Title: Advanced Platform for Corporate Incident Detection and Management

Author: Fabio Ghioni

Postal Address: Piazza Einaudi, 8 - 20124 Milano, Italy

Telephone: +39 02 6219224

Fax: +39 02 6213820

e-mail: fabio.ghioni@telecomitalia.it

Abstract

Today companies are faced with a growing number of threats which undermine the integrity of their own business and information. Most threats arise from the heavy dependence of services upon information technology and the high flexibility of IT infrastructures which poses problems in terms of potential misuse.

Information leakage is one of the most sensitive instances of corporate incidents entailing a criminal intention. Nevertheless, other causes can be ascribed to an inadequate protection of critical information, i.e. a lack of policy enforcement or poor classification system. The end goal is to achieve an information infrastructure that ensures the availability of critical information while guaranteeing its integrity through a suitable Information Lifecycle Management strategy.

However, such policies heavily rely on technological infrastructures and need to be supported by *ad hoc* tools. Hence, since it is not always possible to ensure accurate operations on the entire infrastructure, it is vital that organizations are able to monitor and manage incidents, cyber attacks and fraud against themselves and their clients through an integrated platform. An adequate unified control system will, on the one hand, gather incident alarms from both internal and external sources (directories, black lists, etc.) as well as through probes and peripheral agents, on the other hand, monitor traffic on a parametric basis. This platform will provide an environment which will support the operator during the whole process of case management.

List of Keywords

Asymmetric Environment
Classification Model
Clearance
Critical Infrastructure
Data Classification
Incident Management
Information Protection
Integrated Platform
Interoperability
Network and System Security
Parametric Interception
Peripheral Agent
Probe

Introduction

The Information Age has brought about an unprecedented revolution in our everyday lives and has dramatically changed the way in which the functioning of our societies is intertwined with technology. Today most services depend upon Information Technology and a great number of vital and private information is exchanged through the network. Providers delivering essential services are required to guarantee the integrity of the underlying infrastructure since they have become the backbone of social and economic life worldwide.

In the last decades the rapid changes in technology, national regulatory practices, market conditions and industrial realignments have challenged the core concepts of traditional infrastructures, leading to their progressive convergence. In this context information infrastructure has become crucial for managing and integrating all other Critical Infrastructures; conversely, its high flexibility combined with the great interconnection among systems using open architectures and technologies, poses serious security problems in terms of potential misuse and interruption of critical services. Indeed, the Internet has created a new medium for perpetrating crimes; the anonymity provided by the net, as well as its global and unregulated nature, has produced an exponential explosion in the number and types of technology-based crimes.

This leads to the concept of Asymmetric Environment, where small groups of individuals or processes can access information resources, typically stored in databases, or dispersed information located in diverse IT infrastructures, with a minimum amount of effort and risk. The wide variety of devices which can be used to access a system and the independence from physical proximity between the performer and the target are the most significant aspects of an Asymmetric Environment. The concept is borrowed from the military definition of Asymmetric Warfare, or "the attempts to circumvent or undermine an opponent's strengths while exploiting his weaknesses, using methods that differ significantly from the opponent's usual mode of operations" by utilizing "unconventional approaches or inexpensive means"[1].

This very empowering scenario is all the same highly risky in terms of disclosure of sensitive information to unauthorized entities; identity theft is a typical instance of such threat. In order to ensure safe electronic transactions, a new approach to the security of IT Infrastructure is necessary. The vast number of protocols underlying the information exchange processes complicates the monitoring of such transactions with the traditional methods used so far. In particular, the telecommunications network plays a crucial role as most information is exchanged through it and most services rely upon its infrastructure. A service-independent telecommunications network,

[1] Lieutenant-Colonel La Carte, D. A., 2001-2002, Asymmetric Warfare and the Use of Special Operations Forces in North American Law Enforcement, *Canadian Military Journal*

where the intelligence is taken out of the switch and placed in computer nodes, allows the operator to develop and control services more efficiently.

Therefore, in order to secure the correct functioning of IT infrastructures, the following key aspects, strictly interwoven among them, have to be taken into account: data classification, interoperability and overall network and system security. The end goal is to achieve an information infrastructure that ensures availability of critical information while guaranteeing its integrity.

1. Data Classification

Information leakage is one of the most sensitive instances of corporate incidents entailing a criminal intention. Nevertheless, loss of critical information may also depend upon inadequate protection, i.e. a lack of policy enforcement or poor classification system.

Information must be adequately protected from threats which undermine its confidentiality, integrity and availability; for each of the three key aspects it is important that internal data protection policies are enforced through *ad hoc* organizational and technological countermeasures. Information must be correctly classified in terms of confidentiality levels so that only authorised individuals, organizations or processes can access them. An important issue related to data classification concerns the maximization of interoperability between diverse classification systems while respecting the different organizational structures and needs. Convergence between a conservative and secure data classification system and the usability of such data by authorised users only is the real challenge which all organizations are faced with.

The end goal is to achieve an information infrastructure that ensures the availability of critical information while guaranteeing its integrity through a suitable Information Lifecycle Management strategy.

Thus, the essential requisites of an effective classification system are:

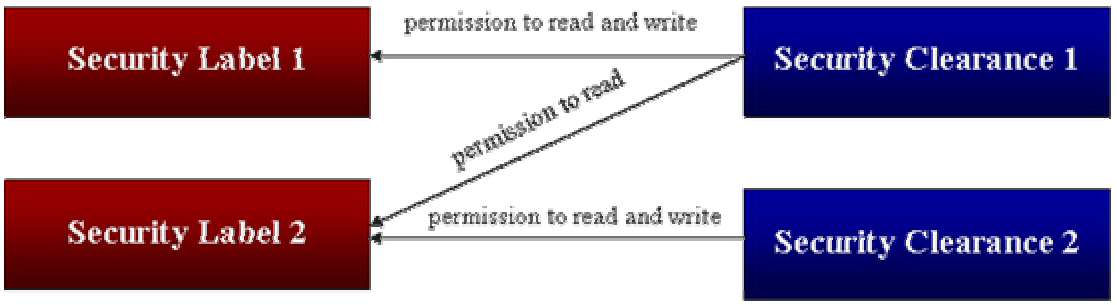
- Integration and enforceability of company policies
- Definition of confidentiality levels based on the information relevance
- Availability in terms of role
- Compliance with the “need-to-know” principle, according to which permissions are strictly related to the execution of role duties
- Compliance with the “separation of duties” principle through restrictions aimed at avoiding conflicts of interests
- Access management

The automation of the information management process must be maximized in order to lower risks related to human errors and optimize the storage layers.

In order to facilitate the automation process it is necessary to switch one's attention from classification based on mere content to the application of theoretical models regulating access to information. Today most data are stored and managed electronically; therefore it is necessary that organizations pay special attention to developing effective document management platforms, based on the five pivotal security services suggested by ISO 7498-2: identification and authentication, access control, confidentiality, integrity and non-repudiation.

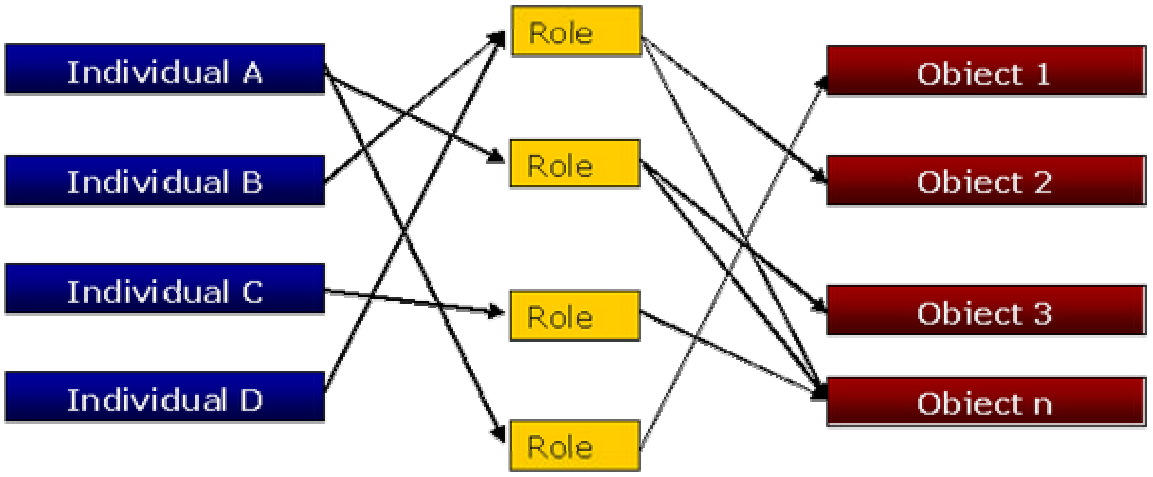
The definition of a comprehensive clearance procedure, based on efficient permission parameters, is essential to the implementation of a data classification system. No single classification model, among the existing ones, can suit the needs of a large organization, which often imply complex communication flows and business structure. This study proposes a mixed model merging the MAC concept of clearance and the RBAC definition of roles.

The Mandatory Access Control attributes a centralized "security label" to all objects containing information and a "security clearance" to all individuals dealing with such information. The following scheme describes the correspondence between security labels and security clearance:



This mechanism ensures that the information flow is limited among objects with equivalent security levels.

In the RBAC model, the security clearance is attributed in compliance with the roles that each individual holds within the organization and is predefined by the organization itself.



The mixed model, instead, defines a "clearance matrix" where roles are matched with the appropriate clearance level. Depending on the operational needs, the attribution of the security clearance can be integrated with rules regarding hierarchical consistency among levels, i.e. higher clearance can access all information with lower clearance within the same department. Once the clearance matrix is completed, it is possible to create tables where classified information is matched with the different permission levels (e.g. generate, read, read and write, administrative clearance, etc.).

It is vital that the abovementioned procedure is carried out *a priori* by an entity other than the owner of the information and be supervised by a corporate department.

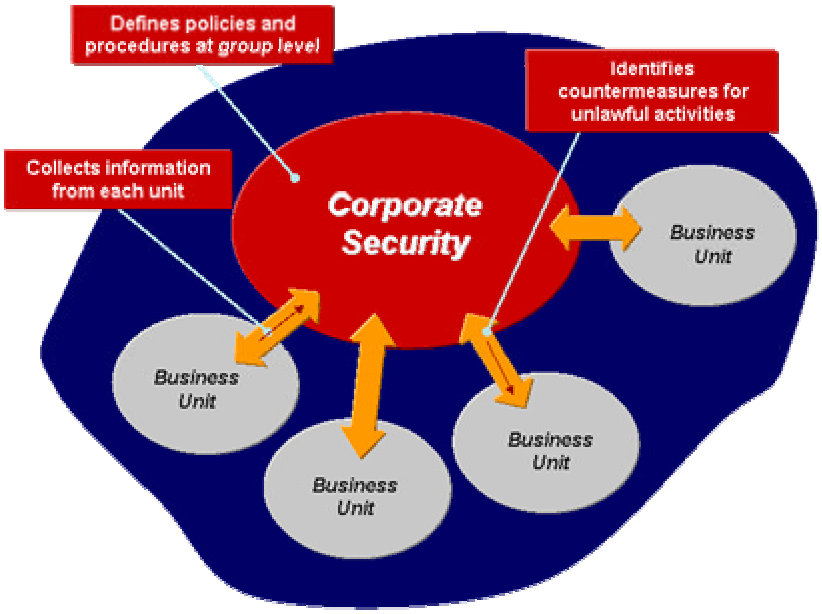
Such classification model needs to be supported by and adequate technological platform, which ensures:

- watermarking of documents according to the attributed clearances
- automatic tracing of documents both within and outside the company, according to the following possibilities:
    - documents are traced when leaving the company and an alarm is sent to the Control Room
    - documents notify each time they are opened outside the company
    - documents are scrambled when leaving from a given domain
    - the solution can be implemented also for documents printed or saved on hard devices (i.e. Floppy Disk, USB or local printer) and can integrated the existing alerting technologies (SOC or Control Room)

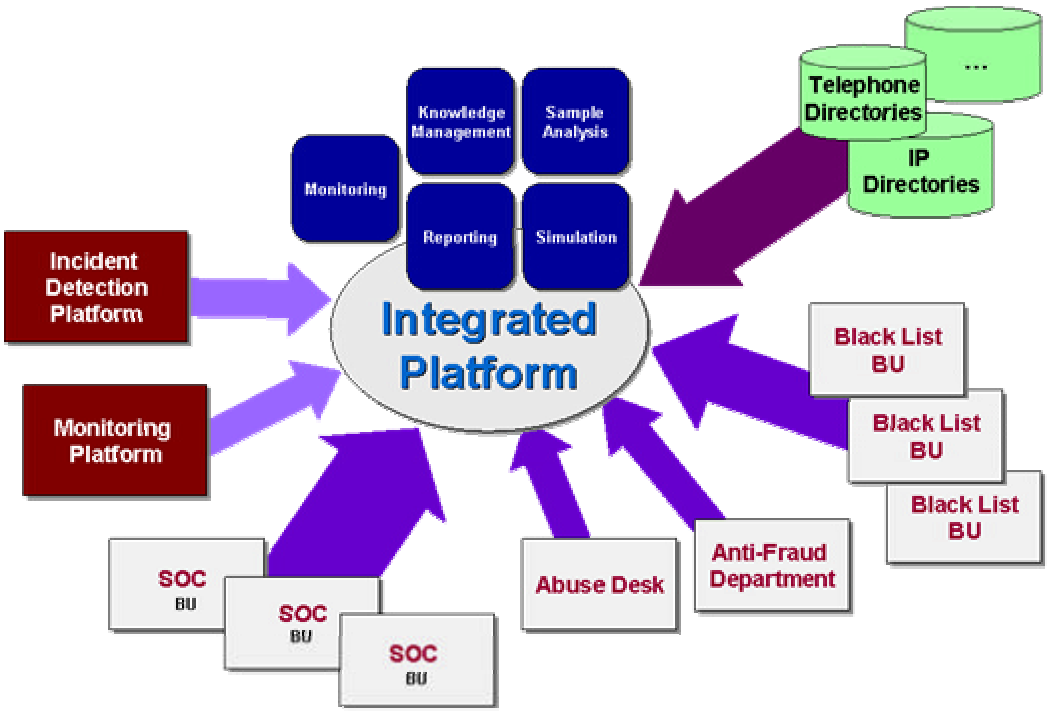
2. Interoperability

In a pervasive and ubiquitous computing environment data are processed through diverse systems and travel across a large number of different transmission media, both wireless and wireline. In this scenario, it is crucial that transmitted data can be processed in a consistent way by all entities involved in the process even if they perform on different platforms and architectures.

Hence, since it is not always possible to ensure accurate operations on the entire infrastructure, it is vital that organizations are able to monitor and manage incidents, cyber attacks and fraud against themselves and their clients through an integrated platform.



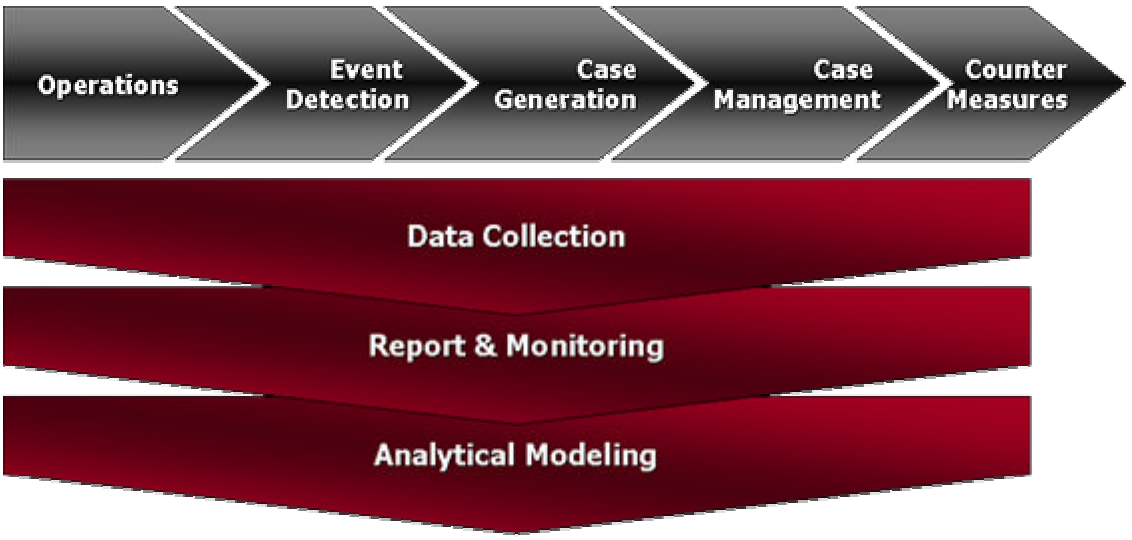
The urge for an effective communication process between the different business units and the corporate security departments is one of the main issues within large organizations. Therefore, an integrated platform, on the one hand, gathers and standardises scattered information elaborated by systems which have been conceived and implemented in different times and contexts; on the other hand, it has to provide tools and procedures to identify the appropriate countermeasures for the detected unlawful activities through a toolkit approach.



The toolkit concept encompasses legal, policy, practice and technology aspects and solves the problems related to the isolation within the organization.

Each operational system logs the daily activities related to service provisioning, conveying the necessary information for the definition of typical usage patterns. Therefore, it is possible to detect frauds and unlawful behaviours by identifying the atypical usage patterns (e.g. traffic peaks) which characterize them. The system detects significant events through specific filters and sends alarms to the case generator which matches the new information with the historical data. Frauds are thus identified and inferential engines and dynamic scoring help to assess their severity level. Each case is then managed in compliance with the company's internal procedures, i.e.:

- Assessment of potential damages
- Identification of technical and procedural causes
- Co-operation with the departments involved
- Set up of preventive measures
- Set up of specific countermeasures



The data produced in each phase of the process are collected and standardised and can be monitored both on a dashboard and through historical or multi-dimensional reports. The whole process is constantly refined and modified thanks to the acquired expertise (new analytical models) and is thus capable of adapting to new issues.

3. Network and System Security

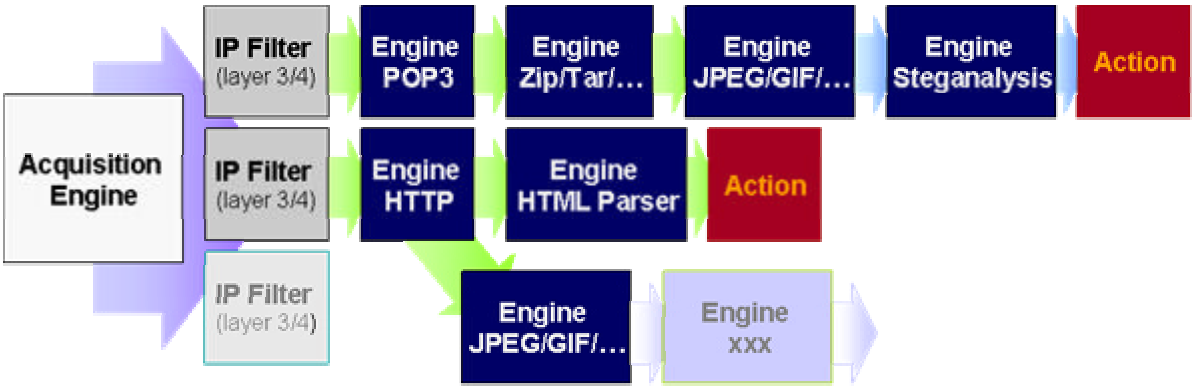
When dealing with the security of strictly interconnected systems and networks it is necessary to view them both in their single components (from ultraportable devices and Personal Area Networks to the dimension of great databases or large corporate WANs) and on the whole.

An adequate platform for incident detection and management will rely on distributed "intelligent" probes and peripheral agents which will gather alarms from monitored systems and will screen traffic on a parametric basis.

Such systems rely on the recent concept of parametric interception. With the upsurge of terrorist organizations worldwide, which increasingly rely upon the Internet as a tool for the circulation of subversive communication, the need has arisen to identify a technique for intercepting traffic flows. Parametric interception was first used in the field of criminal investigation as a method for outlining an "electronic identikit" of the alleged offender, based on the "telematic fingerprints" which everyone scatters through the net while connected. In other words, it is possible to identify specific parameters, such as words, web or e-mail addresses, within a given data flow, with the aim of tracking down all those users who are compatible with the identikit.

A preventive application of parametric monitoring within organizations stemmed from such investigative approach. Indeed, it is possible to set a number of parameters which relate to specific criminal activities and monitor all electronic traffic falling within the given parameters. This

introduces to the concept of probes behaving as peripheral agents. These agents are able to detect events or trace atypical activities by performing a real-time analysis of a given subnet or connection. A decision tree structure enables a real-time management of traffic:



The solution provides an essential tool for detecting and analysing anomalous activities which threaten the security of most organizations. For instance, the following areas should be focused upon when dealing with IP technology:

- detection and monitoring of scan activities or anomalous network access (port scan, network scan, SNMP scan, NETBIOS query, computer browsing, etc;
- detection of DoS attacks (Denial of Service) through correlation of traffic peaks towards a specific IP address, of port, of transport protocol and of payload within the detected packets;
- detection of virus spreading through the analysis of outgoing packets from a single machine;
- content analysis on virus/DDoS packets
- "near-real-time" statistical analysis on network traffic and Trend Analysis on: "Top20 Source IP", "Top20 Destination IP", "Top20 Packet Dimension", "Top20 Protocol", "Top20 Destination Port", etc;
- detection of ARP poisoning activities used for sniffing corporate LAN.

The issues presented so far are strictly technical and constitute the building blocks of an effective monitoring activity aimed at protecting the organization's network infrastructure.

However, such tools are not confined to basic network protection; their functionality can be enhanced so as to detecting the content of specific data flows. Indeed, companies are also faced with attacks which undermine the integrity of their intangible assets, such as intellectual property, the loss of which can cause serious damage in terms of economics or image. As described elsewhere, most data are stored electronically and their protection is a major business requirement. For instance, it is possible to trace unauthorized transfer of classified documents identified by adequate watermarks or detect exchange of pedo-pornographic material by correlating image filters with the file format.

Conclusion

The Information Age has undoubtedly enriched our way of living by increasing the communication opportunities worldwide. On the other hand, the wide availability of technological tools and the growing automation of most everyday activities pose serious security problems in terms of potential misuse of the IT infrastructure and interruption of vital services.

The present paper has proposed an integrated approach to face the ever changing threats which undermine corporations' physical infrastructure and intangible assets. An advanced platform for corporate incident detection and management will focus upon three pillars: an effective data classification system to secure that sensitive data are accessed by authorised entities only; interoperability to guarantee a centralized management of incidents and information flows; network and system security tools, such as probes, to detect potential attacks against both physical and intangible assets

References

1. Setola, R, 2003, La Protezione delle Infrastrutture Critiche Informatizzate, *Automazione e Strumentazione*
2. Anderson, P.S., 2002, Critical Infrastructure Protection in the Information Age, *Networking Knowledge for Information Societies: Institutions and Intervention*
3. Matthews, H.S., 2001, Analyzing Critical Infrastructure Dependencies: Security and Survivability Effects in the Service Sectors
4. La Carte, D. A., 2001-2002, Asymmetric Warfare and the Use of Special Operations Forces in North American Law Enforcement, *Canadian Military Journal*
5. Goodwin P., 2004, Information Life-Cycle Management and Enterprise Content Management: the Confluence of Technology and Business
6. Ferraiolo D. F. and Kuhn R. D., 1992, Role-Based Access Controls, *Proceedings of the 15th NIST-NSA National Computer Security Conference, Baltimore, Maryland, October 13-16*
7. De Stefano C., 2004, Le Indagini della Polizia Giudiziaria
8. Telecom Italia, 2004, Internal Document on Data Classification
9. Telecom Italia, 2003, Internal Document on Centralized System for Incident Handling
10. Telecom Italia, 2003, Internal Document on Probes and Parametric Interception