
IBIMA
Publishing
mobile

Journal of Information Assurance & Cybersecurity

Vol. 2013 (2013), Article ID 934483, 33 minipages.
DOI:10.5171/2013.934483
www.ibimapublishing.com

Research Article

A Cooperative Agent-based Security Framework

Authors

Carlos Rompante Cunha, João Pedro Gomes and Elisabete Paulo Morais

Polytechnic Institute of Bragança – EsACT, Mirandela, Portugal

Received 16 February 2013; Accepted 20 May 2013; Published 30 September 2013

Cite this Article as: Carlos Rompante Cunha, João Pedro Gomes and Elisabete Paulo Morais (2013), "A Cooperative Agent-based Security Framework," Journal of Information Assurance & Cybersecurity, Vol. 2013 (2013), Article ID 934483, DOI: 10.5171/2013. 934483

Abstract

The actual economic paradigm is based on a strongly cooperative model that tries to support a more competitive and global organizations response. With cooperation comes an intrinsic need - interconnection and interoperability of information systems among business partners. This represents, in many areas, a huge organizational challenge, being the field of information, and communication security one emerging key issue and a natural enabler for cooperative behavior and to the proper establishment and support of trust among network partners. Security frameworks, that can be able to describe and act on the basis of interoperability, cooperation and proactivity, became essential to support the new needs of modern business models. This paper present a framework that aims to contribute to a

sustainable organizational information security-processes support, based on the ability to describe the allowed business process interactions among cooperative partners; furthermore, the framework presents a cooperative security perspective among partners basis on the idea that, if organizations have business cooperation, they should also have active security cooperation and regulation. If organizations, that need to cooperate, do not feel secure when they interconnect their information systems, the all cooperative perspective can fall down. Trust being one basic need for cooperation, impulse the need of a new security approach for cooperative scenarios.

Keywords: Security, framework, cooperation, agents.

Introduction

Modern business paradigms are built on the established perspective that organization can't be isolated environments but they must be strongly cooperative environments. Being organizations "cooperative islands", and having them business processes supported by information processes, inevitability emerges the need for interoperability on their Information System (IS), in order to have information interchange and, in a more mature vision, the generation of knowledge obtained from the intersection of information and skills of all links in the cooperative network, that in a pure cooperation perspective must converge to a common goal or at least in a symbiotic relationship.

Among the set of challenges that exists in organizations cooperation, we focus on the security.

Our approach is based on the principle that organizations can and should maintain their individuality in what concerns to their internal security policies but at the same time must have a secure support to business interoperability, and a cooperative vision of security as a principle of cooperation. Interconnect IS cannot translate on the weakening of individual security, nor result in a cooperative network that, needing to interoperability their IS, neglect the individual security and/or materializes an insecure cooperative network. In our opinion it is necessary to rethink the security models in order to support such business models and we think that business networking don't should stop on business

cooperation, but should necessary have a security cooperative layer when cooperative network is build.

The Business Perspective

Organizations are seeking today, so incessant and increasingly desperate, new business models, suitable to the paradigm of Digital Economy (Österle et al., 2001). In this search, the concept of relationship amounts to becoming crucial to the success of organizations (Tapscott, 2002). In order to achieve these relationships organizations have been pursuing the establishment of partnerships, upstream and downstream of theirs core business and embarked on mergers and/or acquisitions. This drive is an embodiment of the networking capability, which boils down to the ability that organizations

must establish mechanisms for cooperation with other organizations, through rapid and efficient bundling of business, supported by technology platforms (Österle et al., 2001). There are many reasons for inter-organizational cooperation, there are many prominent examples: the pharmaceutical industry in the development of collaborative R&D projects or open source community, in the development of software systems (Buxman and König, 2000).

The perspective of networking, envisions a model able to withstand the challenges of cooperation networks, being the timely-concept of cooperation networks a more static or more dynamic interrelationship. Particularly the dynamic perspective of cooperation, where the cooperative network is rapidly changing by the in/out partners movements, will incur in

additional complexity of IS security models, and will demand a more exigent and efficient management.

The Information System Perspective

Today and tomorrow, urges consider new ways and structures for business; to be based on our ability to re-think IS and believes that the information is the foundation of business success (Edwards et al., 1991). Based on this perspective, organizations spend a significant part of their time/capabilities in creating IS that can materialize competitive advantage for their business.

Companies around the world are gradually and consistently, to be more interconnected (Davenport, 2000). According to a perspective of business networking, the requirements in terms of

IS are significantly increased if compared to the models of the organizations working in isolation. This implies that if organizations leave a more surround-closed definition of business and starts to be open systems capable of supporting interoperability with other organizations. The vision of individual tradition security will fall, and will emerge a more unified security perspective.

We are interested in IS highly integrated, and environments of strong cooperation. Such environments have constant exchange of information among cooperating IS, and multiple shared accesses to databases of information in order to support and facilitate the business processes across the network. Particularly we refer to the change of perspective in the generation of

knowledge - now only possible thanks to the interoperability and information sharing of all IS.

Although this view of IS evoke multiple areas of research are particularly interested in the security field. We are aware that a cooperative environment is particularly adverse to the implementation of security models effective-capable.

An Agent-Based Security Framework

This chapter explains the framework vision and present is components, trying to focus on the role and contribute of each one for the implementation of a security cooperative approach.

Framework Perspective

Cooperative security architecture should protect the specificity of each organization but without compromising the necessary interoperability. This principle stems from the requirement that each organization is free to establish their internal security policies.

An interconnection among IS necessarily lead to a greater potential fragility of individual IS, as it requires extending the access permissions to resources that were previously inaccessible to the external context. But the interconnection of IS is necessary for support cooperation.

For the basic principles that should govern the planning of the security architecture should reflect these (Bishop, 2003):

- Minimum privileges: an organization IS shall have only the privileges absolutely necessary to complete their tasks.

- Fault / Denial default: unless a given object have been given at the time of its creation, explicit access permissions, it should be denied is access.

- Access control: there should be a mediation in order to determine whether a given entity that requests the use of a privilege or may not enjoy the same.

- Open architecture: the robustness of the architecture should not only reside in the aspects of secrecy of its construction.

- Psychologically accepted: the security architecture should not be an obstacle to usability and interoperability of IS and an obstacle to the normal work of the organizational internal collaborators.

All access to the resources of each organization can only be reached in one of two ways: either it is a programmed access that will be accepted, or is "request for access" that is not scheduled and that will be subject to evaluation according to the rules pre-established (or if they are missing through human decision).

The security architecture should monitor all access in order to detect abnormal patterns of behavior and possibly trigger alarms and/or take safeguard measures to keep the network safe. It is also have complementary action by automatically inform all partners about the abnormality and measures taken (if this is the procedure expressed by the predefined rules), thereby ensuring that each of the IS of the cooperation network can implement their individuals measures in accordance with their rules, fostering a desirable group reaction.

The prospect of security should always be cooperative (preserving the individuality of each partner), in the sense that the security systems of each partner should share information with each others, leading to increased the security of the group.

The Proposal Framework Architecture

To operationalize these principles of architecture proposes a model that we hope to demonstrate, by implementing a prototype to be able to implement a consistent security policy based on rules and whose skills fit the access control and intrusion detection and cooperation. This architecture should be able to detect abnormal behavior that departs resources business partners of the cooperation network to mirror the relationship of trust between business partners. The Figure 1 presented our Framework Architecture that is after explained, in a components-contribution approach.

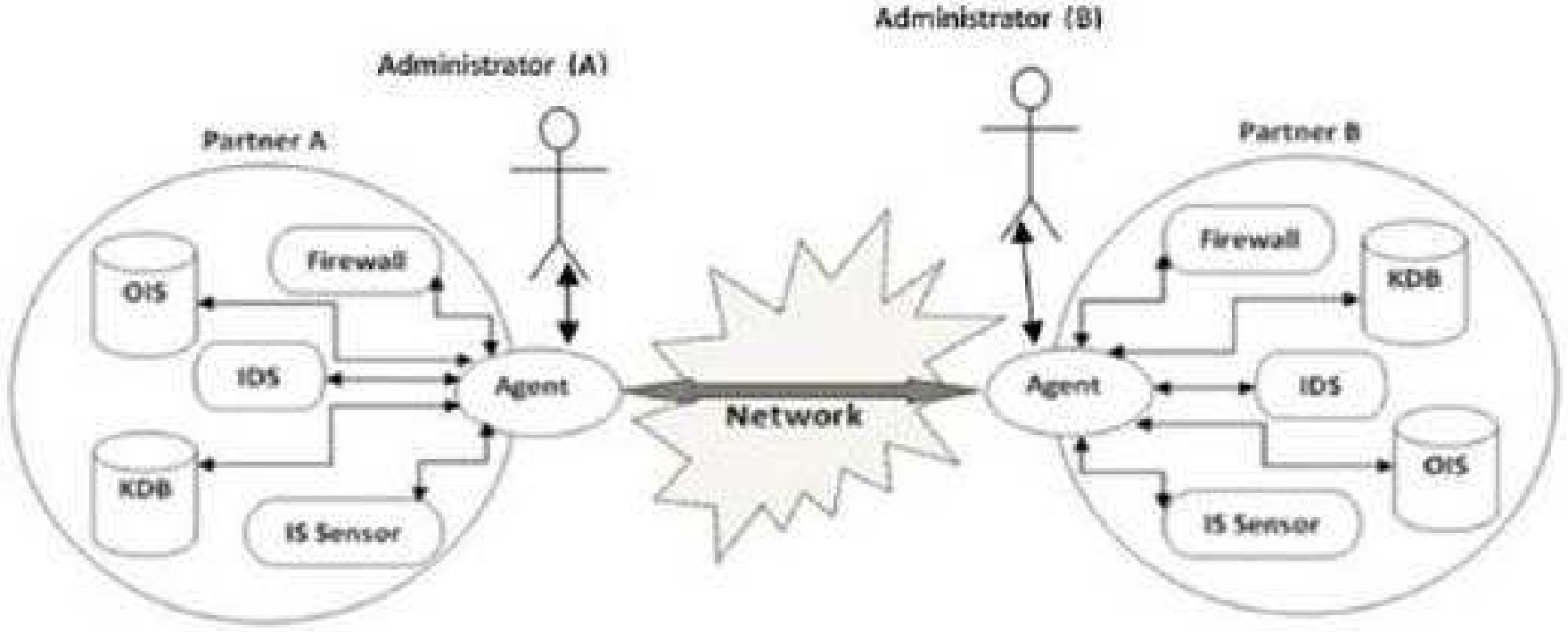

Fig 1. Framework Architecture: An Example for Two Cooperating Organizations

Framework Components

***Intrusion Detection System (IDS)*:** Resource able to detect patterns of attacks (e.g. DoS) from the observation of abnormal behavior and inconsistent with existing security policies (Denning, 1987). IDS are particularly important for detecting internet patens attacks, but it lack in mostly on recognizing traffic that seems innocuous but hasn't an organization logical context (and in this case is suspicious). This is also a common approach focuses on the belief that the potential threat is outside the organization and not inside. Defense against internal attacks is typically neglected (Dayarathna, 2009)

***Firewall*:** Entity responsible for mediating access to the network, allowing or denying certain types of access on a given security policy (Bishop, 2003). This is a helpfully framework-component and it is the typically way of blocking traffic, based in rules that, as the IDS cannot easily describe the business workflow perspective.

***Knowledge Data Base (KDB)*:** This component has a description that translates the organizational cooperation rules, based in a business perspective and bridging the gap between business security rule and security technical rules. This will be the repository where will be described how each agent should assess and decide the action to the situations they encounter. This entity must translate the adaptive relations of trust among network partners.

It should be noted that this KDB should describe the behavior and Interoperation accepted as normal among business partners contributing to the blockage of the inadvertent and inappropriate actions that depart from elements of the same network or from cooperative partners. It is a key element of the security architecture for its ability to describe the very model of cooperation and interoperability.

***Internal Security Sensor (IS Sensor)*:** Although some of the described technologies, such as IDS, whose detection engine and approach can be very diversified (Teodoro et al., 2009) can be used to oppose to domestic attacks and also to better understand the behavior of their users, looking how these technologies are used in organizations allows us to verify that there is a clear tendency to use them only as a shield against attacks from

outside. In this context IS sensor is a component that should translate the internal attack point-of-view and should result as an internal IDS component. Controlling the internal users is particularly important on cooperative scenarios, because internal collaborators can have a privileged access to resources of cooperative partners, and their actions should be controlled.

***Agent*:** This component is responsible for, after consulting its Knowledge Database (KDB), act to safeguard organizational interests by cooperating with the IDS and the FW. The agent should be responsible for granting or denying requests for access to resources on your network. It should also, after consultation with the KDB, decide the reconfiguration of the FW and IDS, notify the system administrator and / or other agents of the organizations of the cooperation network (where they will act in

accordance with their KDB) to redefine the policies established. This must be proactive by its ability to predict and report before things go wrong.

***Administrator*:** Receive alerts and manage the agent. He is the maximum responsible in the working-maturity of the agent enabling that the agent reflects the correct security policy that the organization wants to apply.

***Organization Information System (OIS)*:** This framework component represents the organizational information system, which only can be reached through the Agent.

Framework Implementation: One Overview of Our Work in Progress

The proposal framework architecture implementation is currently being study. Interoperability is a very hard task because organization IS typically grows up in an unique way and their security structures also: they face the IS heterogeneity problems. So, when organizations need to cooperate, they face the problem of interconnect and full interoperate their systems.

Fortunately, in the last year, the Service Orientated Architectures (SOA) has contributed to bridge the gap between interoperability problems. Currently an architecture based on services using web services is one of the best options in use to promote

interoperability among heterogeneous information systems (Liu et al, 2009).

Web services are considered as a mean to improve interoperability among heterogeneous applications, in several domain organizations. For instance, they are commonly accepted and increasingly used approach to m-commerce, as stated in (Chen et. al., 2007; Kim et. al., 2006) or in health systems, where web services are used to promote interoperability among heterogeneous information systems (Serbanati et al, 2011).

We think that SOA approach should be the mainstream of the framework architecture implementation, in what concerns to the support of the interoperability among the different agents, and how they can communicate among themselves.

Artificial Intelligence (AI) is also one other key issue to implement the proposal architecture. AI is needed to insure that the agent can be able to decide correctly in all different kinds of requests, being also capable of learning with his decisions/results and the decisions of the Administrator.

Execution Primitives represent the agent-component capable of interact with the security components of the organization (e.g. IDS, Firewall). This component should be, typically, one organization-unique implementation, because it must match with the specificity of the security components of each organization.

The Agent component referred in the Figure 1, can be represented, in a more detailed implementation perspective, in

Figure 2, where he show the role of SOA and AI in the functioning of the Agent.

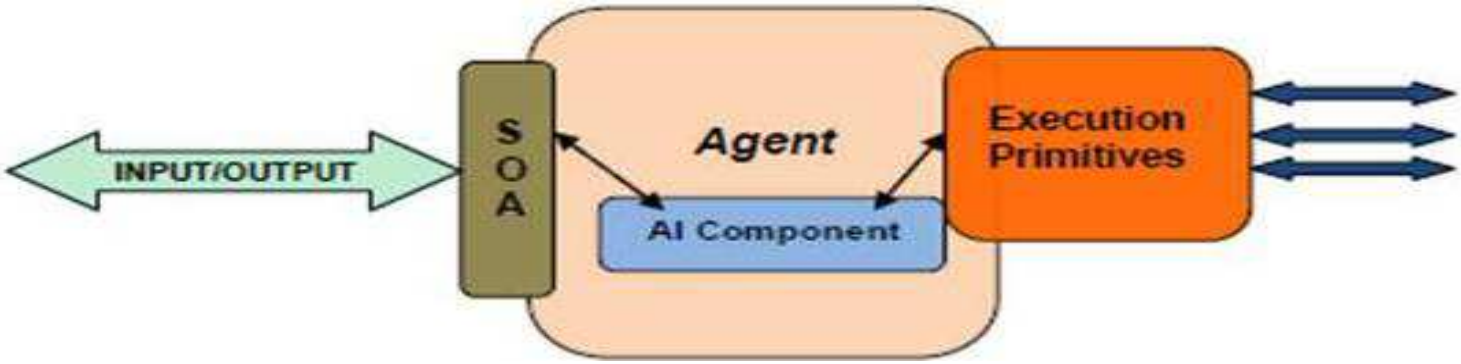

Fig 2. Agent Component

Conclusion and Final Remarks

This paper, presents a security framework for cooperative scenarios, based on an agent-based security framework. It is also

focus on the maintenance of individual organizational security policies control. It contributes for a better description of security rules, policies and actions in a business cooperative perspective and not on a security-only view. This framework also works on a full cooperation perspective for security cooperation that should exist among partners of a cooperative network. Implementation of the presented architecture is also discussed and there are pointed solutions for prototype this framework. We believe that only with strong and reliable security architectures organizations can face the problems and challenges of a more and more networked vision of an organization. This paper is a contribution for business cooperative scenarios, and especially for the implementation a cooperative perspective of security among organizations.

References

Bishop, M. (2003). 'Computer Security: Art and Science,' *Addison Wesley*, 2ª Edition.

Buxman, P. & Konig, W.. (2000). Inter-organizational Cooperation with SAP Systems, *Springer*.

Chen, M., Zhang, D. & Zhou, L. (2007). “Empowering Collaborative Commerce with Web Services Enabled Business Process Management Systems,” *Decision Support Systems*, vol. 43, no. 2, 2007, pp. 530-546.

Davenport, T. H. (2000). Mission Critical, *Harvard Business Press*.

Dayarathna, R. (2009). “The Principle of Security Safeguards: Unauthorized Activities,” *Computer Law and Security Review*, vol. 25, pp. 165-172.

Denning, D. E. (1987). “An Intrusion-Detection Model,” *IEEE Transaction on Software Engineering*.

Edwards, C., Ward, J. & Bytheway, A. (1991). The Essence of Information Systems, *Prentice Hall*, 2ª Edition.

Kim, W., Chung, M. J., Qureshi, K. & Choi, Y. K. (2006). “WSCPC: An Architecture Using Semantic Web Services for Collaborative Product Commerce,” *Computers in Industry*, vol. 57, no. 8-9, pp. 787-796.

Liu, V., Franco, L., Caelli, W., May, L. & Sahana, T. (2009). “Open and Trusted Information Systems/Health Informatics Access Control (OTHIS/HIAC),” *Proceedings of 7th Australian Information Security Conference*. Wellington, New Zealand, 99-108.

Österle, H., Fleisch, E. & Alt, R. (2001). Business Networking: Shaping Collaboration between Enterprise, *Springer*, 2ª Edition.

Serbanati, L. D., Ricci, F. L., Mercurio, G. & Vasilateanu, A. (2011). “Steps towards a Digital Health Ecosystem,” *Journal on Biomedical Informatics*.

Tapscoot, D. (2002). 'Winning through Relationship Capital: A New Presentation,' 2002

Teodoro, G. et al., (2009). “Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges,” *Computers and Security*, vol. 28, pp. 18-28.