IMPLEMENTING KNOWLEDGE MANAGEMENT TECHNIQUES FOR SECURITY PURPOSES

Petros Belsis, Stefanos Gritzalis
Department of Information and Comnmunication Systems Engineering, University of the Aegean, Karlovasi, Samos, Greece

Christos Skourlas
Department of Informatics, Techological Education Institute,Athens, Greece

Ioannis Drakopoulos
Ilyda S.A. Kifissias 180 Ave., Athens, Greece

Keywords: Security, Knowledge Management, Multimedia.

Abstract: Due to its rapid growth, Information Systems Security becomes a new era of expertise, related to a vast quantity of knowledge. Exploiting all this knowledge becomes a difficult task, due to its heterogeneity. Knowledge Management (KM) on the other hand, becomes an expanding and promising discipline that has drawn considerable attention. In this paper we deploy our arguments about the benefits of KM techniques and their possible applications to assist security officers in improving their productivity and effectiveness. To prove this, we exploit possible technological prospects, and we present the architecture of a prototype developed to implement selected innovating KM components, embedding state-of-the-art multimedia java-based applications.

1 INTRODUCTION

Security becomes a major headache for many different categories of people. Security experts, managers, often face the side effects of Information Systems Security violations. New techniques and advanced technology features are emerging on a daily basis, making security management a difficult and knowledge dependent task. As a consequence, a vast amount of knowledge is necessary in order to achieve security management.

Therefore, there is an obvious necessity for exploiting this knowledge with the assistance of technology means. Several attempts in the relevant literature, try to focus on the effective management of security related documents (Fung et al., 2001).

Others try to facilitate security officers difficult task by making use of automated tools (Vermeulen et al., 2002). Lately, there is also a considerable research interest in extracting useful patterns through the application of data-mining in security-related sets of data (Ertoz et al., 2003) (Yurcik et al., 2003). Security experts themselves, on the other hand, try to support each other through communities of practice, which facilitate knowledge exchange through indirect means –such as posting information on specialized internet sites – or direct, such as contacting each other through mailing lists. Typical examples are the CERT and SAGE (community of systems administrators) organizations. Our approach focuses on applying KM techniques to Information Systems security related knowledge, and by doing so, improve the effectiveness of security officer's competency. We do not restrict our approach to conventional technological approaches, but beyond that we embed state of the art such as Voice over IP (VoIP) transmission, through java based multimedia applications.

Belsis P., Gritzalis S., Skourlas C. and Drakopoulos I. (2004).
IMPLEMENTING KNOWLEDGE MANAGEMENT TECHNIQUES FOR SECURITY PURPOSES.
In *Proceedings of the Sixth International Conference on Enterprise Information Systems*, pages 535-540
DOI: 10.5220/0002655605350540

The rest of the paper is organized as follows: In Section 2 we present our arguments about the benefits of establishing KM techniques, and how top international companies gained competitive advantage due to their KM platforms. In section 3 we present the main technological challenges in KM implementations and we present how new technologies can be helpful, describing our contribution in relation to contemporary KM approaches. Section 4 concludes the paper describing how under certain circumstances our approach can assist security experts in increasing their productivity and effectiveness, and also resuming where we attempt to innovate, describing also our scheduled further steps towards adding more functionality to the system.

2 MOTIVATION FOR KM IN IS SECURITY

Information Systems security is a rapidly changing knowledge intensive business, involving many people with different kinds of expertise. Organizations base their security on people, which are not a steady asset for an organization. Security related knowledge is diverse and its proportions immense and steadily growing. Organizations face the challenge to identify the content, location and exploit knowledge. An improved use of this knowledge is the basic motivation for KM and deserves deeper analysis.

2.1 Knowledge Management fundamental concepts

The three levels of refinement of knowledge items are data, information and knowledge. By knowledge, - a term fraught with history and definitional peril – firms generally mean codified information with a high proportion of human value-added, including insight, interpretation, context, experience, wisdom, and so forth (Davenport et al., 2001). Although often the terms information and data can be used interchangeably, we could define information to be ‘‘interpreted data’’ and knowledge to be ‘‘information to be transformed into capability for effective action’’ (Vouros, 2003).

2.2 Knowledge types

Philosopher Polanyi (Polanyi, 1966) distinguishes knowledge in two types: tacit, which is embedded in the human brain and cannot be expressed easily, and explicit knowledge, which can be easily codified (Davenport et al., 2001). Most KM systems implementations focus on managing explicit knowledge. The real challenge is to exploit tacit challenge. For example, a security professional’s expertise is an intangible asset which can be under certain circumstances used, without his physical presence, as we try to demonstrate at a later section, by embedding multimedia technologies in our prototype.

2.3 Benefits of KM

Knowledge management is an emerging discipline that promises to capitalize on organizations’ intellectual capital (Rus et al., 2002). As a concept, KM appeared the late decade. Today, it has been transformed to a core business function, among top-level companies. According to a major study undertaken at 1996 (Chase, 1997), by Ernst & Young Business and Intelligence among the key benefits of establishing KM, the following can be distinguished:

- Improved decision making
- Improved efficiency of people and operations
- Improvement of innovation
- Improved products/services.

Among KM benefits we could also distinguish enhanced collaboration and communication, new knowledge creation, knowledge retention and increased knowledge availability and access (Rus et al, 2002).

2.4 Well-known case studies

Several major companies have gained from implementing KM functions. Among the most popular case studies, we can distinguish Ernst & Young, Microsoft, Siemens (McCampbell et al, 1999) (Davenport et al, 2001).

2.4.1 Ernst &Young

Ernst & Young is one of the “big six” professional services firms, which traditionally offered audit, tax and management consulting. Due to the geographical dispersion of E&Y, technology had to be used as an enhancement to its knowledge base accessibility. In the beginning, Lotus Notes was used as the main platform, whereas by the growth of the key documents and databases a shift to a web-based intranet was performed.

2.4.2 Microsoft

Microsoft maintains advantage over its competition for more than 20 years because of the knowledge and capabilities of its employees (McCampbell et al, 1999). Microsoft's IT group has invested in time and human resources in order to maintain and identify knowledge competencies.

Implementation of these knowledge management strategies proceeded on an international level involving a large number of employees and utilizing a cross-section of all job-types (Davenport, 1998).

2.4.3 Siemens

By making the move to knowledge management Siemens faced an extraordinary transformation (Davenport et al., 2001). Aspects of knowledge management that involve technology-enabled repositories and sharing networks help to overcome geography barriers. Also by sharing knowledge across business units, one unit can take advantage of the learning and expertise of another. Second, the firm depends on technology, which changes radically in short periods. In order for a high-tech company to remain competitive, keeping knowledge up to date is essential, as well as enabling knowledge sharing by new technology means exploitation.

3 IMPLEMENTING KM FOR SECURITY PURPOSES

Our approach emphasizes on making a step forward, proposing to the security experts community a new framework to assist security specialists in their everyday tasks, and to help them overcome obstacles, by sharing knowledge between them with the assistance of technology means. Implementing KM involves many challenges and obstacles. Several issues are particularly important:

- Technology. Several tools and technological platforms exist, but it becomes difficult to integrate all of them in order to achieve the desired result.
- Organizational structure. Exploiting technological solutions is not a panacea. Creating a knowledge culture and focusing on methodology in order to establish functioning KM procedures are equally important factors.
- Motivation. Employees must have a motive to contribute their knowledge and codify it in repositories in order to establish an effective knowledge base. Lack of motivation or commitment is supposed to be one of the main causes of failure for KM systems (Chase, 1997).

The most practical way to define KM is to emphasize that it largely involves new applications based on the existing IT infrastructure (King et al., 2002). Such applications include:

- *Knowledge repositories*. Databases allowing storage and retrieval of explicit knowledge research containing both technical and management related knowledge, in text format.
- *Best practices and lessons-learned systems*. Knowledge repositories used for explication, storage and retrieval of business best practices and for making the lessons learned in projects available to others.
- *Expert networks*. Networks of individuals identified as experts in some specific professional area who are electronically accessible by others with questions related to that expertise.
- *Communities of practice*. Networks of self-organizing groups whose members share common professional interests and who may live or work in dispersed geographical settings.

3.1 Making the system work

Among the basic functions of a KM prototype as it has been already mentioned, is the codification of explicit knowledge. In order to reduce querying time-costs a retrieval mechanism is necessary. For the purposes of our research, we created a prototype which emphasizes both in exploiting explicit knowledge as well as in exploiting tacit knowledge- which as stated at an earlier paragraph – is the challenge for a KM attempt. Our prototype has been implemented in two platforms: Java and Visual C++. An architecture overview is presented at Fig. 1.

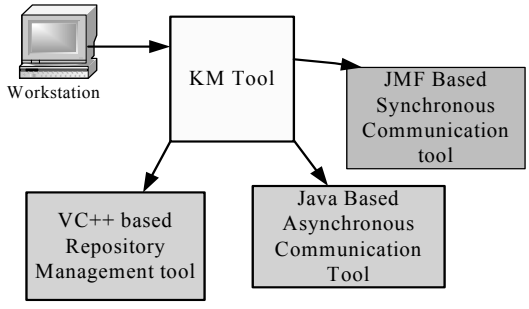

Figure 1: Architecture overview of the developed prototype

A part of the prototype is implemented in Visual C++, specifically the part that deals with codifying and retrieving explicit knowledge. Handling explicit knowledge is one of the main functions, such an application should support. Knowledge is codified in semi-structured text documents (a relational database is not suitable in our case); therefore implementing a search engine to allow information retrieval was a necessary priority, a task that was carried out in C++. Each document is structured in the following way: In the beginning several keywords are provided, followed by a more analytical description in raw text. Though, we obtain the possibility of describing in the beginning the most important topics, which are analyzed further in the text. By providing certain keywords and by specifying the possible location (directory) of the semi-structured text, the search engine searches the entire document looking for the provided by the user keywords and classifies the documents according to the occurrences of the founded in the text keywords. The search is not only limited to the first lines of the document which exist as a means of facilitating the user to decide between similar documents according to the relevancy of all the related words, but we also search through the whole document.

3.2 Utilizing tacit knowledge

The second two components are implemented in Java, and they aim to assist in exploiting tacit knowledge, in detail they attempt to help capitalize the intangible knowledge assets of an organization's employees, like human experience for example. Most of the implemented KM platforms depend very much on inter-organizational communication. Email platforms prove to be promising applications towards this direction. Not only they are a cheap way of communication, but also they do not expect someone to be always on-line. With a logical delay, experts can give a brief suggestion to another employee, often very valuable, since never codified knowledge could replace human expertise. For these purposes, we have embedded an email application, JMailer, written entirely in Java. This application,

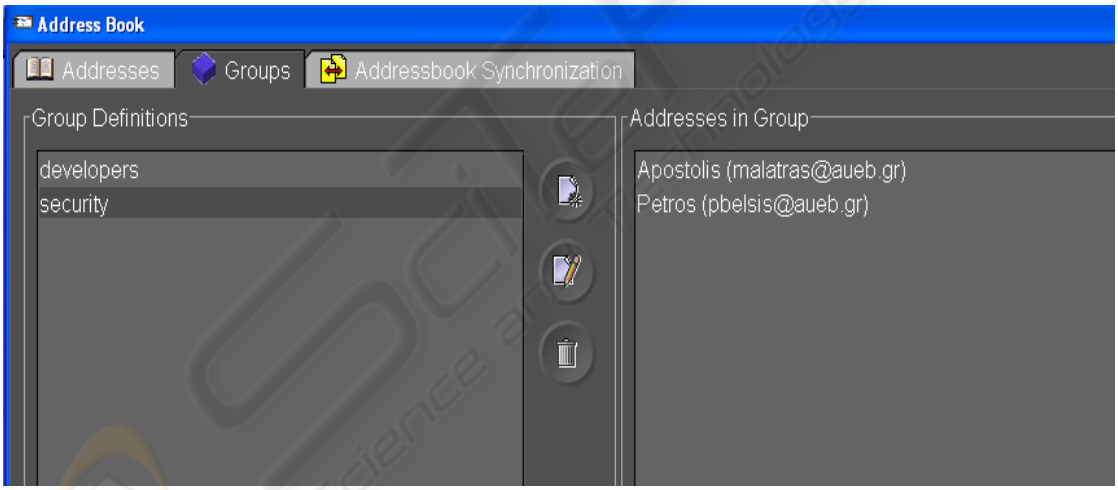

Figure 2: Sending targeted mails to expert's mailing lists

gives the possibility to create mailing lists based on different kinds of expertise, and therefore depending on the category of advise someone seeks, s/he can send targeted mails to all members of a group. Therefore, somebody is quite possible to have faced a similar problem in the past, and offer some advice, overcoming by this way, geographical or time barriers. Fig. 2 presents the possibility to create groups and therefore send targeted mails according to the group's classification.

3.3 Embedding multimedia functionalities in KM applications

Most of the existing KM platforms base their communications on asynchronous applications, or leave that matter to the employees, who can communicate further through traditional means of communications, for example telephone. Our effort to support security experts through KM practices, attempts to utilize multimedia capabilities. This possibility aims to provide employees who can

under certain circumstances provide further assistance -than simply send a mail to other colleagues- with the ability to communicate on-line and provide detailed assistance. For this purpose, the third component is a multimedia application based on the Java Media Framework (JMF).

JMF provides a development framework in order to enable sound or video stream through a data-network channel. It provides a set of classes and methods in Java, for coding, handling and achieving synchronization which is a fundamental prerequisite for Quality of service purposes, so as the provided service to be at an acceptable quality level (JMF).

Our application consists of a server, which controls the messages and monitors

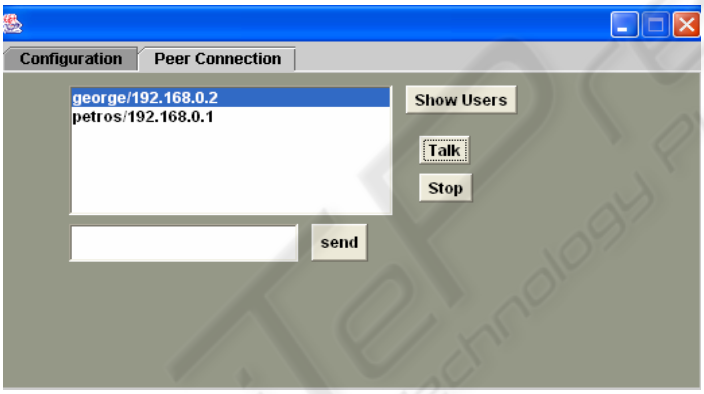

Figure 3 The JMF based communication software component in action

communication, enabling clients to participate. On each user's workstation it is necessary to have the JMF platform and Java2 Platform installed (JDK), and run the client software. Then, by providing the server's address and choosing an available audio capture device, the server recognizes the client and handles the necessary messages, creating an RTP session for each client (Fig. 3).

Recapitulating, knowledge codification has been implemented through semi-structured documents creation, while information retrieval is being facilitated with by means of a search engine facility. Knowledge capture and personalization are supported in two ways:

- Through an asynchronous Java-based communication tool, which assists communities of experts to communicate and provide guidance to each other, and
- Through a multimedia application, able to provide on-line help in cases where it is necessary and human resources are available and able to help.

4 CONCLUSIONS

We have examined so far the presence of an existing gap in utilizing security related knowledge. Experts usually even within the boundaries of an organization, face the same problems independently, or they treat more than once with a specific kind of problem, which has been already solved in the past, wasting time and effort. By exploiting both documented (explicit) knowledge, as well as tacit knowledge, security experts can increase their productivity and their effectiveness. To test the above in action, several software modules have been integrated in a prototype, which attempt to support the following processes:

Knowledge Codification/Retrieval. Through the repository administration tool, explicit knowledge can be shared between security experts. Moreover, whenever important details come out while dealing with a specific problem, experts can retain this knowledge by creating semi-structured documents, which can be retrieved later by the search engine provided for administering the repository.

Knowledge sharing. Knowledge sharing is supported in two ways: a) Explicit knowledge can be shared through the repository utility. b) Tacit knowledge can be shared by the asynchronous communication tool, which enables users to communicate with each other by sending targeted mails to specific mailing lists, and getting responses from geographically dispersed locations,

overcoming time or instant availability limitations, or by making use of the synchronous communication tool, which facilitates voice transmission over IP networks, providing a more flexible and effective way for communication between experts. So, our effort focuses in two directions: a) to provide an effective way of increasing productivity and effectiveness of security experts by exploiting KM techniques, and b) integrating in our prototype state-of-the art technologies, such as Voice over IP through multimedia applications written in Java based platforms.

Among our priorities, is to enhance our prototype with further multimedia capabilities, such as video stream transmission from distributed video servers, and to enhance the repository administration utility tool with context and user-specific facilitation capabilities, through agent and ontology technologies. Also an independent module of the overall system is currently under design, dealing with data mining on security related data sets, such as network traffic logs. By doing so not only we offer a compelling solution towards the improvement of security expert's competency, but also we integrate multimedia capabilities in KM systems, an innovating aspect relatively to most similar applications, as it proves from examining the recent relevant literature.

REFERENCES

Chase R. L 1997. "The knowledge-based Organization: An International Survey", The Journal of Knowledge Management, vol. 1, No 1, 1997.

Davenport T., S. Volpel 2001 "The rise of knowledge towards attention management", Journal of knowledge management, vol. 5, No 3, pp 212-221.

Davenport, T 1998. "Knowledge management case studies", Graduate School of Business, University of Texas at Austin, www.bus.texas.edu/kman.html.

Ertoz L., Eilertson E., Lazarevic A., Tan P., Dokas P., Kumar V., Srivastava J., 2003. "Detection of Novel Network attacks using data mining", ICDM 03, Workshop on Data mining for computer security, Nov. 2003 Melbourne.

Fung P., Kwok L., Longley D 2001. "Electronic Information Security Documentation", Conference on Information Security management and small systems security, Nevada, USA.

JMF, 2001. Java Media Framework Guide, available at www.sun.com

King W., Marks P., McCoy S, 2002. "The most important issues in Knowledge Management", Communications of the ACM, Sept. 2002, vol.45, No. 9.

McCampbell A., Mordhead Clare L., Howard Gittters S, 1999. "Knowledge management: the new challenge for the 21st century", Journal of Knowledge Management, vol. 3, No 3, pp 172-179.

Polanyi M., 1966. "The Tacit Dimension", Routledge & Kegan Paul, London.

Rus I., Lindvall M,2002. "Knowledge Management in Software Engineering, IEEE Software, vol. 3, pp.26-38.

Vermeulen C., Solms Von R, 2002. "The information security management toolbox – taking the pain out of security management", Information Management & Computer Security, 10/3, pp. 119-125.

Vouros G, 2003. "Technological Issues towards Knowledge-Powered Organizations", Knowledge Management Journal, Vol 7, No. 1.

Yurcik W., Lakkaraju K., Barlow J., Rosendale J., 2003. "A prototype tool for visual Data Mining of Network Traffic for intrusion detection", ICDM 03, Workshop on Data mining for computer security, Nov. 2003 Melbourne.