Proactive Security Monitoring in a Policy Managed Network*

Till Dörges, Klaus-Peter Kossakowski
{td,kpk}@pre-secure.de
PRESECURE Consulting GmbH

Mar 20, 2006

Abstract: *The complexity of today's networks can only be handled by the use of more and more sophisticated approaches and tools. A very promising approach is centralized policy based management. This means the policy for the entire administrative domain is managed from a single point.*

But defining and distributing a policy is only half the work as the policy has to be enforced – otherwise establishing a policy is pointless.

This paper presents a tool for the continuous monitoring of networked systems and applications for the compliance with a given policy. The Proactive Security Monitor (PSM) employs proactive and reactive methods for monitoring the network. Apart from the "usual" alert overview it also provides support for semi-automatic changes of the current policy. This can be useful if evidence suggests that a network is under stress and immediate reaction seems advisable.

The Proactive Security Monitor is part of POSITIF*, which itself will provide a framework and tools for centralized policy based management of networked systems and applications (see [10]).*

Keywords: *Proactive Security Monitor, PSM,* POSITIF*, Policy, Policy Based Management, Monitoring, Policy Enforcement, IDS*

1 Introduction

Policy based management is one possible solution to the ever growing complexity of today's computer installations. POSITIF will[1] supply administrators with a framework and tools for centralized management of computer networks. The schematic workflow for managing a network by POSITIF means is indicated in figure 1.

The two global key components for POSITIF are the System Description Language (SDL) and Security Policy Language (SPL). Using these the administrator(s) of a given network describe(s) the

system including network topology, connected hosts with operating systems, installed applications etc. as well as the

policy stating allowed and forbidden actions.

*This work is part of the POSITIF project, funded by the EC under contract no. IST-2002-002314

[1] POSITIF still is an ongoing project

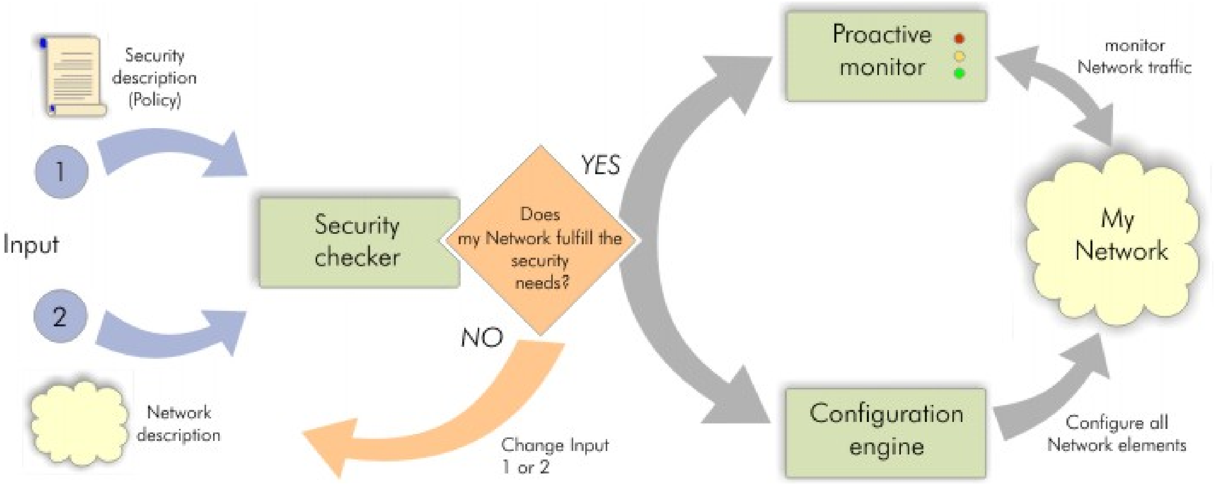

Figure 1: Schematic Workflow for Managing a Network with POSITIF

These descriptions will then be syntactically and semantically verified. If verification is successful the policy will be applied, i. e. automatically deployed to all networked equipment managed by POSITIF. For a more thorough discussion of policies in general see for example [1]. And for a more detailed description of the inner workings of POSITIF see [10]. After the deployment phase the PSM steps in because from now on compliance of all activities with the given policy needs to be monitored.

The remainder of this paper is structured as follows: Section 2 will explain the PSM from a top level view focusing on its external interfaces. Following (section 3) is a detailed description of all the internal components of the PSM. Section 4 will give a short example. In section 5 related works will briefly be discussed. The paper ends with section 6 providing outlook and conclusion.

2 Specification of the Proactive Security Monitor as Black Box

The Proactive Security Monitor can be seen as a black box (figure 2).

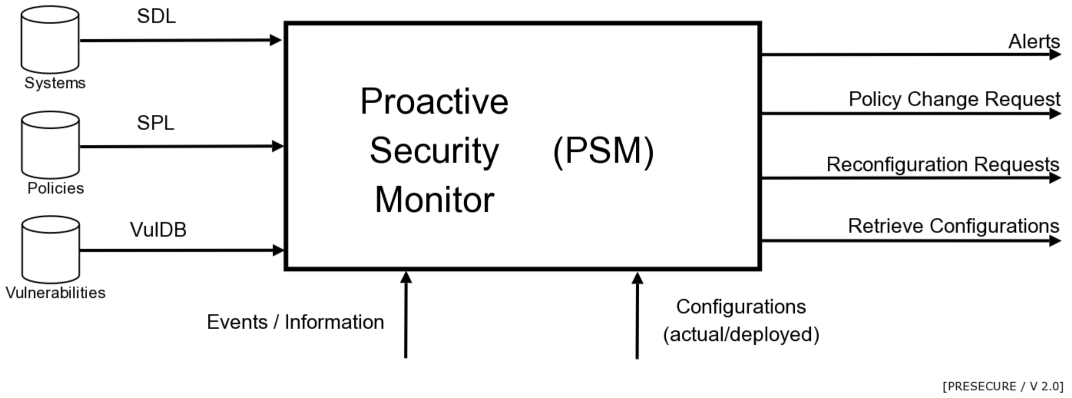

Figure 2: PSM as a Black Box

The in- and outputs are as follows:

SDL description of the systems to be observed and checked;

SPL description of the policies to be enforced and controlled;

VDL or VulDB description of the vulnerabilities to check for;

Events / Information all incoming information that is processed by the PSM in order to evaluate the networks and connected systems with respect to the descriptions available;

Configurations the PSM will continuously check whether the configurations actually running on a security block have not been altered after their deployment;

Alerts indication that a forbidden status – according to the effective policies – has occurred;

Policy Change Requests requesting a policy change throughout all the networks and connected systems (if supported) based on the change in status;

Reconfiguration Requests under certain circumstances altered configurations should be reset automatically;

Retrieve Configurations this triggers the retrieval of both actual and deployed configurations for each security block.

It is important to note that the PSM features clear APIs both for inbound and outbound data. As message passing protocols either web services (see [17]) or BEEP ([12]) are used. The messages sent by the PSM generally use IODEF (see [4]). As for the inputs (SDL, SPL, ...) please see [10].

3 Detailed Specification of the Proactive Security Monitor

Depicting the next level of detail (figure 3), internal components of the PSM, which might themselves be distributed systems, become visible:

IDS a sensor, most namely an Intrusion Detection System, which is observing events and information, sending it up the chain.

SEM a lightweight IDS, suitable for embedded computers.

IDS and SEM Correlation a collector of all information from IDS and SEM components, as they are very similar to each other. In addition to collection correlation is also part of this component.

Its design was stronly influenced by [15].

PSC the Proactive Security Scanner actively tries to retrieve and collect information about systems in order to conduct further analysis on different levels to identify existing vulnerabilities and other risks. Some PSCs – operating on different technical levels of sophistication – will most probably exist.

PVS Policy Violation Sensor is another passive sensing component which will recognize policy violations not already covered by the IDS and SEM components.

PCC the Proactive Configuration Checker will continuously verify that the configurations of the security blocks haven't changed.

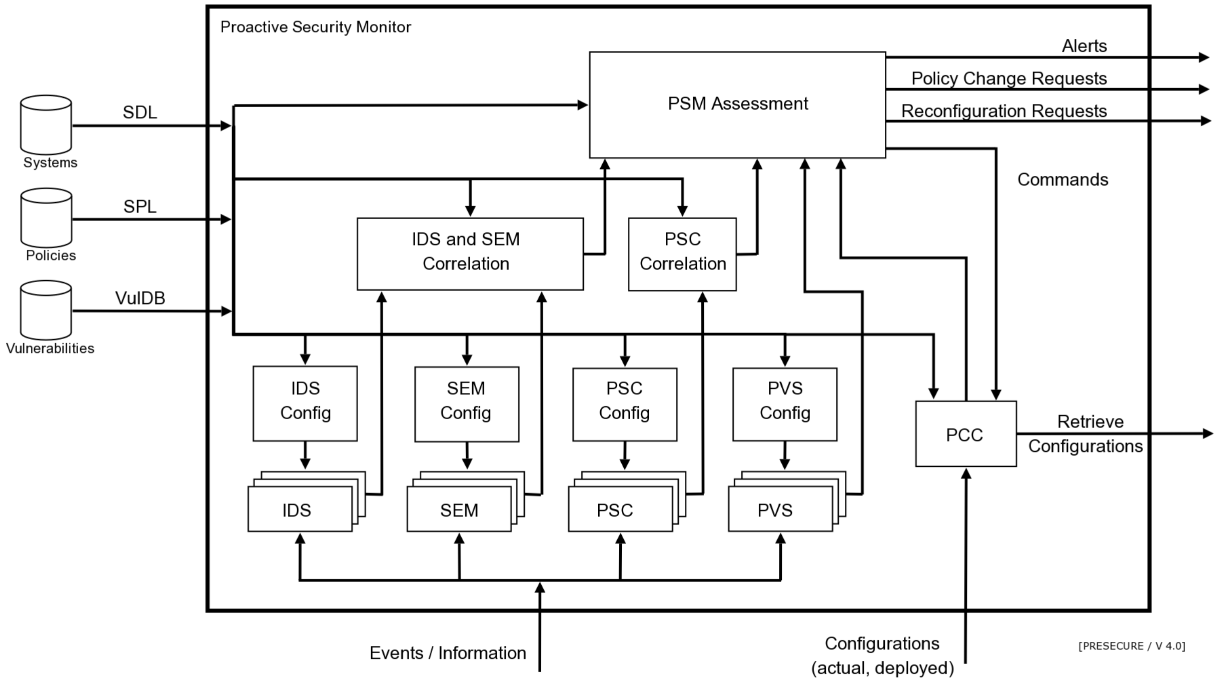

Figure 3: Internal PSM Components

PSC Correlation again, as many information might actually point or relate to the same root cause, a collection and correlation of retrieved events is necessary.

PSM Assessment based on the correlated information available from the reactively oriented IDS and SEM components and the proactive oriented PSC components a correlation on a higher level needs to be established. As this effectively results in two major kinds of outputs – alerts and policy change requests – this component needs to provide the ultimate assessment (in terms of the PSM). From the PSM perspective, it is not defined, whether its output is handled automatically or manually. This decision will reside with the management responsible for the deployment of the POSITIF framework, while the framework will allow for automation according to the work plan.

Key approaches for its implementation are similar to those described in [13] and [2].

Unfortunately this paper can only briefly touch the inner workings of the PSM not to mention the entire POSITIF framework. For more details please refer to [10].

Table 1 shows a comparison of all the different sensors currently utilized by the PSM. Please note that thanks to the flexible architecture of the PSM new sensor types can easily incorporated.

Sensor Type	Behavior	Recognizes
IDS/SEM	reactive	Attacks / Policy Violations
PVS	reactive	Attacks / Policy Violations
PCC	proactive	Misconfigurations, Potential Attacks and Potential Policy Violations
PSC	proactive	Vulnerabilities, Potential Attacks and Potential Policy

Table 1: Comparison of the different sensor types found inside the PSM

As the SPL is strongly based on CIM (see [5]) and PCIM (see [7] and [6]) it has to be noted that several different policy types need to be distinguished. The concept of PSM sensors, however, is orthogonal to the policy types.

Again, quite a bit of effort was devoted to specifying clear APIs between all components inside the PSM. This is absolutely necessary as the PSM is not only monitoring distributed systems but is distributed in itself. The means of transport (BEEP [12]) as well as the message formats (IDMEF [3], IODEF [4]) were chosen to match the external APIs.

4 Examples

When operating the PSM to monitor a given policy one has to be aware of the capabilities of the different sensor types. Table 2 gives a few potential incidents and shows which sensor type is able to detect it.

Incident	**IDS/SEM**	**PVS**	**PCC**	**PSC**
port scan	yes	no	no	no
cmd32.exe exploit	yes	yes	no	yes
reach. of forbidden serivce	yes	yes	yes	yes
denial of allowed service	no	yes	yes	yes
faul ty configuration	no	no	yes	yes
write to forbidden dirs	yes	yes	yes	yes
forbidden attachments	no	yes	no	yes
succ. auth, wrong method	no	no	yes	yes
SSL conn., wrong certs	no	yes	no	yes

Table 2: Policy Violations and Attacks are detected by different sensor types

SDL and SPL can be constructed using a graphical tool. The internal representation, however, is XML. The following example (see figures 4 and 5) is not overly complex but it should give at least a rough idea of the nature of SDL and SPL. It describes part of a firewall with interfaces and part of the filtering rules.

```
<firewall id="Firewall">
        <interface id="eth0" number="1" technology="Ethernet" connector="RJ45"
                   protocol="10-100BaseT">
                <addr type="ipv4" netmask="255.255.255.128">1.2.3.4</addr>
        </interface>
        <interface id="eth1" number="2" technology="Ethernet" connector="RJ45"
                    protocol="10-100BaseT">
                <addr type="ipv4" netmask="255.255.255.240">1.2.3.5</addr>
        </interface>
</firewall>
```

Figure 4: SDL example describing part of a firewall

5 Related Works

There are far too many related projects and products in order to mention all of them. This section will just try to name a few examples with a strong bias on Open Source projects. From the

```
<xCIM_FilterEntry>
        <CIM_FilterEntryBase.Name>access1</CIM_FilterEntryBase.Name>
        <IsNegated>false</IsNegated>
        <TrafficType>IPv4</TrafficType>
        <MatchConditionType>Source Address and Mask</MatchConditionType>
        <MatchConditionValue>1.2.3.4/255.255.255.255</MatchConditionValue>
        <Action>Permit</Action>
        <DefaultFilter>false</DefaultFilter>
</xCIM_FilterEntry>
```

Figure 5: SPL example describing part of a filtering rule

monitoring point of view Snort [11] and Nagios [8] certainly are related; their focus, however, is too network-centric. Further interesting projects include [9] and [16]. But [16] realizes only the correlation part of the PSM and [9] does not provide a coherent integration with an entire management framework as the PSM does with POSITIF.

6 Outlook and Conclusion

This paper presented an overview of the Proactive Security Monitor that is being realized as part of the EC-funded POSITIF project. The PSM monitors a given network as specified by the SDL for compliance with a given policy as specified by the SPL. One of the most important features of the PSM is the ability to integrate information from many different sensor types. This is achieved through a modular architecture. The PSM is able to provide assessment of the current network health status.

Looking ahead the first goal certainly is to finish the PSM along with the complete POSITIF project. This is expected for the year 2007. Possible areas of future investigation for the entire project are support for more dynamic polices as well as support for a more heterogeneous structure of administrative domains. Just looking at the PSM it would be interesting to identify the requirements for integration with other monitoring and management tools, e. g. [14].

References

[1] Matt Bishop. *Computer Security: Art and Science*. Addison Wesley, March 2003.

[2] Yao-Min Chen and Yanyan Yang. Policy management for network-based intrusion detection and prevention. In *IEEE Network Operations and Management Symposium*, 2004.

[3] David A. Curry, Hervé Debar, and Benjamin Feinstein. Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition. http://www.ietf.org/internet-drafts/draft-ietf-idwg-idmef-xml-15.txt, 2005. IETF internet draft - work in progress.

[4] Roman Danyliw, Jan Meijer, and Yuri Demchenko. The Incident Data Exchange Format Data Model and XML Implementation. http://www.ietf.org/internet-drafts/draft-ietf-inch-iodef-04.txt. IETF internet draft - work in progress.

[5] Distributed Management Task Force, Inc. Common Information Model. http://www.dmtf.org/standards/cim/, 2005.

[6] B. Moore (Editor). RFC 3460: Policy Core Information Model (PCIM) Extensions. http://www.rfc-editor.org/rfc/rfc3460.txt, January 2003.

[7] B. Moore, E. Ellesson, J. Strassner, and A Westerinen. RFC 3060: Policy Core Information Model – Version 1 Specification. http://www.rfc-editor.org/rfc/rfc3060.txt, February 2001.

[8] Nagios. http://www.nagios.org/.

[9] OSSIM – Open Source Security Information Management. http://www.ossim.net/.

[10] POSITIF. Policy-based Security Tools and Framework. http://www.positif.org/.

[11] Martin Roesch. Snort – Lightweight Intrusion Detection for Networks. In *13th Systems Administration Conference (LISA '99) Proceedings*. Usenix Association, November 1999.

[12] M. Rose. RFC 3080: The Blocks Extensible Exchange Protocol Core. http://www.rfc-editor.org/rfc/rfc3080.txt, March 2001.

[13] Ambareen Siraj, Rayford Vaughn, and Susan Bridges. Decision making for network health assessment in an intelligent intrusion detection system architecture. *International Journal of Information Technology & Decision Making (IJITDM)*, 3(2):281–306, 2004.

[14] SIRIOS – Vorfallsbearbeitungssystem für Computer-Notfallteams. http://www.cert-verbund.de/sirios/, 2005.

[15] Fredrik Valeur, Giovanni Vigna, Christopher Krügel, and Richard Kemmerer. A Comprehensive Approach to Intrusion Detection Alert Correlation. *IEEE Transactions on Dependable and Secure Computing*, 1(3):146–169, July-September 2004.

[16] Yoann Vandoorselaere. Status of correlation within prelude. http://prelude-ids.org/pipermail/prelude-user/2006-March/001511.html, March 2006.

[17] W3C. Web services activity. http://www.w3.org/2002/ws/.