The current issue and full text archive of this journal is available at
www.emeraldinsight.com/0968-5227.htm

Incident response requirements for distributed security information management systems

Sarandis Mitropoulos, Dimitrios Patsos and Christos Douligeris
Department of Informatics, University of Piraeus, Piraeus, Greece

Abstract

Purpose – Security information management systems (SIMs) have been providing a unified distributed platform for the efficient management of security information produced by corresponding mechanisms within an organization. However, these systems currently lack the capability of producing and enforcing response policies, mainly due to their limited incident response (IR) functionality. This paper explores the nature of SIMs while proposing a set of requirements that could be satisfied by SIMs for the efficient and effective handling of security incidents.

Design/methodology/approach – These requirements are presented in a high-level architectural concept and include policy visualization, system intelligence to enable automated policy management, as well as, data mining elements for inspection, evaluation and enhancements of IR policies.

Findings – A primitive mechanism that could guarantee the freshness and accuracy of state information that SIMs provide in order to launch solid response alarms and actions for a specific incident or a series of incidents is proposed, along with a role based access control administrative model (ARBAC) based on a corporate model for IR. Basic forensic and trace-back concepts that should be integrated into SIMs in order to provide the rich picture of the IR puzzle are also examined.

Practical implications – The support of policy compliance and validation tools to SIMs is also addressed.

Originality/value – The aforementioned properties could greatly assist in automating the IR capability within an organization.

Keywords Information systems, Data security

Paper type Research paper

1. Introduction

The complexity of an incident response (IR) capability within a corporate environment dictates the need for adaptive security policies, since every security incident has to be treated differently according to a variety of factors that rule their significance, magnitude and side effects. So far, such policies have been formulated manually and have been applied with the assistance of first-generation security devices (also called single-purpose security devices), where critical decisions always required the human involvement. With the launch of next-generation security management tools, like security information management systems (SIMs), it seems that one can automatically adjust response actions to a variety of security incidents.

Currently, SIMs are providing a unified platform for integrated security management. Nevertheless, the automated responses to security incidents could be further improved, therefore increasing the overall enforcement of an enterprise-wide

This paper has been partially supported by GSRT under a PENED grant and by the IST FET Coordination Action ACCA (006475).

Information Management & Computer Security
Vol. 15 No. 3, 2007
pp. 226-240

0968-5227
DOI 10.1108/09685220710759568

security policy. The primary concern of this paper is to advance the way SIMs are evolving, taking under consideration that SIMs are an emerging technology.

More specifically, in this paper, we explore and describe the basic services provided by a SIM (like monitoring, event/data correlation, and root-cause analysis) and we propose the basic characteristics that should be incorporated in order to assist for automated responses, like policy visualization, administrative role-based access control, system intelligence to enable automated policy management as well as data mining elements for inspection, evaluation and enhancements of IR policies. We continue by proposing mechanisms that guarantee the freshness and accuracy ("liveness") of state information that SIMs provide in order to launch solid response alarms and actions for a specific incident or a series of incidents. This is very important since network security devices handle volatile and perhaps falsified data, or data that describe a state that has changed while the original state descriptive data are being delivered to the SIM. We later propose a role based access control administrative model (ARBAC) based on a corporate model for IR. Finally, we examine basic forensic and trace-back concepts that should be integrated into SIMs in order to provide the big-picture of the IR puzzle.

2. The problem space

During the last decade, there have been tremendous advances in information security technologies that now form a necessary part of every modern IT environment. Firewalls (FWs) are perhaps the most celebrated ones, followed by intrusion detection systems (IDSs), content filtering (CF) technologies and dozens of others. The purpose of these systems is either to protect the corporate assets or detect the presence of a security incident, while providing limited response actions.

IR, on the other hand, is the process that intends to minimize the damage from security incidents and malfunctions that inevitably occur in a corporate environment, and monitors and learns from such incidents (BSI, 1999). IR has been always treated as an important aspect of every corporate information security policy, but there has been little progress in developing a solution or a standard that could automatically handle every security incident.

The obvious reason is that, unlike single-purpose security products (like FWs that enforce access control policies at the network perimeter, IDSs that perform pattern recognition of known attacks and inform the system administrators or antivirus software (AV) that checks every file against a database of signatures) a unified solution would require the processing power, intelligence, storage requirements, etc. of nearly all current and – probably – future security systems. More than this, these systems lack the capability of enforcing adaptive security policies, in the sense that they cannot easily communicate with other security systems, decide and automatically coordinate the appropriate response actions.

Apart from that, it is still at question how a single-purpose security device should handle a blended attack. Blended attacks contain two or more attacks merged together to produce a more potent attack (Hansman, 2003). For example, a traditional FW cannot detect the presence of a virus in a network connection but can hopefully log this – like any other – connection. On the other hand, a traditional host IDS or AV solution that could detect the virus payload cannot tell where this connection really originates from, but can also produce a detailed security log for this virus. In order to respond to

this incident, an intelligent platform should correlate these two security logs and alert the system administrators. Keeping similar analogies, the problem is vital for complex corporate environments, where security events are related to complex systems and platforms. Like information is data in context, security events are security logs in context (of a given environment), and security incidents are security events in context (of certain correlation conditions).

One of the most recent advances, in the context of information security management, are the so-called SIMs that, under certain conditions, could provide the tactical solution to the automated IR issue. SIMs were originally developed to counter the log-correlation issue but provide some interesting features like policy compliance checking, security policy visualization, forensic information, etc. that are briefly explained in the following sections and could be used in enforcing an IR policy within an organization.

Our aim is to highlight the IR policy requirements that a SIM should provide, serving as a single point of response coordination.

3. SIM features

A SIM provides six fundamental functions regarding security-related information, as shown in Figure 1, that are briefly explained in the following sections.

3.1 Audit log collection

The overall benefit of SIMs is based on their ability to read and consolidate audit logs, thus understanding security-related information. In modern corporate environments, security-related information comes from various sources: platforms (e.g. Windows, UNIX/Linux, proprietary operating systems, etc.), systems (e.g. servers, desktops, PDAs, laptops, etc.), applications (ERP, Database, CRM, Groupware, mail, custom, etc.), security systems (e.g. FWs, IDSs, AV, vulnerability scanners, etc), as well as, miscellaneous other sources (e.g. networks). Moreover, information regarding a security incident can be found in log files lying in completely different systems.

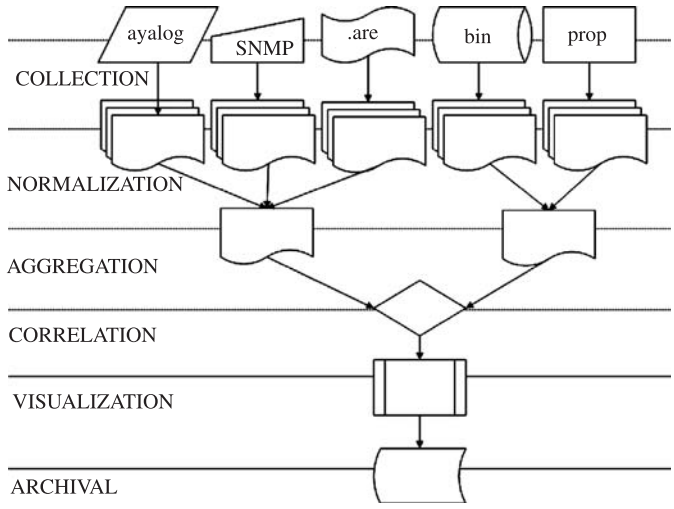

Figure 1.
SIM system features

For example, information regarding a worm could be possibly logged by the gateway (or the desktop) AV system, the operating system and, possibly, the IDSs or the FW as mentioned before. The first fundamental design concept of a SIM is that it should facilitate security log collection from heterogeneous sources and facilitate security knowledge. Finally, different systems log the same security incident differently. For example, a Windows web server log file might contain an HTTP connection message. The same information comes from the FW as "successful connection to TCP port 80."

3.2 Normalization

By default, most systems are not configured to produce any security logs. Even if the case is that all systems were configured to log specific information, the issue is how to extract the potential security information since there is no globally accepted standard for security logging.

For example, UNIX/Linux systems mainly use the syslog technology, Windows systems use the.evt format, network devices use the SNMP technology to send and receive traps, while many applications use text or proprietary binary formats to log security information. Therefore, the second fundamental design concept of a SIM is that it should be able to normalize the various formats and sizes of log information collected. Typically, the form of a normalized security log is a $n \times 1$ matrix, having the abstract format of Figure 2

However, we have to state that there are currently some important international standardization efforts regarding security logs like CIDF (Feiertag *et al.*, 1999), IETF IDMEF (Debar *et al.*, 2005) and IODEF (Arvidsson *et al.*, 2001). Their explanation is beyond the scope of this paper.

3.3 Aggregation

After security logs have been collected and normalized, the third fundamental design concept of a SIM is their ability to aggregate different event streams. For example, if an attacker uses an automated tool to break into a system account, a system would produce dozens of log entries, one for every attempt. This result is redundant and, most of the time, useless information, which is often treated as "noise." According to a survey conducted by Aberdeen Group (2003), nearly 75 percent of IDSs information and approximately 95 percent of the desktop information are irrelevant security noise, as shown in Figure 3.

3.4 Correlation

The fourth fundamental design principle of a SIM that is closely related with IR policies is their ability to correlate events coming from various sources and therefore provide information about incidents, not merely about signs of attacks. For example, a network attack (like an intrusion attempt) can be concurrently logged in multiple systems like FWs, proxy servers, IDSs but certain alerts about an attack cannot be triggered unless this information is correlated and certain thresholds are reached.

In security, "event correlation" can be defined as improving the threat identification and assessment process by looking not only at individual events, but also at their sets, bound by some common parameter ("related") (Chuvakin, 2004).

system	Event type	Src IP	Dst IP	Prt Num	Error Code	Comments

Figure 2.
Abstract format of a normalized security log

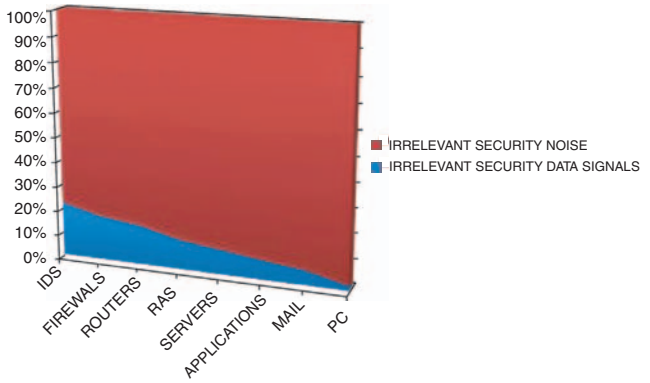

Figure 3.
Typical steady-state security signal-to-noise ratios

3.5 Visualization and reporting

The fifth fundamental design principle of modern SIM systems is their ability to provide a graphical representation of a security incident. For example, if an incident is targeting a specific system the SIM can provide a graphical map of the affected topology while providing side-information regarding this specific system or, in some cases, the complete path from the entry point to the target system. Furthermore, it has to provide clear reports about an incident in a chronological and time-consistent form and, in some cases, important forensic information (as described in section 4.7).

3.6 Archival

Finally, the sixth fundamental design principle of a SIM is their archiving capability. Considering that it primarily acts as an audit log collection storage area, a SIM must provide a large enough database to store raw audit data while on the other hand it has to maintain an archive of past incidents, therefore facilitating various policy compliance issues.

4. IR requirements

An IR policy usually comprises of six different phases (NIST, 2004; Mitropoulos *et al.*, 2006):

(1) *Preparation phase,* where all the necessary preventive and detective countermeasures are configured according to what the IR policy states.

(2) *Identification phase,* where various pieces of information regarding an incident are collected and the incident is categorized according to certain conditions.

(3) *Containment phase,* where short-term solutions are applied according to the incident's magnitude and severity.

(4) *Eradication phase,* where mid-term and long-term actions are taken in order to prevent the incident's recurrence.

(5) *Recovery phase,* where the incident is completely eliminated from the affected systems that are possibly configured from scratch.

(6) *Follow-up phase,* where the actions taken against a specific incident are documented and archived, while the IR policy is refined.

The identification phase is the most mission-critical phase since this is when an incident is assessed and categorized where all the other following phases and actions taken are primarily based on this decision. This is where the SIM features can provide useful information in order to reach useful conclusions before taking any actions against a specific security incident. In the following sections, we provide the most important requirements that should be incorporated in SIMs, in the context of IR.

4.1 Open architectures and integration with the core infrastructure

A fundamental design concept for next generation SIMs is their open architecture. Currently, most commercial products fall into one of the following main categories: open-source, vendor specific, and vendor-independent.

Open source SIMs provide a global open platform while leaving the open-source community to develop software agents to support vendor specific devices (like routers, switches, FWs, antivirus engines, etc.). On the other hand, vendor-specific SIMs support their full range of products using proprietary methods for information exchange and often little support for global system requirements (e.g. a vendor can produce FWs and IDSs but no AV). On the other hand, there is a limited or no support for third-party or competitor products. Finally, vendor-independent products seem to provide full support for a wide range of products of various vendors but they cost a significant amount of money (since a lot of R&D is involved in the process of development) and they follow a rather "closed" architecture, so it is not easy for custom agents to be developed and incorporated into the SIM.

Apart from the main developing technology, support of a standardized security event format is also essential for enforcing an automated IR policy. Most of the times, security incidents are spread within seconds so it is crucial for a SIM to collect, normalize, aggregate and correlate security events in real time so as to reach conclusions regarding the scope, magnitude and severity of a security incident to trigger containment and eradication actions (manually or automatically). Furthermore, when security information has to be exchanged between an organization and an analysis centre or a third-party computer security incident response team (CSIRT), this must be done in a unified and standardized format to avoid misinterpretation of sensitive security data.

According to the escalation level a security incident has, appropriate response actions are triggered (Mitropoulos *et al.*, 2006). This classification is based upon the correlation of various pieces of security information, which can be found in completely different systems. It is therefore of major importance that the correlation engine is accurate, facilitating trusted databases of signatures or patterns of attacks, so that appropriate response and remedy actions are taken.

4.2 Integration with vulnerability assessment tools

Vulnerability assessment is the process of discovering potential weaknesses in a given infrastructure. Vulnerabilities are categorized in various categories with a variety of classification methods. Formally, there are many vulnerability lists that entitle and describe vulnerabilities. Perhaps, the most celebrated are the computer emergency response team's (CERT) advisories at Carnegie Melon Software Engineering Institute, the Mitre's Common Vulnerability Enumeration program, the Symantec's Bugtraq, the Nessus' vulnerability list and others. In this context, it is important for a SIM to be able to be integrated with one – or more than one – vulnerability list in order to gain

important information for the response action. Apparently, by integrating vulnerability lists and by understanding IDS information, a SIM could possibly estimate real incidents and reduce false alarms. This is actually true, since many of the false positives associated with an IDS can be mitigated by considering only the vulnerabilities of a – given – protected network. This level of information could result in a higher level of confidence that a system is under immediate threat and decide for appropriate response actions (Gula, 2005).

4.3 Knowledge base

Modern attacks usually carry out a combination of known attack tactics, known as blended attacks. For example, Nimda worm was initially exploiting a flaw in e-mail clients without requiring the user to open the file attached (CERT, 2001). The payload infected immediately file shares and web servers. Nimda then exploited vulnerabilities in web browsers to spread to other client machines. In blended threats, the sequence of events can happen in any order, mostly depending on the vulnerabilities exploited. A detailed description of blended attacks, vulnerabilities and buffer overflow techniques in computer viruses can be found in Chien and Ször (2002). In this context, a blended threat can trigger a number of different events logged by different systems and correlated by the SIM. When this is the case, different patterns would be detected by the IDSs, the FW(s) or the antivirus system and different individual actions would be taken.

The issue of correlating security information into security incidents requires intelligence that may not be available in security logs or network traffic data. SIM systems should incorporate or provide a knowledge base that includes information about attack signatures and heuristics as well as statistical relationships between attacks. Relationships between security event alerts and event interpretation are basically described by the so-called production rules, a superset of attack signatures.

A sample production rule is described in the following pseudo-code piece to describe an unauthorized change in a web site (Sullivan, 2005):

```
http_Unauth_change rule:
  IF there is an HTTP event in the IDS AND
    the http_user is not a "Trusted_Admin" AND
    the http_command is "http_put" AND
    the http_reply is "success"
  then
    issue the alert - http_unauth_change_attack
  ENDIF
```

A formal description of an attack specification language that describes attacks can be found at Krugel *et al.* (2001). Production rules can also be used during the aggregation function. For the above simplified paradigm, three different security events were aggregated to one incident and an appropriate response action was initiated by the corresponding alert issued. Moreover, a production rule can detect and initiate responses to anomalous events while they can be added to the knowledge base without requiring changes to the existing production rules.

However, we must consider important factors like rule timeout (how long the rule will be in a certain state), transition (when a certain rule is changed) and action (what is the actual response) (Chuvakin, 2004).

4.4 Information freshness and liveness

Two very important aspects when correlating security incidents or providing information regarding a security incident are the properties of "freshness" and "liveness." When a SIM is correlating security logs from various sources and provides state information regarding an incident, it also has to provide some form of assurance that this information is on one hand "fresh" (i.e. information origin and integrity are checked) and on the other hand "live" (i.e. there has been no modification to this state ever since it was produced by the SIM).

Freshness mechanisms require the use of globally synchronized clocks within the boundaries of a corporate IT environment. This requires that the whole infrastructure either has reliable access to an accurate time source (e.g. national radio broadcast time) or the NTP protocol is used for all systems (IETF, 1992), or – at regular time intervals – an authentication protocol not based on physical time-stamps is used (e.g. use of logical time stamps or numbers used once – nonces).

Logical time-stamping mechanisms imply that every pair of communicating entities (e.g. a log source and the SIM engine) store a pair of sequence numbers used only in communications between that pair. An example logical time-stamping mechanism is described in the following.

Assuming that the SIM engine and an event source are the communicating parties A and B, respectively, both A and B have to maintain two counters: N_{AB} and N_{BA}. Every time A sends B a message, the value of N_{AB} is included and N_{AB} is incremented. Every time A receives a message from B, then the sequence number put in the message by B (N say) is compared with N_{BA}:

- If $N > N_{BA}$ then the message is accepted as "fresh" and N_{BA} is reset to equal N.
- If $N \leq N_{BA}$ then the message is rejected.

On the other hand, a nonce-based protocol requires that when A sends B a nonce as a challenge B includes the nonce in the response to A. Because, the nonce has never been used before, A can verify the freshness of B's response (given message integrity is protected by some cryptographic functions). An example simplified nonce and integrity mechanism is described in the following:

- $B \rightarrow A: M_1 = R_B \parallel \text{Data}_1$
- $A \rightarrow B: M_2 = \text{Data}_3 \parallel f\, K_{AB}\, (R_B \parallel B \parallel \text{Data}_2)$,

where R_B is a random number sent by B to A, Data_1, Data_2 and Data_3 are data strings exchanged between A and B, $f\, K_{AB}$ is a cryptographic check value using a symmetric cryptographic key K_{AB}. In the previous mechanism, B's identity is included in the message sent from A to B so that B can be sure that the message is intended for it.

4.5 Handling of encrypted traffic

In most corporate environments, cryptographically protected communications are a commodity. Common applications of that kind include remote systems management and encrypted peer communications that are mostly using conventional cryptographic mechanisms as well as e-commerce applications that are mostly based on asymmetric cryptographic mechanisms. By default, security systems are not able to examine encrypted traffic unless this traffic is decrypted at the endpoint. For example, if a corporate site serves a web-based application using the SSL protocol, then all traffic is

directly passed through the FW and network-based IDSs and the data stream is decrypted only at the endpoint. If a data stream carries a malicious payload, and the endpoint is not appropriately protected then the attack will be successful and not detected (and neither logged in some cases).

In modern security systems, encrypted traffic is handled either by some special security products that perform SSL off-loading functions or form an integral part of high-end FWs or intrusion prevention systems (IPSs). Whatever the case, a SIM has to be aware of encrypted communications through detecting and logging specific information.

4.6 Role-based access control administration and support

When an IR policy is implemented within an organization many different corporate and external parties (known as IR contacts) have to participate, each one serving different roles and having different responsibilities. An abstract IR management framework was proposed in Mitropoulos *et al.* (2006). Based on this framework and following the NIST proposed standard for role based access control (RBAC), we propose the most important corporate roles in an attempt to define RBAC functions that have to be, in turn, supported by a SIM (Ferraiolo *et al.*, 2001). We define public information as the pieces of information regarding an incident that can be handed to third-parties for further analysis. We define as private the information that must be scrutinized before handed to third-parties.

- *Users (U)* the corporate users are obliged to report every security incident through a management channel. In our case, the SIM serves this purpose. In other words, Users have only "append" (blind write) access rights of private and public information to the SIM through specific channels (e.g. the corporate users).
- *Managers (M)* the managers, according to their scope, must have "read only" access to the SIM. The IR capability leader should have fully privileged read permissions both to private and public information in order to complete the security picture of an incident (e.g. the IR capability leader, senior management, etc.)
- *Administrators (A)* the administrators should have both "read" and "write" access to private and public information of the SIM (i.e. systems and network administrators, members of the CSIRT, etc.).
- *Support staff (SS)* other people with "read" access limited to private information (e.g. human resources, help desk, etc.)
- *Information dissemination executives (IDE)* people that are authorized to disseminate information to third parties should have read access to public information (e.g. corporate investigations group, information security officer, legal advisor, etc.).

The ISO/ODP standard defines that a role is an "identifier for a behavior, which may appear as a parameter in a template for a composite object, and which is associated with one of the component objects of the composite object" while a behavior is a "collection of actions with a set of constraints on when they may occur" (ISO, 1995). In this context, a management policy should be used to define the obligations and authorizations for a given group of managers, as well as the behavior expected from

managers assigned to a particular organizational position, or to a system management platform. According to Lupu and Sloman (1997), a role is a set of policies applied to a group (domain) of managers, so-called position domain (PD). In turn, managers can be assigned to or removed from a role without redefining the role policies. Furthermore, roles should interact with each other and have obligations and authorizations towards each other. Thus, all the proposed roles can be defined as a set of obligations/authorizations (positive and negative permissions) towards each other and towards the SIM.

Finally, all roles, in the context of IR, must be mutually exclusive in order to prevent unauthorized modification to sensitive forensic information kept by the SIM. In other words, each role corresponds to a separate PD. An alternative solution using the ARBAC97 administrative model could also be used, however this is among our next research steps (Sandhu *et al.*, 1999).

4.7 Exception handling

IR is not a static process and is heavily dependent on the business needs of an organization. Based on this, what may consist abnormal activity for an organization may not be the case for another. Also, even within a security domain that is mandated by a formal security policy, there may be the need for exception handling (in order to avoid policy violation).

As an example, the CSIRT of a Financial Institution should normally have privileged access to security or hacking sites (e.g. in order to be informed of virus outbreaks or attacking targets) that ordinary users are usually restricted from, so there may be the case that CSIRT are violating the user access policy (since they could be also "users" themselves).

Apart from that, exceptions form an important aspect of IPSs that perform behavioral analysis apart from single attack pattern recognition. Even if there is a successful intrusion to a corporate site, the IR policy may not require that this intrusion is stopped (e.g. by terminating the connection) since there may be the need to collect important information regarding the attack source (e.g. through a trace-back mechanism) or gather electronic evidence to be later used as evidence during a forensics analysis.

In terms of using a SIM to enforce an IR policy, exceptions have to be carefully managed either when collecting or correlating security events as well as when response actions are mandated from the SIM to the affected hosts (e.g. by the use of SNMP, CISL or STATL commands (Eckmann *et al.*, 2002)).

4.8 Forensics information and chain-of-custody

Digital Forensics is the science dealing with the "preservation, identification, documentation and interpretation of computer data" (Kruse and Heiser, 2002). A vital element of every forensics analysis is the proper timeline of events as well as the handling or the response actions taken so that the analysis is preserved from accidental or malicious modification.

In order to accomplish this, a SIM should preserve information tagged as "forensic information" in a secure area. Among others, the most important security services that a SIM should provide to this area are:

- *Identification and authentication* – so that only the authorized users are granted access to this sensitive information, whereas their identity is verified. Use of

strong authentication mechanisms like one-time-password mechanisms (OTPs) or qualified signed certificates must be supported whereas all communication should be encrypted.

- *Access control and authorization* – based on a role-based access control model (see Section 4.5) so that users get only the permissions implied by the IR Policy.
- *Accountability and auditing* – is needed to log all security relevant actions in order to make users accountable for their transactions. Audit trails are used to find patterns of abnormal use which are often a sign of (attempted) compromise.

Finally, based on the RBAC policies described in section 4.5 and the synchronization techniques presented on section 4.3, the SIM should automatically provide the so-called "chain of custody" for a forensics analysis. The chain-of-custody is usually requiring the following information for the affected system and can be used as evidence to courts:

- the location (within the corporate premises) of the system;
- the IP address, conventional name and any other logical information regarding the affected system;
- the names of the employees that could possibly have access to this room;
- the location of the individual computer system on the room;
- the state of the system (preferably a photograph of the system to displaying all the visible information at this time);
- the serial numbers, models and makes of all the components of the system examined; and
- the peripherals attached to the system.

4.9 Trace-back integration

Apart from providing detailed information regarding a security incident, a SIM must be capable of tracing the source(s) of it, i.e. to perform trace-back functions, in order to reach to the actual attacker(s).

The trace-back problem is to identify the actual IP addresses of hosts $h_{n\text{-}1},\ldots h_1$ given the actual IP address of host h_n, when $C = h_1 + h_2 + \cdots + h_i + h_{i+1} + \cdots + h_n$ is the connection path between hosts h_i (where $i = 1,\ldots n$). It is of major importance for a SIM to be able to integrate related trace-back mechanisms when situations require so. Since, running in application level, a SIM could either incorporate IP marking techniques or ICMP trace-back that operate in the network-level or either application level trace-back mechanisms, such as the IDIP (Schnackenberg *et al.*, 2002; Feiertag *et al.*, 1999). We refer the reader to Mitropoulos *et al.* (2005) for a categorization of trace-back mechanisms and to Kuznetsov *et al.* (2002) for a performance evaluation of IP trace-back methods.

In terms of IR, a SIM provides the big picture of a security incident by providing visual information on global or selected topology maps. When integrated with appropriate trace-back mechanisms it should facilitate a connection tracing (e.g. by a "trace" command issued by the SIM on the topology map) beyond the boundaries of the corporate network and a complete reconstruction of the attack path.

4.10 Visualization enhancements

Modern SIMs offer a real-time monitoring of the security incidents as well as associated response actions or short description of the attacks in progress (or attacks remediated). An IR policy, however, requires global knowledge of the underlying IT infrastructure, so it is of major importance that a SIM console provides – at least – the following visualization enhancements:

(1) network and system topology maps;

(2) attack path (by importing trace-back information as described in Section 4.8);

(3) time-line of events (to fulfill the Forensic requirements described in Section 4.7);

(4) executive and technical briefings and reports based on:

- collecting and correlating the security events that form an incident;
- the forensic information provided; and
- the short/complete attack description according to the knowledge base and the vulnerability lists supported.

(5) access to the raw security logs as well as links to the correlated information; and

(6) a selection menu for associated response actions to a security incident (e.g. stop a session, block a connection, reset a connection, trace an attack, record a session, etc.) according to the formal description of the IR policy.

Figure 4 shows an integrated distributed SIM architecture, including the corporate elements that participate in an IR Policy in an attempt to facilitate the automated response process as well as to assist in the global overview of any security incident.

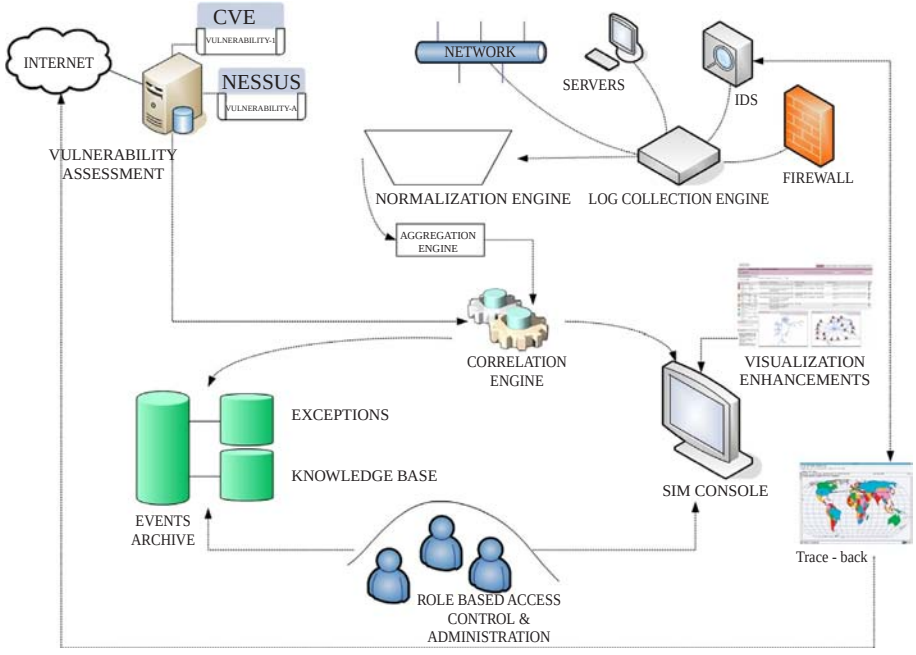

Figure 4.
An integrated distributed SIM architecture

The nature of a SIM system is by definition distributed due to the involvement of various wide-spread components.

4.11 IR policy evaluation

Finally, the importance of policy evaluation in terms of IR is of major significance, since response actions to security incidents may require the adjustment or the refinement of the security policy.

Use of a SIM significantly assists in this by reducing the number of false positive alerts (by correlating security information, therefore producing alarms only for actual events). A SIM is primarily based on the configuration of the existing security mechanisms installed in a corporate environment and is not itself another security mechanism, so the issue of false negatives still remains open and should not be underestimated.

Integration of a SIM with a security policy compliance tool would be beneficial for an organization, but this implementation feature has not yet been addressed in terms of IR by the vendors. Such a policy compliance and validation tool implementation could be supported by a number of existing formal policy specification languages (Damianou *et al.*, 2001). This approach could lead in the development of policy based security models using artificial intelligence techniques for the purpose of managing synergy, conflict and compliance between activated policies. Furthermore, this approach would allow for adaptive policies based on the incident's significance and magnitude as well as the appropriate remedy actions.

5. Conclusions and future work

In this paper, we proposed fundamental IR Policy requirements for SIMs. In turn, we proposed a role-based access control approach for a corporate IR capability with the use of such a system. Finally, we proposed various mechanisms that could be mandated by appropriate adaptive policies for enhancing the overall security of a SIM. It is among our next immediate steps to evaluate different categories of SIMs in our academic environment in order to assess the IR features they provide. Furthermore, our main target is to develop an open-source prototype for the description of specific responses and by integrating the proposed requirements into a SIM try to automatically adjust these responses to real security incidents. In addition, it is in our purpose to develop an overall policy-based security framework for handling the IR requirements and structuring the management tasks induced from these requirements.

References

Aberdeen Group (2003), "Turning IT security into effective business risk management", An Executive White Paper, available at: www.ca.com

Arvidsson, J., Cormack, A., Demchenko, Y. and Meijer, J. (2001), "TERENA's incident object description and exchange format requirements", RFC 3067, available at: www.ietf.org

BSI (1999), *Information Security Management, BS7799, Part 1: Code of Practice for Information Security Management*, BSI, Bonn.

CERT Advisory CA-2001-26 (2001), *Nimda Worm*, available at: www.cert.org

Chien, E. and Ször, P. (2002), "Blended attacks exploits, vulnerabilities and buffer-overflow techniques in computer viruses", paper presented at Virus Bulletin Conference, New Orleans, LA, September.

Chuvakin, A. (2004), "Security event analysis through correlation", *Information Systems Security*, Vol. 13 No. 2, pp. 13-18.

Damianou, N., Dulay, N., Lupu, E. and Sloman, M. (2001), "The ponder policy specification language", *Proceedings of Policy 2001: Workshop on Policies for Distributed Systems and Networks, Bristol, Volume 1995 of Lecture Notes in Computer Science*.

Debar, H., Curry, D. and Feinstein, B. (2005), "The intrusion detection message exchange format (IDMEF), (internet-draft)", available at: www.ietf.org

Eckmann, S., Vigna, G. and Kemmerer, R. (2002), "STATL: an attack language for state-based intrusion detection", *Journal of Computer Security*, Vol. 10 Nos 1/2, pp. 71-104.

Feiertag, R., Kahn, C., Porras, P., Schnackenberg, D., Staniford-Chen, S. and Tung, B. (1999), "A common intrusion specification language", available at: http://people.emich.edu/pstephen/

Ferraiolo, D.F. *et al.* (2001), "Proposed NIST standard for role-based access control", *ACM Transactions on Information and System Security*, Vol. 4 No. 3, pp. 224-74.

Gula, R. (2005), "Correlating IDS alerts with vulnerability information", White paper, Tenable Network Security, available at: www.tenablesecurity.com

Hansman, S. (2003) *A Taxonomy of Network and Computer Attack Methodologies*, technical report, Department of Computer Science and Software Engineering, University of Canterbury, Christchurch.

IETF (1992), *Request for Comments (RFC) 1305, Network Time Protocol (Version 3) – Specification, Implementation and Analysis*, available at: www.ietf.org

ISO (1995), *ISO/IEC JTC1/SC21, Basic Reference Model of Open Distributed Processing, Part 2: Descriptive Model*, ITU-T X.903-ISO/IEC 10746-3, ISO, Geneva.

Krugel, C., Toth, T. and Kerer, C. (2001), "Decentralized event correlation for intrusion detection", *Proceedings of Information Security and Cryptology, Volume 2288 of Lecture Notes in Computer Science*.

Kruse, W. and Heiser, J. (2002), *Computer Forensics*, Addison-Wesley, Ontario.

Kuznetsov, V., Simkin, A. and Sandström, H. (2002), "An evaluation of different IP trace-back approaches", *Proceedings of Information and Communications Security: 4th International Conference, ICICS 2002, Singapore, Volume 2513 of Lecture Notes in Computer Science*.

Lupu, E. and Sloman, M. (1997), "Towards a role based framework for distributed systems management", *Journal of Network and Systems Management*, Vol. 5 No. 1, pp. 5-30.

Mitropoulos, S., Patsos, D. and Douligeris, C. (2005), "Network forensics: towards a classification of trace-back mechanisms", *Proceedings of Security and Privacy for Emerging Areas in Communication Networks, Workshop of the 1st International Conference on Network Forensics, Athens*.

Mitropoulos, S., Patsos, D. and Douligeris, C. (2006), "On incident handling and response: a state-of-the-art approach", *Computers and Security*, Vol. 25 No. 5, pp. 351-70.

NIST (2004), *Computer Security Incident Handling Guide*, NIST Special Publication 800-61, NIST, Gaithersburg, MD.

Sandhu, R., Bhamidipati, V. and Munawer, Q. (1999), "The ARBAC97 model for role-based administration of roles", *ACM Transactions on Information and System Security (TISSEC)*, Vol. 2 No. 1.

Schnackenberg, D., Djahandari, K., Reid, T. and Wilson, B. (2002), Cooperative Intrusion Trace-back and Response Architecture (CITRA), Boeing Phantom Works and NAI Labs, Prepared Under Contract N66001-01-C-8048 for Space and Naval Warfare System Center (SSC), San Diego, CL.

Sullivan, D. (2005), "The definitive guide to security management", Realtimepublishers.com, available at: www.ca.com

About the authors

Sarandis Mitropoulos is a visiting Lecturer at the Department of Informatics of the University of Piraeus, Greece, and a System Analyst at a Bank supervised by the Ministry of Economics of Greece. He completed his PhD at the Department of Electrical and Computing Engineering of the National Technical University of Athens (NTUA) in 1994. His PhD dissertation focused on Distributed System and Network Management. He received his degree in Informatics and Computing Engineering for the same department of NTUA in 1990. He has been working in technical and project management and business development in European R&TD and integrated solution projects, in the areas of system and network management, of advanced telecommunication/telematic services, and of management information systems, as well as of system and network security. He taught in NTUA from 1991 to 1994. He is a senior member of IEEE and member of CNOM, and Technical Chamber of Greece.

Dimitrios Patsos is a PhD Candidate at the Department of Informatics, University of Piraeus (Greece). He holds a BSc in Informatics from the Athens University of Economics and Business (Department of Informatics), an MSc in Information Security from Royal Holloway University of London (Department of Informatics, Information Security Group), and various professional certifications. He has been serving as an Information Security Consultant for a Major Greek Systems Integrator since 1999, dealing with various aspects of Information Security with a strong emphasis on the Financial Institutions Sector and especially to Banks. His main research interests are security management, cryptography, network security, IR and electronic crime. He is a member of the Permanent Scientific Committee on Industry and Standardization of the Greek Computer Society (EPY) and a formal member of EPY.

Christos Douligeris received the Diploma in the Electrical Engineering from the National Technical University of Athens in 1984 and the MS, MPhil and PhD degrees from the Columbia University in 1985,1987,1990, respectively. He has held positions with the Department of Electrical and Computer Engineering at the University of Miami, where he reached the rank of associate professor and was the associate director for engineering of the Ocean Pollution Research Center. He is currently teaching at the Department of Informatics of the University of Piraeus, Greece. He has served in technical program committees of several conferences. His main technical interests lie in the areas of performance evaluation and security of high speed networks, neurocomputing in networking, resource allocation in wireless networks and information management, risk assessment and evaluation for emergency response operations. He was the guest editor of a special issue of the IEEE Communications Magazine on "Security for Telecommunications Networks" and he is preparing a book on "Network Security" to be published by IEEE Press/Wiley. He is an editor of the IEEE Communications Letters, a technical editor of IEEE Network and a technical editor of Computer Networks (Elsevier). Christos Douligeris is the corresponding author and can be contacted at: cdoulig@unipi.gr