A Knowledge Management Framework for Security Assessment in a Multi Agent PKI-based Networking Environment

Gustavo A. Santana Torrellas
Instituto Mexicano del Petróleo
Perforación y Mantenimiento de Pozos
Eje Central Lázaro Cárdenas N°152
CP 07730, México, D.F
gasantan@imp.mx

Abstract

This paper deals with one of the probably most challenging and, in our opinion, little addressed question that can be found in Information Security Management today, that of the methodological design of a Multi-Agent PKI-based Networking Environment. It relies on three important notions: (1) independence from the implementation techniques; (2) definition of a Multi-Agent System as a set of three different levels of roles; (3) specification of a methodological process that reconciles both the bottom-up and the top-down approaches to the problem of system design using a Knowledge Management Framework. As dynamic and flexible domains such as PKI-based Network Environment are continuing to grow in complexity, it becomes more difficult to evaluate and define a proper risk management and their security goals in the domains where unexpected events can occur. This paper presented an information and knowledge management framework to support a Security Architecture using Multi Agent Technology in a PKI-based Network Environment domain. We employ the concepts related to SAMARA – A Security Architecture Multi-Agents Systems Risk Assessment. The focus of this paper is to define a knowledge management framework for self-organization and information security exchange among SAMARA agents. It addresses two important issues: (1) How the information and security knowledge should take place among agents to allow them to respond successfully to user requests and unexpected situations in the security domain; and (2) How individual agents should be interconnected so that their security capabilities are efficiently used and their security goals are accomplished effectively and efficiently. Knowledge can be exchanged among the agents by using a combination of facts, rules and commands transfers. A Distributed Security Assessment in Multi Agent PKI-based Networking Environment can be characterized as a group of individual agents running security tasks and co-operating with other agents to solve a security deployment and maintenance problem. In this article we propose a framework for developing an Organizational Information Security using Knowledge Management. It is anticipated that application of this framework will facilitate development of new Security Models that are better suited to the Risk Assessment in PKI-based Networking Environment characterized by dynamic and discontinuous changes..

1.1. Introduction

1.1.1. The “Sine qua non” of Information Security

In the current networked world, it is clear that security has become a “sine qua non” condition for serious public and private commercial, administrative and technical activities carried out by means of network applications. Communication without security is dangerous because third parties can easily read, forge, or block messages. To deploy security within closed user groups, secret-key cryptography could be a solution, but when it comes to open groups of users (as in the case of Internet) public-key cryptography represents today the most used technique. It permits to easily obtain integrity and confidentiality for the data exchanged between network applications, and also authentication of the involved parties. But the deployment of public key cryptography in worldwide networks requires the so-called *public key infrastructure* (PKI) that plays the role of a trusted third party, enabling trust and confidence in network environments. Now coming into the topic of the paper, the problem of security system management is always a complex one in real-life IT systems. The solution to such problems must not ignore the security aspect.

It is highly possible that an agent with a responsibility in a dynamic environment faces unexpected events. In order to be responsive, the agents should have enough knowledge to deal with unexpected events. If an agent is not able to deal with a particular event on its own, it can take the following actions: 1) Learn how to solve the problem by experimenting with different solution strategies. 2) Let some other knowledgeable agent solve the problem and then use the results. 3) Learn how to solve the particular problem by acquiring the necessary knowledge from other agents capable of solving the problem. 4) Ignore the unexpected event.

For a real time application domain such as the Security in a PKI-based Networking Environment, action 1 may not be suitable because it may take a long time to obtain the solution. Action 2 is a natural way for co-operating agents to solve the problem. However, it is not suitable for scenarios where there are large volumes of data involved in either the event or result. For action 3, there may be no huge volume of network transferred data; however, the agents themselves must be quite sophisticated. They need temporarily (maybe permanently) to keep the knowledge acquired from other agents and then to learn how to use this knowledge to solve the particular problem.

For the domain of Security in a PKI-based Networking Environment, we proposed a multi-agent framework for Security in a PKI-based Networking Environment (SAMARA – Security Architecture Multi Agent Risk Assessment). SAMARA is a closely collaborating agent system in which every agent has its own specialised capabilities and knowledge, and no one agent has the whole knowledge about the security world. All the security task specific SAMARA agents are situated on different host or nodes in the network environment. Hence we need to concern about huge volume data transfers over a network. Based on the discussion above, the SAMARA agents will take actions 2 and 4 listed above to deal with a particular event. The objective of this paper is to investigate and recommend a framework to support distributed problem solving for action 2. In this paper, we address two important issues:

> 1) How individual agents should be interconnected so that their capacities are efficiently used and their security goals are accomplished effectively and efficiently.
> 2) How the information and knowledge transfer should take place among agents to allow them to respond successfully to user's request and unexpected situations in outside world.

A variety of conceptual frameworks can be useful in planning and designing Information Systems and Information Security Processes. From our point of view these frameworks help ensure that a plan relates to individual and organizational development and to systemic change. The following frameworks, considered together, provide guidance in planning comprehensive, Systemic Security Model using a Knowledge Management approach:

> **Building a Information Security Knowledge Base**. The purpose of this phase is to acquire new Information Security Knowledge and information and to build a conceptual understanding of it.
> **Analyzing Real Security Models and Environments**. The purpose of this phase is to study security cases and examples in order to develop a practical understanding of the research.

Reflecting on Your Security Practice. The purpose of this phase is to analyse your security practice on the basis of new Information Security Knowledge.

Changing Your Security Practice. The purpose of this phase is to translate your new Information Security Knowledge into individual and collaborative plans and actions for organizational and transactional change. Activities might include action research, peer-coaching, support groups, and security empowerment.

Gaining and Sharing Security Expertise. The purpose of this phase is to continue to refine your instructional practice, Information Systems and Security with and from colleagues while also sharing your practical wisdom with your peers.

Using previous considerations for classify information security models suggest a five steps model that are useful for accomplishing the goals of security development:

- Risk Assessment Guided Development.
- Observation and Risk Assessment.
- Involvement in a Security Development
- Development of Security Improvement Process.
- Training in Information Security.
- Inquiry and Compliance.

The breakdown of the rest of this paper is as follows: Section 2 gives some background about the applications of agents in Security in a PKI-based Networking Environment domain. Section 3 briefly describes the SAMARA framework. Section 4 discusses in detail the information and knowledge management exchange framework used in the SAMARA agents. Section 5 gives the conclusion for this paper.

1.2. Conceptual Framework for Information Systems and Security-based Approach

1.2.1. Background of Information Security

In order to introduce the reader into the specificity of the problem, it is necessary to explain some of the security notions that will be used in the paper.

The access into a secure information system must always respect a preliminary procedure. The system needs the means to verify the entity requesting login and this process is known as *authentication*. Authentication is always composed of two steps that is the identity of the entity willing to enter the system should be acknowledged (*identification*) and verified (*verification*). During the identification step, the entity presents an identifier to the security system. Identifiers should be assigned carefully, because authenticated identities are the basis for other security services, such as access control service (i.e., authorization). During the verification step, the system generates authentication information that confirms the binding between the entity and the identifier. Since the process of authentication is straightforward and implies only identification and verification of the identity of a certain user, a secure system must have the means for allowing or limiting the rights that user may have inside the system after being authenticated. This is called shortly *access control* or *authorization*.

Authorization denominates the process of granting rights to a user of an information system. Once you have authenticated a user, the user may be authorized to perform different types of access or activity. Typically, a user logs in just once, and then he is transparently granted access to a variety of permitted resources, with no further login being required until the user logs out. Single sign-on prevents users from choosing bad passwords, a major component of systems insecurity and is therefore highly desirable but difficult to implement. Automatic authentication/authorization can be easily obtained by a cryptographic challenge based on public keys: one key per user, per node or per application server. Therefore such a system has the advantages of being user friendly and enabling authentication to be managed consistently across an entire enterprise, and has the disadvantage of requiring all hosts and applications to trust the same authentication mechanism. In general, authorization to computing resources is classified into two main categories: ACL-based authorization and capability-based authorization.

In the second category, capability is usually represented by a *token*: an unforgivable data value (sometimes called a *ticket*) that gives the holder the right to access a system resource. Possession of the token is accepted by a system as proof that the holder has been authorized to access the resource named by the token. This type of authorization has the disadvantage of being less practical and more prone to attacks. The usual way authorization is granted is by means of the so-called *access control lists* (ACL) — these are lists of entities, together with their access rights, which are authorized to have access to a resource. A form of identity-based access control is the *role-based access control* (RBAC) where the system entities that are identified and controlled are functional positions in an organization or process.

Intelligent agents are software that act on behalf of their human users in order to carry out arduous information gathering and processing security tasks, such as locating and accessing information from various on-line information sources, resolving inconsistencies in the retrieved information, filtering away irrelevant or unwanted information, integrating information from heterogeneous information sources and adapting over time to their human user's information needs. Intelligent agents work by allowing people to delegate works that they could have done, to the agent software. Agents can automate repetitive security tasks, remember things you forget, intelligently summarize complex data, learn from you, and even make recommendations to you.

The agent technology is especially suitable to address those issues concerning the security portfolio management domain. Recently, author analyzed the security assessment task of the security portfolio management domain, pointed out that this is the security task of providing an integrated security status picture for managing a security portfolio over time, using the information resources already available over the

Internet. This security task environment has many interesting features, including: (1) the enormous amount of continually changing, and generally unorganized information available about threats and viruses, (2) the variety of kinds of information that can and should be brought to bear on the security task (security policy environment data, security assessment status data, security and trust models, analysts' security reports, viruses alarm news, etc.), (3) the many sources of uncertainty and dynamic change in the environment.

The overall security task in the security portfolio management domain is to provide the best possible rate of return for a specified level of risk, or conversely, to achieve a specified rate of return with the lowest possible risks. A multi-agent system approach is natural for security portfolio monitoring because the multiple control threads in such a computational model are a natural match for the distributed and ever-changing nature of the underlying sources of data and news that affect higher-level decision-making process. A multi-agent system can more easily manage the detection and response to important time-critical information that could appear suddenly at any of a large number of different information sources. A multi-agent system provides a natural mapping of the multiple types of expertise to be brought to bear during any security portfolio management decision-making. Rus and Subramanian, in 1997, presented a customizable architecture for software agents that capture and access information in large, heterogeneous, distributed electronic repositories. The key idea is to exploit underlying structure at various levels of granularity to build high-level security assessments indices with security task specific interpretations. Information agents construct such security indices and are configured as a network of reusable modules called structure security detectors and security assessment analyzers. They illustrate their architecture with the design and implementation of smart information filters in two contexts: retrieving security policy environment data from Internet newsgroups and retrieving technical reports from Internet FTP sites. Santana [2] presented a methodology of studying the complex phenomena emerging in security policy environments. Their methodology is based on the use of distributed multi-agent models with minimal knowledge representation and reasoning capabilities that have proven to be a powerful modeling tool for complex security systems. Unlike neural models, they reported that their models allow a comparative and incremental evaluation of validity and relevance to the observed phenomena. The possibility of their application to the modeling and study of security policy environment phenomena was demonstrated on a simple example of a central agency that regulates the behavior of the security assessment agents. Delgado et al., in 1999, investigated a hybrid learning system that combines different fuzzy modeling techniques. In order to implement the different methods, they proposed the use of intelligent agents, which collaborate by means of a multi-agent architecture. This approach, involving agents that embody the different problem solving methods, is a potentially useful strategy for enhancing the power of fuzzy modeling systems.

Working with security policy environments requires constant monitoring of the continuously changing security information, and the ability to take decision instantaneously based on certain rules as the changes occur. We recently reported a framework for implementing a deliberative multi-agent system for this domain. This system can be used as a proactive tool for expressing and putting to work high-level Security in a PKI-based Networking Environment strategy. In the framework, agents are able to monitor and extract the security policy environment information via the World Wide Web and, using the domain knowledge provided in the form of feasible rules, can reason in order to achieve the established security goals.

Even though there are several agent-based approaches reported in literature that address the issues in the security domain, most of the current agent-based approaches focus on how to get the information from the distributed resource (the Internet). The use of intelligent agents to support decisions has not been thoroughly explored and merits serious consideration. In current practice, security portfolio management is carried out by security policy agencies that employ teams of specialized security agents for finding, filtering and evaluating relevant information. Based on their evaluation and on predictions of the economic future, the specialized security agents make suggestions about delivering or deploying various security status instruments.

The current practice, as well as software engineering considerations, motivates our research in multiple agent systems for the Security management. A multiple agent system approach is natural for security portfolio management because of the multiplicity of information sources and the different expertise that must be brought to bear to produce a good recommendation for a Security buy or deploy decision.

1.3 General Structure of Information Security with Knowledge Management and Multi-Agent Systems Engineering – SAMARA Framework

We begin by identifying some of the various types of Information Security Knowledge that administrators need to know:

- Conceptual Information Security Knowledge, such as the concept of confidentiality, integrity and availability.

- Factual Information Security Knowledge, such as the risk assessment and risk evaluation.

- Representational Information Security Knowledge, such as how to draw and use a security policy.

- Strategic Information Security Knowledge, such as the ability to recognise the applicability of a concept, such as, confidentiality is conserved when there are no external risks or threats, or that security state is conserved when there are no non-standard attacks.

- Meta-cognitive Information Security Knowledge, for example, the awareness of underlying security assumptions, or that an answer should be checked by solving the problem a different way.

- Self Information Security Knowledge, such as knowing one's likely sources of mistakes, or knowing that one should be more procedural when solving security problems.

- Operational Information Security Knowledge, such as how to take the information security procedures in a safe state.

- Procedural Information Security Knowledge, such as when to use a policy schema, or when to specify a co-ordinate actions in order to fix problems, or when to re-adequate a policy framework.

- Problem-state Information Security Knowledge, which are the features of a problem used for deciding how to solve it. Examples are: knowing that there are no external attacks in a particular problem, or that there are no risk measures in the problem.

In order to discuss the organizational and structural aspects of Information Security using Knowledge Management, we have found it convenient to broadly classify these types into three general categories. We call these three groups: Conceptual Information Security Knowledge, Operational and Procedural Information Security Knowledge, and Problem-State Information Security Knowledge.

We are developing an agent-based planning and control system for a flexible network security system with multiple policies agents. The input of the system is the general policy model of the network to be protected. The output of the system is the final security's state network. The general flow diagram that indicates the global operation of the system is shown in Figure 1. This flow is mainly divided in two stages: an off-line stage and an on-line stage. The off-line stage performs network security task decomposition. It produces a preliminary security plan that consists of a sequence of security procedures and operations and the precedence relationships among them. The input to this off-line stage is the general policy model of a system that is composed of parts. It then generates a preliminary security assessment plan based on risk analysis and vulnerabilities evaluations about accessibility and network stability. The security assessment operations that make up a preliminary information security plan are task level operations. Currently we have implemented two such operations:

- Security Requirements Assessment

- Threat & Risk Assessment

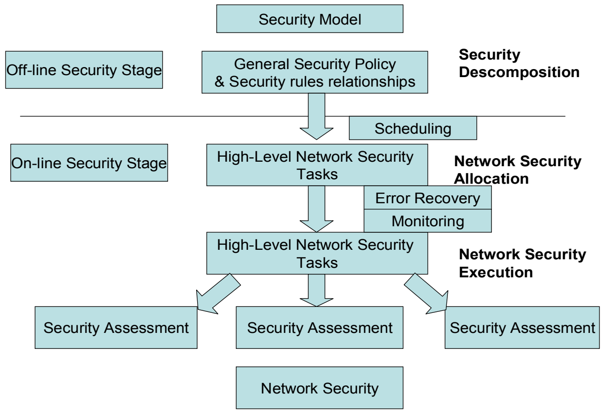

Fig. 1. A representation of an expert's structure of Information Security Knowledge with Multi Agent

This new Information Security using a Knowledge Management approach elements is what some refer to as a schema and often involves problem-state Information Security Knowledge as well. Since the Information Security Knowledge element is conceptual in nature, it becomes replicated (i.e., repeated) in the conceptual bubble. Security Knowledge is one, if not the, principal factor that makes personal, organizational, and societal intelligent behavior possible. Given the importance of Information Security Knowledge in virtually all aspects of daily and commercial life, two Information Security Knowledge-related aspects are vital for viability and success at any level:

1. Information Security Knowledge assets - the valuable Security Knowledge available to be used or exploited - must be nurtured, preserved, and used to the largest extent possible by both individuals and organizations'.

2. Information Security Knowledge-related processes -- to create, build, compile, organize, transform, transfer, pool, apply , and safeguard Information Security Knowledge -- must be carefully and explicitly managed in all areas affected.

In this context, Information Security using Knowledge Management in organizations must be considered from two perspectives with different horizons and purposes (and, require very different expertise) although they to a large extent rely on the same insights in to the organization's Information Security Knowledge status. These perspectives are:

Information Systems and Security Perspective -- which focuses on why, where, and to what extent the organization must invest in or exploit Information Security Knowledge. Which strategies, products and services, alliances, acquisitions, or divestments should be considered from Information Security Knowledge-related points of view.

Information Systems and Security Management Perspective -- which focuses on determining, organizing, directing, and monitoring Information Security Knowledge-related activities required to achieve the desired Information Systems and Security strategies and objectives.

1.4 Information and knowledge management exchange framework for SAMARA in a PKI-based networked environment

SAMARA is a middle layer agent system between the demand side of information (i.e. security assessment agents in security policy environment) and the supply side of information (i.e. the Internet). The major functions of SAMARA include:

- Security information Retrieval – this function is not a unique function of our system. Nowadays many online security agents and commercial Security analysis software can provide this function. Thus our research does not focus on this field. Our system will provide this function because it is a basic requirement of security assessment agents and users. SAMARA will provide four categories of information retrieval:

  (a) security history and current security quotations, such as the information of Opening Security level, Highest Security level, Lowest Security level, Current Security level, Security Volume for the selected Security on given Security date;

  (b) browsing Security technical analysis charts, such as security level movement chart (for example Candlestick Chart), Security volume chart, and various technical indicators chart;

  (c) listed company's fundamental data and security status health information retrieval, such as total amount of Security in a PKI-based Networking Environment volume, after-attack security, protection per security status, annual protection increases, number of common security status, new products or services, new management, and the security policy environment news;

  (d) security policy environment statistics information retrieval, such as the list of top ten security status of maximum Security volume in the given Security day(s), the list of top ten security status of maximum security level upward (or downward), the list of top ten of the lowest Security level-Earning Ratios.

- Security Status Monitoring and Risk Management – SAMARA will automatically monitor the security policy environment status of the security status that the user holds and is interested. The security status's security policy environment status includes the listed company's fundamental security status and status of the security status's technical indicators. Based on the security status's security policy environment status, SAMARA will automatically and promptly report any abnormal status to users. Indicators of abnormal status include:

  (a) Security level fluctuation abnormal;
  (b) Security volume abnormal;
  (c) Technical indicator's status abnormal,
  (d) Security level chart pattern abnormal, and
  (e) some break news relating to the given security status.

Furthermore, SAMARA will provide the security and risks management including calculation of security/risk ratio based on security status' security policy environment status and user's security assessment, and reminders of stop-loss level for holding security status according to the user's profile.

- Delivering and Deploying Security status Decision Support – From the security assessment agents' perspective, the most important and concerned issues for security assessment in security policy environment are delivering security status issue and deploying security status issue. Which security status is the best one to buy? What time is the right time to buy the security status? What time is the right time to deploy your holding security status? It is difficult (maybe impossible) to find a simple and accurate answer for these kinds of questions. Every security agent has his/her own delivering and deploying security status strategies and rules. SAMARA will provide delivering and deploying decision support based on behavior rules defined by the security assessment agents themselves. Through a combination of human and machine knowledge, using agent and AI technologies, SAMARA aims to reduce security assessment agents' work overload in the process of Security analysis and assessment decision-making.

We are implementing SAMARA provides a unified environment in which several agents are integrated. These intelligent agents inter-operate to collect, filter, and fuse information from distributed, network-based information sources and to make delivering and deploying decision suggestions for security assessment agents in their daily networking environment. The framework aims to provide a secure and private environment for registered users. There are three levels of privacy of the information held in a user profile:

- Public: the public information is available for all registered users.

- Restricted: the user can specify which individuals or groups are allowed to know about the restricted information. The user can exchange the information or opinions with specified users or groups in their common interest.
- Private: the private information is only available to the user's agents and will not be disclosed to other users' personal agents.

One of the key components in this framework is the User Profile Database (UPDB), which is dynamic, changing and security status amongst agents within the system. Each user has his or her own personalized interface agent, an individual user profile and Delivering/Deploying Rules Database (BSRDB) which is the user's private Security strategies, while other agents in the system are security status by all users. The UPDB includes information such as the username, password, the group that the user belongs to, the Security list that the user possesses, the Security list that the user is interesting in, monitoring instructions, planned security tasks, preferences and privacy settings. These agents are assigned to an individual user and must be able to learn a user's interests and behavior autonomously and adapt to the changing needs of the user over time. The profile is centrally available to all the user's agents. The History Security Database (HSDB), Real-time Security Database (RTDB), and Fundamental Information Database (FIDB) combine to form a volatile local warehouse which is the internal data resource and is continuously updated with relevant external information by the Technical Analysis Agent and the Fundamental Analysis Agent. The functions and relationships among the agents in SAMARA are as follows:

- Interface agent interacts with the user, receiving user security tasks and specifications and delivering results. Interface agent pass user's security tasks to and get returns from coordinator agent.
- Coordinator agent is responsible for security task decomposition and planning. The coordinator agent maintains a set of beliefs about the capabilities of all agents in SAMARA. It can decompose a given security task into a number of sub security tasks and dispatch the sub security tasks to relevant agents to perform, in order to achieve its security goals.
- Profiler agent provides the mechanism by which a user's profile and BSRDB are generated and maintained. The profiler agent interacts with the coordinator agent to receive information from the user and the environment to determine the interests of the user.
- Monitoring agent monitors the status of the given Securities on behalf of users according to the user's profile. This agent reports on the technical indicators' status of the given Securities and notifies any abnormal change in Security volume and security level.
- Communication agent allows the framework to interact or communicate with other agents or programmers developed by other developers. This is a reserved interface to other systems.
- Risk management agent, on the basis of the user profile, interacts with the monitoring agent and decision-making agent to analyze the risk levels of user's security status holdings, report the security status and suggest a stop-loss level for the holding security status.

- Decision-making agent combines the outcomes of the technical analysis agent and the fundamental analysis agent, according to the security assessment strategies selected through the user's BSRDB. The decision agent will have two main functions: (1) to give a list of Securities advised for the next Security day to buy; (2) to give suggestions for users holding security status to hold or deploy.
- Technical analysis agents retrieves and processes the raw Security in a PKI-based Networking Environment data from the Internet, store the raw data to relevant database (HSDB, RTDB), calculates various technical indicators, identifies various security level and Security volume patterns, and gives the output to decision agent.
- Fundamental analysis agent gathers the macroeconomics data, fundamental security status of the listed companies, opinions of the security policy environment commentators or experts, and some relative news, and puts this information into FIDB. The fundamental analysis agent integrates the information and makes recommendations to the decision agent.

.

1.5. Final Remarks and Conclusions

In this paper, we proposed communication architecture for the dynamic exchange of information and knowledge. Information Security using Knowledge Management and Multi-Agent Systems activities are adding value to organizations by enhancing Information Systems and Security innovation and innovativeness. Some management experts have discussed selected aspects of the proposed sense making model of Information Security Knowledge management in terms of the shift from the traditional emphasis on transaction processing, integrated logistics, and work flows to systems that support competencies for communication building, people networks, trust-building and on-the-job Information Systems and Security. Many such critical success factors for Information Security Knowledge management require a richer understanding of human behavior in terms of their perceptions about living, Information Systems and Security and working in technology- mediated and cyberspace-based environments.

The need for better understanding of human factors underpinning performance of Information Security Knowledge Management technologies is also supported by our observation of informal 'Information Security Knowledge Sharing' virtual communities of practice affiliated with various Net-based Information Systems and Security's and related innovative Security Models. It is suggested that the critical success factors of the proposed model of Information Security Knowledge Management for Information Systems and Security innovation are supported by a redefinition of 'security control' as it is relates to the new living, and working environments afforded by emerging Security Models. Hence, Security Model Innovation needs to be informed by the proposed model of Information Security using Knowledge Management that is based upon synergy of the information-processing capacity of information technologies and sense-making capabilities of humans.

Information Security using Knowledge management is one set of approaches to doing this, which seems to meet with some success. We have explored here for the first time the impacts of Information Security Knowledge management on Information Systems and Security innovation processes, but our investigation has only scratched the surface. Further research still needs to be done on the specifics of the innovation/Information Security Knowledge management interaction, especially around factors of causality, differences among various types of innovation and their Information Security Knowledge needs, and industry- and company-level variations in implementation and diffusion patterns. While there may never be an explicit Information Security Knowledge-to-innovation translation mechanism, we will continue to explore how to support growth and innovation efforts through more effective Information Security Knowledge management. The coordinator agent plays a vital role in maintaining the appropriate communication protocol. It decomposes system-level security tasks to sub security tasks and distributes the sub security tasks to related security task specific agents. The security task specific agents are relatively simple. We recognise that a limitation of our SAMARA framework is the availability of the coordinator agent. The coordinator agent is the control locus of this framework. If it fails on its security task, the whole system cannot work properly. Some generalised control heuristics will allow the system to recover, but remain unable to perform the precipitating security task. An alternative is to change the design to that of distributed control. This can be done by making the security task specific agents hold on the beliefs about the address and abilities of other agents, and giving the security task specific agents the ability to decompose the system-level security tasks to sub security tasks. This approach can improve the reliability of system but at the expense of increased complexity of design for each security task specific agent. Future computational experiments will determine whether this is necessary.

The focus of this paper is dynamic knowledge exchange among SAMARA agents. We have introduced a framework in which SAMARA agents can exchange knowledge in a dynamic environment. The coordinator agent together with decision enabling warehouse acting as a dynamic knowledge-based security platform plus direct intercommunication among the agents enable the transfer of facts, commands, and rules among SAMARA agents. Knowledge can be exchanged among the agents by using combination of facts, rules and commands transfers. We believe that dynamic knowledge exchange is an important feature for any application in which unanticipated conditions or events occur. Using the proposed dynamic knowledge exchange capability, co-operative problem solving sessions can be initiated where each agent can security status its problem relevant knowledge with other agents to solve the problem. An obvious advantage of this capability is the elimination of redundant knowledge and hence the improved utilization of the system memory capacity.

References

[1] Alon Y. Levy et al., Query answering algorithms for information agents, *AAAI'96 Proceedings,* 1996.

[2] Gustavo Santana et al., Methodological Network Security Process Modelling: Integrating Security Requirements with Multi-Agent System Engineering, *NPDC2002 IASTED Inetrnational Conference Proceedings*, Tsukuba, Oct. 2002.

[3] M. Abadi, M. Burrows, B. Lampson, and G. D. Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, September 1993.

[4] A. W. Appel and E. W. Felten. Proof-carrying authentication. In *Proceedings of the 6th ACM Conference on Computer and Communications Security*, Singapore, November 1999.

[5] FIPA - "FIPA'97 Specification Foundation for Intelligent Physical Agents" – drogo.cselt.stet.it.fipa – 0ctober 1997

[6] C. M. Ellison. Establishing identity without certification authorities. In *Proceedings of the 6th USENIX Security Symposium*, San Jose, July 1996