AISF – A Proposal for Standard Intrusion Signature Representation

ARTUR R. ARAUJO DA SILVA, MARCELO DE SOUZA, ADRIANO M. CANSIAN
ACME! Computer Security Research Lab.
UNESP – Universidade Estadual Paulista
15055-000, São José do Rio Preto, SP, BRAZIL
{artur, marcelo, adriano}@acme-ids.org – http://www.acme-ids.org

Abstract: - Some efforts must be devoted to research new attack detection methods, so that they favor the intrusion detection and counter-measure procedures. This paper proposes an enhancement over network-based intrusion signatures handling, from storage to analysis. It presents a new intrusion signature representation model named AISF (ACME! Intrusion Signature Format), based on the XML specification. With AISF, the process of storing and analyzing information about intrusion signatures becomes a standardized and less difficult process.

Key-Words: - network, security, intrusion, IDS, signature, XML

1 Introduction

The need for a more efficient and uninterrupted monitoring of the activities pertinent to a network caused the appearance of software denominated intrusion detection systems, responsible for seeking attack attempts that were thrown against a network, generating files with the diagnosed occurrences, so that the damages can be prevented or repaired later.

This paper will present an intrusion signature representation format, named AISF (ACME! Intrusion Signature Format). The main goal of AISF is a clear definition of the intrusion signatures codification, storage and analysis processes. Thus, any intrusion detection related entity or person can commit into a standard for attack signatures reporting and analysis.

2 Computer network intrusion detection

This section presents the main concepts required for further understanding about computer network intrusions and their detection procedures, essentially regarding recognition of intrusion signatures. Therefore, the first step is to strictly define what a computer network intrusion is, and how intrusion detection systems can trace and possibly stop them.

2.1 Computer network intrusions

Computer network intrusions (or attacks) are defined by Heady et al. [1] as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource", disregarding the success or failure of those actions.

Three types of attacks are most commonly known to happen on a computer network environment: system scanning, DoS (denial of service), and system penetration [2]. Next, there is a brief description about these attacks:

- Scanning Attacks occur when an attacker probes a target network or system by sending different kinds of packets.
- Denial of Service Attacks attempt to slow or shut down targeted network systems or services.
- Penetration Attacks are the unauthorized acquisition and/or alteration of system privileges, resources, or data.

A typical attack scenario is well-known and simple: at a first step, intruders scan the network or the target computer, searching for specific vulnerabilities in order to establish a target address database containing potential candidates to be attacked. When vulnerabilities are found, the attacker tries to explore them, checking if the expected failures really exist in that box [3].

There are different approaches to detect the attack classes described above, as they require different types of analysis and response. The next subsection will describe how these intrusion detection capabilities are built.

2.2 Network intrusion detection

Intrusion detection is defined in [4] as "the problem of identifying people who are using a computational system without authorization (i.e., 'crackers') and those who have legitimate access to the system but are abusing their privileges (i.e., 'insiders')".

A network-based intrusion detection system, hereafter referred as IDS, can be defined as software or hardware mechanisms in which the process of

monitoring events happening in a computer network is automatic.

Current approaches for network intrusion detection can be broadly classified into two categories:

- Anomaly detection is based on the premise that intrusive activity often manifests itself as an abnormality. The usual method here is to detect statistically large variances on normal utilization metrics.

- Misuse detection attempts to encode knowledge about the attacks as well defined patterns, monitoring for the occurrence of these patterns.

Intrusion signatures, the main focus of this paper, are the key components for misuse-based detection techniques. Thus, our work concentrates on this approach, knowing that it is related to the definition and precise observation of intrusive behaviors, and that there is always a component of misuse-based detection in the majority of IDS, since isolated statistical techniques are not adequate to determine every security event.

The next subsection will bring some further discussion about intrusion signatures, showing their unanswerable importance in the world of intrusion detection.

2.3 Intrusion Signatures

The attack scenario described in subsection 2.1, as well as any similar one, is divided into patterns that can be tracked down and observed in any intrusive action. Such patterns consist of what are called 'intrusion signatures', the primary resource of information for an IDS.

Formally speaking, [5] defines an intrusion signature as a specification of aspects, conditions, arrangements and inter-relationships between events that mean an attack, a breaking of access, another type of abuse or any attempt of these.

Thus, for every intrusion event there may be an IDS mechanism able to match the intrusion signatures. This can be as simple as a pattern match.

With all this knowledge, it is possible to say that an IDS functionality can be enhanced when its intrusion signatures handling mechanism is improved. Under this situation we are motived to define the AISF model.

3 The AISF model

AISF can be shortly defined as a proposal for standardizing the acts of coding, storing, processing, exchanging and reporting intrusion signatures, in such a way that they can be used freely among the systems and entities involved in detection of attacks.

Technically speaking, AISF (ACME! Intrusion Signature Format) is a data structure comprised of an independent set of modules, which contains intrinsically related information that allows the accurate and concise reporting of attack signatures, listing from descriptive characteristics to implicit details of network protocols.

Another employment for AISF is the possibility of being used by less complex systems, taking into account signature analysis, like a simple scan detector, or a network dump analyzer that can compare the dumps with the AISF objects. Alert reporting can be highly facilitated, once AISs are generated with descriptive texts, besides the own useful contents of signatures.

3.1 AISF design using XML

The AISF organization is based on the XML (Extensible Markup Language) specification [6], which supplies after all, simplicity, adaptability, high portability, flexible use and maintenance. XML is springing up all over the Internet as a means to create standard data formats for the exchange of information between systems, irrelevant of their technology.

An AISF instance will be referred from now on as an AIS, or AISF object, which consists of a properly formatted XML document containing important data of an intrusive event. For each event there will be only one AISF object, which can be revised and generate new versions.

In the next section there is the complete definition of the AISF modules and some description of its fields. It is important to notice that the modules described will serve for visualization purposes only, since the specification itself follows XML patterns.

3.2 The AISF data structure

The first and most important AISF module consists of the Signature Identification Module (Table 1). It is responsible for the identification of an event, as well as some details about the model itself.

Name	Description
Version	Identification of the AISF model.
ID	Identifies the attack described by the AIS.
Name	Common name of the intrusion event
Serial Number	Number that describes the AIS version, based on the generation date
Credits	AIS authors (entity or person)
Next Module	Identifies the next AISF module

Table 1 – *Signature Identification Module*

This initial module is the only one that should obligatorily contain all of its fields properly filled. Below there is a list of the fields and its functions:

Note that the Next Module fields must contain the name of the subsequent data module. If this one does not exist, the field should be left blank.

The second module (Table 2), Signature Information Module**,** is responsible for more descriptive information about the attack. This module, as well as the following one, is optional.

Name	Description
Module Length	Number of module fields
Security Level	Number (from 0 to 100) describing how dangerous this event can be;
Category	Intrusion event category, like scan, DoS, or interactive attack
Description	AIS event description
Other Ids	Reference IDs for this attack, like CVE [15] or BugTraq ID [16];
Impact	What is the consequence of this event;
Attack Scenario	What is needed for this attack to happen
Target System	Systems that are more commonly affected by this intrusion
Next Module	Identifies the next AISF module

Table 2 – *Signature Information Module*

The third module (Table 3) pertaining to the informative modules class is the Signature Characteristics Module, which can report some attack inherent information.

Name	Description
Module Length	Number of module fields
Ease of Attack	Number (from 0 to 100) describing how easily this attack can be realized;
False Positive Level	Approximation percentage of false positives this event can trigger;
False Negative Level	Approximation percentage of false negatives this event can trigger;
Recommended Actions	Recommended preventive and/or corrective actions to take;
Next Module	Identifies the next AISF module

Table 3 – *Signature Characteristics Module*

The following modules are easily understandable, representing the more technical side of an attack signature. They represent required information for intrusion detection, like data link, network and transport layers data, besides the payload of the session. In the present version of AISF, there are just the more acquainted protocols of these layers, like Ethernet, IP, ICMP, TCP and UDP. Nothing interferes in the addition of other protocols, like PPP, IPv6, application protocols (RPC, HTTP) [17], among others.

The next module, Data Link Protocols Module (Table 4), refers to Ethernet data link protocol data.

Name	Description
Module Length	Number of module fields
Source Address	Source MAC address
Destination Address	Destination MAC address
Next Module	Identifies the next AISF module

Table 4 – *Data Link Protocols Module for Ethernet*

Next, there is the Network Protocols Module (Table 5), referring to inherent network layer data, and in the case of the TCP/IP suite, the IPv4 protocol.

Name	Description
Module Length	Number of module fields
Type of Service	IP packet type of service
Fragment ID	Fragment identification number
Flags	IP protocol flags
Fragment Offset	Packet fragment offset
TTL	IP packet time-to-live
Source Address	IP source address
Destination Address	IP destination address
Options	Packet options
Next Module	Identifies the next AISF module

Table 5 – *Network Protocols Module for IPv4*

The following three tables (Tables 6 to 8) demonstrate how AISF can be used to keep data regarding transport and control layers, trough the Transport and Control Protocols Module. TCP, UDP and ICMP protocols header information used in the attack can be described by these modules.

Name	Description
Module Length	Number of module fields
Source Port	TCP source port
Destination Port	TCP destination port
Sequence Number	Packet sequence number
Acknowledge Number	Packet acknowledge number
Data Offset	Packet data offset

Flags	TCP flags
Window	Window size
Urgent Pointer	Urgent pointer
Options	TCP options
Next Module	Identifies the next AISF module

Table 6 – *Transport and Control Protocols Module for TCP*

Name	Description
Module Length	Number of module fields
Source Port	UDP source port
Destination Port	UDP destination port
Next Module	Identifies the next AISF module

Table 7 – *Transport and Control Protocols Module for UDP*

Name	Description
Module Length	Number of module fields
Type	ICMP Type
Code	ICMP Code
ID	ICMP ID
Sequence	ICMP Sequence number
Next Module	Identifies the next AISF module

Table 8 – *Transport and Control Protocols Module for ICMP*

AISF Payload Information Module (Table 9) is one of the most important. There can be stored information regarding the attack session packets payload. It is considerably useful to describe the interactive attacks, like the ones that explore 'buffer overflows', where a great number of 'NO-OP' instructions can be found. Thus, with this module, one can describe the payload size, where exactly the important data is found in this payload and other details that aid in the search for intrusion tokens. Still in this module, on the Contents field, markup tags are defined to facilitate string matching, like case sensitiveness and data order.

Name	Description
Module Length	Number of module fields
Size	Payload size
Offset	Payload offset to start pattern matching
Depth	How far to search into the packet
Contents	Payload contents
Next Module	Identifies the next AISF module

Table 9 – *Payload Information Module*

4 Conclusion

This work has shown how to create a standard intrusion signature representation model using the XML specification. Throughout this paper, the importance of intrusion signatures and its use by intrusion detection systems was presented. Special attention has been devised to the need for a unified way of storing, processing, analyzing and reporting intrusion patterns.

The present article has also shown the modularization of the model as a very important feature. It provides possibility for different systems to share information related to intrusive events. This modularization, along with the power of XML makes easy the parsing of AISs, diminishing the process overhead, which is a good desirable feature.

References:

[1] Heady, R.; Luger, G.; Maccabe, A. and Servilla, M., The architecture of a network level intrusion detection system, *Technical Report -University of New Mexico*, 1990.

[2] Bace, R. and Mell, P., Intrusion Detection Systems, *NIST Special Publication on Intrusion Detection Systems*, 2001.

[3] Farmer, D. and Venema, W., Being Prepared for Intrusion, *Dr. Dobb's Journal*, 2001.

[4] Spafford, E.; Balasubramaniyan, J.S.; Fernandez, J.O.G.; Isacoff, D. and Zamboni, D., An architecture for intrusion detection using autonomous agents, *COAST Technical Report 98/05*, 1998.

[5] Cansian, A. M., Desenvolvimento de um Sistema Adaptativo de Detecção de Intrusos em Redes de Computadores, *PhD Thesis presented to the Physics Institute of São Carlos – São Paulo University,* 1997.

[6] World Wide Web Consortium, XML (Extensible Markup Language) 1.0, *http://www.w3.org/TR/2000/REC-xml-20001006*, last seen June 29, 2002.