Symposium, August 23-36, 1999, Washington, D.C.
[19] A.K. Ghosh, A. Schwartzbard, and M. Schatz. “Learning program behavior profiles for intrusion detection”, Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring. USENIX Association, April 11-12 1999
[20] Yongguang Zhang, Wenke Lee, “Intrusion detection in wireless ad-hoc networks”, Proceedings of the 6th annual international conference on Mobile computing and networking, p. 275 – 283, Boston, Massachusetts, United States, 2000
[21] http://snort-wireless.org [Online resource]
[22] http://www.loud-fat-bloke.co.uk/ [Online resource]
[23] Sanida Omerovic, Saso Tomazic, Charles Milligan, May 2006 Report on “Concept Modeling,” for Sun Microsystems, USA ,
[24] Tim Berners-Lee, James Hendler and Ora Lassila, “The Semantic Web,” Scientific American. Vol. 284, no. 5, pp. 28-37. May 2001
[25] Cyrus Peikari, Seth Fogie, "Maximum Wireless Security", Sams Publishing, 2002
[26] Sanida Omerovic, Tatjana Filimonova, Saso Tomazic, “Automatic Translation of Natural Languanges with E-speranto,” Proceedings of YU-INFO 2006, Kopanik, Serbia
[27] Matt Bishop, “Computer Security: Art and Science”, Addison Wesley Professional, 2003
[28] Mark Kantrowitz, “The AI Frequently Asked Questions,”maintained by Ric Crabbe and Amit Dubey, available online at www.faqs.org/faqs/ai-faq/general/, January 17, 2003
[29] Thomas Friedman, “Lexus and The Olive Tree,” Anchor Books, USA
[30] Ognjen Scekic, Djordje Popovic, Mina Micanovic, Veljko Milutinovic, IPSI Belgrade team report 2006 on “Concept Modelling,” for Sun Microsystems, USA
[31] Ambareen Siraj, Susan M. Bridges, Rayford B. Vaughn, “Fuzzy Cognitive Maps for Decision Support in an Intelligent Intrusion Detection Systems,”, IFSA World Congress and 20th NAFIPS International Conference, 2001. Joint 9th
[32] Hiren Shah, Jeffrey Undercoffer, and Anupam Joshi, “Fuzzy Clustering for Intrusion Detection,”, Fuzzy Systems, Proceedings of Fuzz-IEEE 2004.
[33] Aly El-Semary, Janica Edmonds, Jesus Gonzalez, and Mauricio Papa, “A Framework for Hybrid Logic Intrusion Detection Systems,” Fuzzy Systems, Proceedings of Fuzz-IEEE 2005
[34] Robert Fuller, “Neural Fuzzy Systems,” In Advances in Soft Computing Series. Springer-Verlag, Berlin/Heildelberg, 2000. ISBN : 3-7908-1256-0.
[35] James P Anderson, “Computer Security Threat Monitoring and Surveillance.”, James P. Anderson Co., Fort Washington, Pa., 1980.
[36] Oleg Kachirski, Ratan Guha, "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks," kmn, p. 153, IEEE Workshop on Knowledge Media Networking (KMN'02), 2002.