Business Governance based Policy Regulation for Security Incident Response

Feltus, Christophe; Khadraoui, Djamel; De Remont, Benoît; Rifaut, André

Published in:
Proceedings of CRiSIS'2007 : International Conference on Risks and Security of Internet and Systems, colocated with IEEE GIIS, Marrakech, Morocco.

Publication date:
2007

Document Version
Early version, also known as pre-print

Business Governance based Policy Regulation for Security Incident Response

Christophe Feltus , Djamel Khadraoui, Benoît de Rémont and André Rifaut

Centre de Recherche Public Henri Tudor – Luxembourg

Email: christophe.feltus@tudor.lu, benoit.deremont@tudor.lu, djamel.khadraoui@tudor.lu *and* andre.rifaut@tudor.lu

***Abstract*—This paper describes the architecture of a policy regulation system and some of its related concepts dedicated to the application domain of computer network security context. The actual architecture is based on a methodology identifying the main phases addressing the needed reactions that could be realized in order to get out of a failure or an attack situation of a network.**

Policy management domain has already been largely discussed in the scientific literature. In fact, large panoply of works focusing on how to develop a policy framework taking into account the business goals, the organisational structure, the operational rules and the links between low-level policy and high-level one [13]. Nevertheless, it is notable that policy regulation remains an area where less work has been done, more specially the policy regulation according to business requirements.

This paper aims to propose a framework for policy regulation that integrates the business layer during the regulation phase.

***Index Terms*—Architecture, Policy, Regulation, Computer network security, Reaction.**

I. Introduction

Today telecommunication and information systems are more widely spread and mainly heterogeneous. This basically involves more complexity through their opening and their interconnection. Consequently, this has a dramatic drawback regarding threats that could occur on such networks via dangerous attacks. These attacks, continuously growing are based on all new attacks techniques, which are actually exposing operators as well as the end user.

The realm of security management of information and communication systems is actually facing many challenges, very often due to the fact that it is difficult to:

- Establish central or local permanent decision capabilities;
- Have the necessary level of information;
- Quickly collect the information, which is critical in case of an attack on a critical system node;
- Launch automated counter measures to quickly block a detected attack;
- Efficiently react against an attack, especially if this needs a change on an equipment configuration, which often necessitate many checks that have to be performed in order to avoid bad side effects (conflict creation, services stability, etc).

Thus, it is crucial to elaborate a strategy of reaction after detection against these attacks. This is mainly the subject of the work presented in this paper dealing with the concepts aiming at fulfilling the mission of optimising security and protection of communication and information systems. The principle is mainly to achieve the following:

- React quickly and efficiently to any simple attack but also to any complex and distributed ones. The reaction is organised in 2 steps: instantaneous reaction based on existing policy to avoided leaving vulnerability in the system and differed reaction aiming in adopting the based policy to avoided new attack occurrence.
- Ensure a homogeneous and smart communication system configuration, that are commonly considered and the main sources of vulnerabilities.

The different phases of an attack and the associated reaction processes are shown in Figure 1. This figure is extracted from the RED[1] project principle [12]. As a partner of this project, our main contribution is actually related to the RED architecture as well as at the policy management level. Some

Manuscript received March 31, 2007. The National Research Ministry of Luxembourg supported this work in progress under a EUREKA project called RED which stands for: Reaction after Detection.

D. Khadraoui. Author is with the Centre de Recherche Public henri Tudor, Luxembourg, 29, Avenue John F. Kennedy, Kirchberg, Luxembourg (corresponding author to provide phone: +352 425991286; fax: +352 425991777; e-mail: djamel.khadraoui@ tudor.lu).

C. Feltus, B. de Rémont and A. Rifaut are also with the Centre de Recherche Public henri Tudor, Luxembourg, 29, Avenue John F. Kennedy, Kirchberg, Luxembourg.

[1] RED: REaction after Detection a European CELTIC project

of these primary elements of the contributions are presented in this paper. These are related to the way to exploit the RED architecture in the context of policy management and more especially in the perspective of policy regulation based on business governance. In [13] the authors presented an innovative and new mechanism for adapting the security policy of an information system according to the threat it receives, and hence its behaviour and the services it offers. This mechanism takes into account not only threats, but also legal constraints and other objectives of the organization operating this information system, taking into account multiple security objectives and providing several trade-off options between security objectives, performance objectives, and other operational constraints.
Our contributions are widely related to [13] in the sense that it uses the context principle of the Or-BAC modelling valid during the crisis period (intrusion context). Our approach is to adopt the same philosophy than in [13] in terms of regulation but at the same time it enhances the business involvement during the policy modification mechanism, which lays down the foundation of a new approach for the elaboration of methodological aspects strengthening the regulation perspectives.

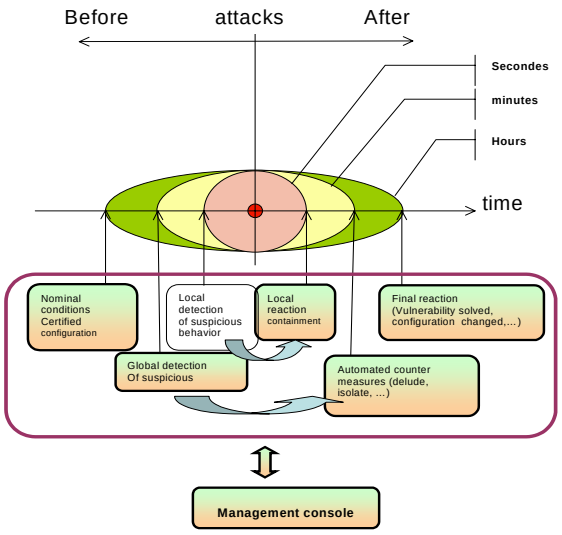

Figure 1: Different phases of attack and main processes

II. ARCHITECTURE

Since the early days of intrusion detection, the question of alert handling has been a daunting task for security officers. The original proposition of intrusion detection is the creation of a trustworthy audit trail that can show and track threats. Intrusion prevention has taken over, proposing to automate the reaction to alerts provided by intrusion detection devices. We are currently at a stage where intrusion-prevention devices, network-based or host-based, are capable of blocking undesired traffic, reconfiguring firewalls or quarantining undesired code.

Unfortunately, this state of the art leaves much to be desired in terms of coherent response. First of all, reaction is based on immediate detection, and is very close to the actual event or audit trail. As a result, the same action from the attacker is going to trigger the same local reaction to the perceived threat, hence possibly overloading the reaction device or the target information system. The location of the response is not optimal either, as the detection/prevention device may be deep into the network; the threat is therefore carried unchecked within the information system whereas it could be stopped earlier.
More fundamentally, the configuration of the response happening on the intrusion prevention device is left to an operator that may not be aware of the operational constraints of the information system or network, but is preoccupied by the protection of its (smaller) territory. Therefore, mistakes and undesired side effects are often likely to happen, or reaction is deactivated because of the fear of side effects.

The need for a more coherent approach to reaction is therefore important to progress in the direction of attack resilience and obtain more secure information systems. We propose to base this approach on policies, and more specifically on security policies and the OrBAC formalism.

More pragmatically, RED architecture consists in a regulation based upon policies. Indeed, the policy modification is a way to adapt the security of a global network. The corporate policy is defined once for all, and isn't modified by the regulation. As it's described on the left of the Figure 2, the corporate rules represent an input to the system, and to the regulation module. The corporate rules, combined with the new rules (issued from the policy's modification) are mapped into technical rules, as described in section IV (*Policy Based Regulation)*. The new technical rules are then instantiate on the network and on the related objects. It's in this instantiation that the reaction is really realized. Thus, at this point, the network reaches a new security status. New observations are realized on the network, and if necessary (as described in the section *IV, Methodology*), new business rules are defined. Optionally, before introducing these new rules in the system, an agreement could be asked to the owner of the corporate policy. This agreement can be automatic or not, depending on the context, the extend of application, the level of abstraction of the policy application's area, the policy owner agreement.

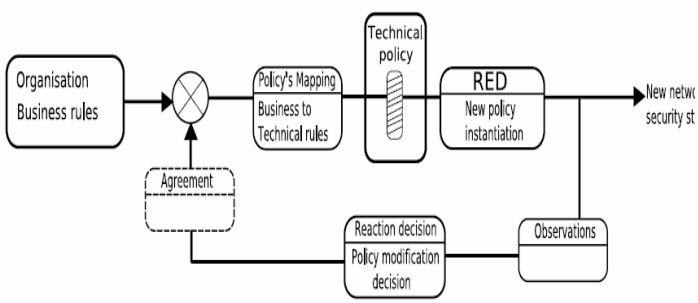

Figure 2 - RED architecture (basic elements)

The Figure 2 represents the main elements of the foreseen RED architecture. This takes the business rules as input, the policy regulation in the loop, and a new security status as output of the system. This is mainly relying on a policy adapted to a specific situation (context).

III. POLICY MANAGEMENT

In the literature, a large number of works has already been realized in the context of policy and policy deployment. The work around Ponder, a language for specifying management and security policies for distributed systems, has defined a policy as several rules that govern the choices in the behavior of a system. Security policy define which actions are allowed, for what, whom, and under which conditions [1, 2]. In [3], Travis Beaux et al. makes a survey over policies and classify the policies in term of:

- high-level *program policies* that address security goals, security staff and their responsibilities;
- *issue policies* that address a single legal or technical security issue such as properly handling financial or health care information, contingency planning, or remote connectivity; and
- *system policies* that concern low level technical policies that describe how to configure specific systems and applications.

Even if at the beginning, research about policies had largely been focused on low-level policy (technical policy), researchers have also devoted some attention to the policy's specification [9]. Arosha K. Bandara et al. [4] propose a method for refinement of high-level goals into operations that could be derived on implementable policies. In [5], Rifaut et al. explain the approach of formalizing BASEL II[2] and ORM[3] with goal models and the ISO/IEC 15504. They present in Figure 3 the idea that low-level policies are issue from higher-level policy.

[2] Basel Committee on Banking Supervision, "International Convergence of Capital Measurement and Capital Standards"; BIS; Basel, June 2004.

[3] Operational Risk Management

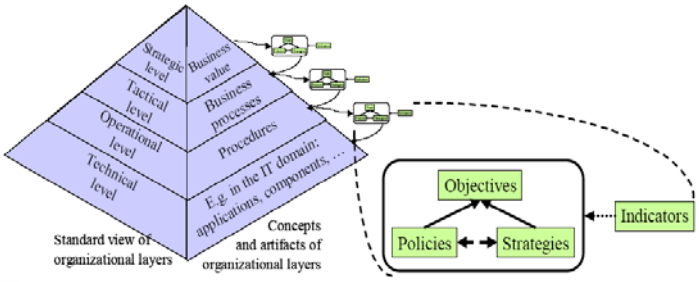

Figure 3: Policy refinement from high-level policies to low-level policies

The above Figure 3 presents a company's abstraction layer structured view from the strategic to the technical one. Policy refinement mechanism from the higher to the lower layer is strongly done in accordance with the corporate objectives down to the technical one. Indicators and strategies are omnipresent in the refinement process.

When an attack occurs, it is necessary to change of policy in emergency or to take action not allowed by the policy. This situation is current for IT employees, but IT managers most of the time do not define procedures to inform or to consult the business managers. In case of an attack or an unusual perturbation in the system, a major constraint in policy adaptation is that it's not allowed to modify low-level policy without referring before to the high level policy. Not taking care about that constraint may be the source of a bad business IT alignment.

The technical policy has to be issued in straight line from corporate policy. The structure between policies, or *policies' hierarchy*, implied that the low-level policy owner is fully accountable to the higher policy level owner. This can be illustrated by the following example:

A healthcare institute has got a corporate policy to ensure the confidentiality of the patient's records. This corporate policy (owned by the board of directors) mentions that only the patient's doctor has access to the patient files. Due to an IT incident (i.e. attack or system intrusion), the IT clerk needs the right to access these records but the IT policy denied such an access. In this case, adding new right to the IT clerk means a policy modification (or regulation) in contradiction with the corporate policy (or policy consign) and need consequently to be approved by the board of director (or by another procedure agreed by the same board).

IV. POLICY BASED REGULATION METHODOLOGY

In order to reach a modification of the policy, several steps are necessary. These steps are identified in specific modules as described in the following:

1) Measurement

First of all, we need to realize some security measures on the network's key elements. These elements could be data, service (DNS), critical applications, equipments, etc. All the unrefined measures should be gathered in a specific place in order to be

processed. This gathering could be done through a distributed solution or via a classic client/server application.

2) Detection

The detection module relies on an application able to parse the measured data representing the status of the entire network's security. In parsing the data coming from different elements, the application must be able to combine them with the last security states, in order to detect predefined failure or intrusion patterns if any.

3) Analysis

Once a pattern found, it is necessary to define which elements of the network are involved in (e.g. an *actor*, realizing an *action* on a (or several) *object*(s)). Considering these three elements, the found pattern and the current state of the network's security the policy's rule(s) to be added, removed or modified could be determined. Furthermore, in this module, it is important to take in to account the business policy, in order to respect it, and to avoid rules conflict generation.

4) Interpretation

Despite the analysis module, conflicts in the policy could appear. The potential modifications that could be applied to the policy must be interpreted. In interpreting a modification, it became possible to specify its consequences and thus, the possible conflicts between several rules. If a conflict is discovered, the application will try to solve it, avoiding a compromising configuration of the policy.

5) Alert

If a modification can be applied without generating any conflict and without modifying the policy, it becomes necessary to advertise the system (by sending an alert to the concerned actors or by logging the modification). If the modification concerns high-risk elements, an approval could be asked.

6) Reaction

To modify the policy, a new rule could be added and/or an older removed or modified, at the business rules level (not specifically and only the technical level). The technical policy corresponding to the new business policy will be generated and applied to the system. In the same way, the technical security could be modified in order to reinforce the network's security. Thus, the entire system becomes dynamic since it is mainly creating a looping feedback by adapting the measures to the new security status.

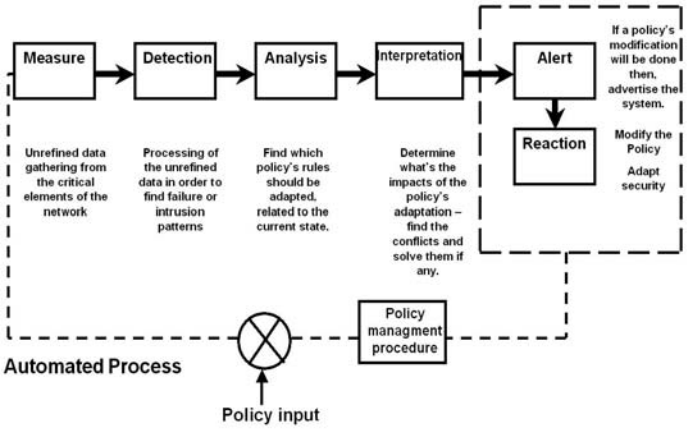

Figure 4: Methodology of the reaction.

The Figure 4 above represents the methodology used to emerge on a policy's modification, based on measures realized on the technical layer of the targeted infrastructure.

V. THE OR-BAC USE CASE

We illustrate the concept of policy regulation in the context of access control policy, and more precisely based on the Or-BAC model [6].

As explain by the author, none of the classical access control models such as DAC, MAC, RBAC, TBAC or TMAC [10, 11], is fully satisfactory to model security policies that are not restricted to static permissions but also include contextual rules related to permissions, prohibitions, obligations and recommendations. In [7], the context in Or-BAC is defined as: "*A context is viewed as an extra condition that must be satisfied to activate a given privilege* ". By using the Or-BAC model, the context can be associated to an emergency situation due to an IT perturbation (attack, intrusion or other). This kind of context is named intrusion context [13].

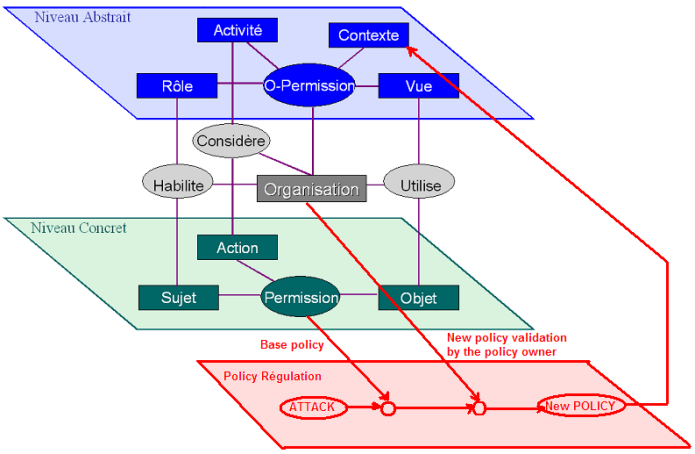

Figure 5: Policy regulation in the Or-BAC modelIn the Figure 5, we mainly added a layer (the bottom layer) in order to illustrate the proposed regulation process of section IV.

In this Or-BAC uses case, a basic policy (issued from the abstract level and validate by the business owner) is running

in the company at the concrete layer. When an attack occurs, the technical IT people first takes actions to face the problem and secondly, initiate a process to modify if necessary the basic policy. This policy modification of the basic policy needs to be validated or improved by the policy owner before being introduced in production, this correspond to the agreement bloc of the figure 2The new validated policy represents the input for the context element of the Or-BAC model at the abstract level.
According to the above example of section III, this means that the new policy may become operational if and only if the board of directors has deliver its opinion again the requested modification.

VI. Conclusion

In the context of this position paper, we have explained the objectives of the RED project in term of reaction after detection. We proposed to improve the regulation chain of policies regulation and adaptation after occurrence of an attack on the network. In our proposed solution, we give a major importance of the business agreement approval during the policy adaptation.

Policy regulation's automation needs in the first hand the existence of a hierarchy between the rules in case of multiple choices due to multiple attacks and in second hand an automatic method to validate the policy's modifications. Cuppens et al. explain in [8] that contexts (and all the concepts of its model like org, role, activity, view…) are organized hierarchically. Since that, when a conflict occurs, security rules associated with the higher context in the hierarchy will override the security rules associated with the lower contexts.

The next steps of our achievements will to concentrate more in the development and the elaboration of the reaction methodology, as well as to experimentally validate the automated way of a policy modification by the business or by the policy owner as it is illustrated in the actual paper.

Acknowledgment

The Ministry of Culture, Higher Education and Research of Luxembourg supports the on-going research work (EUREKA/CELTIC RED project). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding organizations.

References

[1] Charalambides, M., Flegkas, P., Pavlou, G., Bandara, A. K., Lupu, E. C., Russo, A., Dulay, N., Sloman, M., and Rubio-Loyola, J. 2005. Policy Conflict Analysis for Quality of Service Management. In Proceedings of the Sixth IEEE international Workshop on Policies For Distributed Systems and Networks (Policy'05) - Volume 00 (June 06 - 08, 2005). POLICY. IEEE Computer Society, Washington, DC, 99-108. DOI= http://dx.doi.org/10.1109/POLICY.2005.23

[2] N. Dulay, E. Lupu, M Sloman, N. Damianou A Policy Deployment Model for the Ponder Language, Proc. IEEE/IFIP International Symposium on Integrated Network Management (IM'2001), Seattle, May 2001.

[3] Travis Breaux, Annie I. Antón, Clare-Marie Karat and John Karat, Enforceability vs. Accountability in Electronic Policies, IEEE 7th International Workshop on Policies for Distributed Systems and Networks (POLICY'06), London, Ontario, Canada, pp. 227-230, 5-7 June 2006.

[4] Arosha Bandara, Emil Lupu, Jonathan Moffet, and Alessandra Russo, A Goal-based Approach to Policy Refinement, Proceedings 5th IEEE Workshop on Policies for Distributed Systems and Networks, New York, USA, 2004

[5] A. Rifaut and C. Feltus, Improving Operational Risk Management Systems by Formalizing the Basel II Regulation with Goal Models and the ISO/IEC 15504 Approach, Proceeding, REMO2V'2006, International Workshop on Regulations Modelling and their Validation & Verification, to be held in conjunction with the 18th Conference on Advanced Information System Engineering (CAiSE'06), 6 June 2006, Luxembourg

[6] A. Abou El Kalam, R. El Baida, P. Balbiani, S. Benferhat, F. Cuppens, Y. Deswarte, Miège, C. Saurel et G. Trouessin, Organization Based Access Control. IEEE 4th International Workshop on Policies for Distributed Systems and Networks (Policy 2003), Lake Come, Italy, June 4-6, 2003.

[7] F.Cuppens and A.Miège, Modelling contexts in the Or-BAC model, 19th Annual Computer Security Applications Conference, Las Vegas, December, 2003

[8] Cuppens, F., Cuppens-Boulahia, N., Mi`ege, A.: Inheritance hierarchies in the Or-BAC Model and application in a network environment. In: Second Foundations ofComputer Security Workshop (FCS'04), Turku, Finland (2004) 14. Ullman, J.D.: Principles of Database and Knowledge Base

[9] S. Illner, H. Krumm, A. Pohl, I. Lück, D. Manka, and T. Sparenberg Policy Controlled Automated Management of Distributed and Embedded Service Systems Parallel and Distributed Computing and Networks, PDCN 2005, Innsbruck, Austria

[10] D.F. Ferraiolo and D.R. Kuhn (1992) "Role Based Access Control" 15th National Computer Security Conference

[11] R. S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman (1996), "Role-Based Access Control Models", IEEE Computer 29(2): 38-47, IEEE Press, 1996.

[12] RED (REaction after Detection) – CELTIC Project. http://www.celtic-initiative.org/red

[13] H. Debar, Y. Thomas, N. Boulahia-Cuppens, F. Cuppens Using contextual security policies for threat response . Third GI International Conference on Detection of Intrusions & Malware, and Vulnerability Assessment (DIMVA). Germany. Juillet 2006.