BUILDING AN ENTERPRISE IT SECURITY MANAGEMENT SYSTEM

Meletis A. Belsis, Leonid Smalov
Data Knowledge Engineering Research Group, Coventry University, Coventry, U.K.
Tel. +44 24 76 631313, Fax: +44 24 76 888052
E-mail: {Belsis,l.smalov}@coventry.ac.uk

Abstract: Moving towards a knowledge economy, managing effectively and safely the corporate data is the key to an organisation's survival and success. Corporative employees that technologies like computers, mobile and portable devices to access the information. Safeguarding corporate information that flows in unprotected land lines and airwaves is critically important. Adversaries attack information systems, their tools and techniques are numerous and widely available. Analysis of various security incidents has shown that the corporative attempt to achieve and maintain "absolute" security is not always effective and usually is far too expensive. To provide adequate protection for the modern enterprise, security architectures need to be build. These include security mechanisms, tools and policies that provide an acceptable level of protection for the enterprise. This paper presents the work in progress in developing an enterprise information security data model. The proposed prototype aims at presenting security specialists with more effective ways of managing existing security architectures implemented by the enterprise.

Keywords: Security Model, Enterprise Security Architecture, Security Management.

1. Introduction

Information is currently one of the greatest asset corporations have. Information about internal performance and the outside world allows an enterprise to take strategic decisions and expand into different markets. Accurate information allows a company to expand and increase its income, but misinformed enterprises could lose their share of the market [1].

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35691-4_52
D. Gritzalis et al. (eds.), *Security and Privacy in the Age of Uncertainty*

Examples of valuable information to an organisation include: customer details; prototype designs; announcements of new regulations, instabilities in world events; etc [2].

To achieve a better acquisition and processing of information, enterprises spend large budgets in developing Information Technology architectures. These architectures use computer and communication technology for the acquisition, storage and local distribution of information. Some companies go even further, developing decision support systems based on technologies such as Data Warehouses and Data Mining [3]. These systems allow companies to obtain decisions based on special types of information and on performing *'what-if'* analysis. The importance of dealing effectively with information can be established by the existence of organisations whose main product is information management systems.

As corporations decide to connect their IT systems to the Internet to take advantage of the new market, the flow of electronic information has consequently expanded the need for Information Enterprises.

Enterprises are complicated systems and so include complicated IS/IT infrastructures. These infrastructures come from different environments and cover different requirements, which may change daily. Their IS/IT infrastructures must be able to adapt to these changes. To produce secure enterprises it is necessary to ensure that their security infrastructure will be able to follow the enterprise's future changes. The application of security in business environments is discussed in [4-5]. In addition to that security must be applied to fulfil the CIA (*C*onfidentiality, *I*ntegrity and *A*vailability) requirements without neglecting other requirements like system usability, efficiency and flexibility.

To develop such systems security cannot be functionality that is added as an afterthought. It must be an integral part of the overall system. Securing such complicated IS/IT infrastructures can be an extremely difficult task. Mechanisms such as encryption, integrity and access control can be bought off the shelf and installed by anyone on a computer system(s). But these programs are only one part of the solution. In order to provide secure business environments security architectures need to be constructed. These include technologies, processes and policies that need to collaborate in order to provide total protection.

To develop such architectures the security manager and/or analyst will have to review the enterprise's structure. The business processes and goals have to be analysed to produce the security requirements and security policy statements. In addition to this, the company's geographical locations, departments and employees need to be analysed in order to produce the requirements for information classification and employees' access privileges. As with any system investigation, all the previous have to take place alongside with support from the management and system users.

2. Enterprise Security Management

To manage such a dynamic architectures security managers need to be informed about the precise location of the security measures that are installed; who has access on what enterprise data, and, why. This information must be provided in a clear and precise form, of the whole enterprise plan.

Providing such an informational base, especially for large enterprises, is complex. Security technologies, tools, methods and processes have to be analysed in quite a fine detail. Based on this the security experts will be able to provide better advice to the management for security issues, on possible new technologies, and consequently affect the business decision stages.

In more detail some of the positive points of using such a database can be summarised below [6]:

- They promote more consistent and efficient collection of data from any number of diverse sources.
- They inherently force users to follow work processes that have been adopted by the company's best practices.
- They provide much needed information (often data compilations from diverse sources) to decision makers in appropriate formats and in a timely manner.
- They generate performance measures (metrics) for judging the success/health of activities and for making relative comparisons between various activities.

Products that provide such ability are called *Enterprise Security Management* (ESM) software and examples of such include: The *Enterprise Security Manager* by Axent Technologies, the *bv-Control and bv-Admin* by BindView Development Corporation, the *eTrust* by Computer Associates and the *Enterprise Security Architecture System*, by PRICEWATERHOUSECOOPERS ltd. These products utilise an enterprise security data model that is able to hold a detailed description of the enterprise's security architecture and a piece of code that is able to mirror the changes of the security architecture to the data model. ESM utilise the TCP/IP protocol to offer central management of the security products installed in the enterprise.

Unfortunately existing ESM products, with exception the Enterprise Security Architecture System, are concentrate on modelling parts of security architecture (i.e. security policy, authentication mechanisms) and do not represent or manage the totality of the security mechanisms implemented in an enterprise. An example of security information that is usually neglected is the enterprise security incident history, which is a vital part of the informational framework security experts need to have

A second problem found in the current ESM products is that due to the way their data models are designed it is very difficult to attach them to the enterprise's modelling framework. This can have the result that the security model is used decreasingly and is finally outdated.

3. Enterprise IT security data model

The model proposed in this research can be used by security managers to check and review their corporate security policies. Security experts will be able to understand the structure not only of the security mechanisms but also of the rest of the services that run on the systems (i.e. to answer who can access what data and which web servers run on which host). Users will be able to understand the corporate security policy and become aware of the things they can or cannot do as well as the penalty for bypassing specific policies.

The new model records information coming from the application of international security initiatives like *CCTA Risk Analysis and Management,* and *ISO 17799.* In order to be common across different sizes of enterprise the model can not follow, at the detailed level, specific security standards and guidelines. This is what makes the model dynamic and allows enterprises that follow different initiatives to use the same top level model.
In addition to the previous the new model provides solutions to the problems described earlier by incorporating the security history of an enterprise and by clearly describing the links of it with the rest of the enterprise models.

The context model of the proposed structure has four entities. Each one of those entities will be decomposed to form the next level of the proposed structure. The four main entities (figure 1) are the *Enterprise Organisational Infrastructure,* the *Enterprise Information and IT Infrastructure,* the *Enterprise Security Infrastructure,* and the *Enterprise Security Management Infrastructure.*

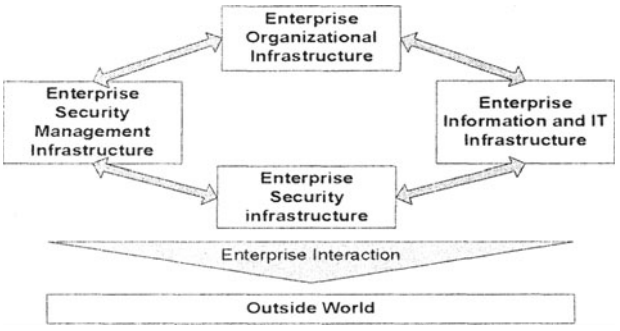

Figure 1 Context Model

The four main entities discussed previously are decomposed further to produce the context model of the proposed data model (figure 2):

Enterprise Organisational Infrastructure:

- *Enterprise Departmental Structure*: The ways the different departments are interconnected and operate are vital to security analysts. This information can be used to identify critical points in the enterprise.
- *Enterprise Employee Infrastructure*: This entity is assigned the job of describing the way the enterprise's employees are organised. Using this entity the security manager can classify employees depending on the security clearance they have.

Enterprise Information and IT Infrastructure:

- *Enterprise Information Infrastructure*: This entity describes the information vital to the enterprise. It classifies the information, describing the level of security that each element needs.
- *Enterprise IT infrastructure*: The number of network hosts, their type and the domain to which they belong are described here. In addition to that the entity describes the hardware specifications, the vendor and the services (i.e. open ports) run by each one of the hosts. The network devices that an enterprise network includes can be categorised using high level terminology in to the following: *Public enterprise server; private enterprise server; internal host; Internal Router; External Router*, and, *Miscellaneous*

Enterprise Security Infrastructure:

- *Enterprise physical security:* Information on the way the enterprise's buildings and offices are protected is stored by this entity. The IT offices and buildings physical protection is vital information for the security manager.
- *Enterprise IT Security*: The software and hardware procedures that protect the IT infrastructure are listed here. Examples of such include encryption and authentication mechanisms, intrusion detection systems and firewalls. The IT security mechanisms are organised according to their functionality into the following: *Firewalls; Secure Communications; Secure Storage; Antivirus; Software patches/ updates; User and Software Management; Security Policy; Load Balancing; Antisniffing; IDS,* and *System Penetration testing.*

Enterprise Security Management Infrastructure:

- *Enterprise Risks*: This entity describes the outcome of the risks analysis process. The risks and threats are stored here. This entity will allow for a number of different risk analysis processes to be used.

- *Enterprise Security History:* It is vital to keep a record on the security history of an enterprise. This record includes the details of security incidents that took place in the past and details of the changes that took place in the overall *Enterprise Security Infrastructure.*
- *Enterprise Security Policy:* This entity is used to capture the information associated with the enterprise's security policy. Every security mechanism and employee must follow the enterprise's security policy. The security policy describes the security mechanisms that are in place to enforce the policy and the penalties that will be applied for those not following the policy.

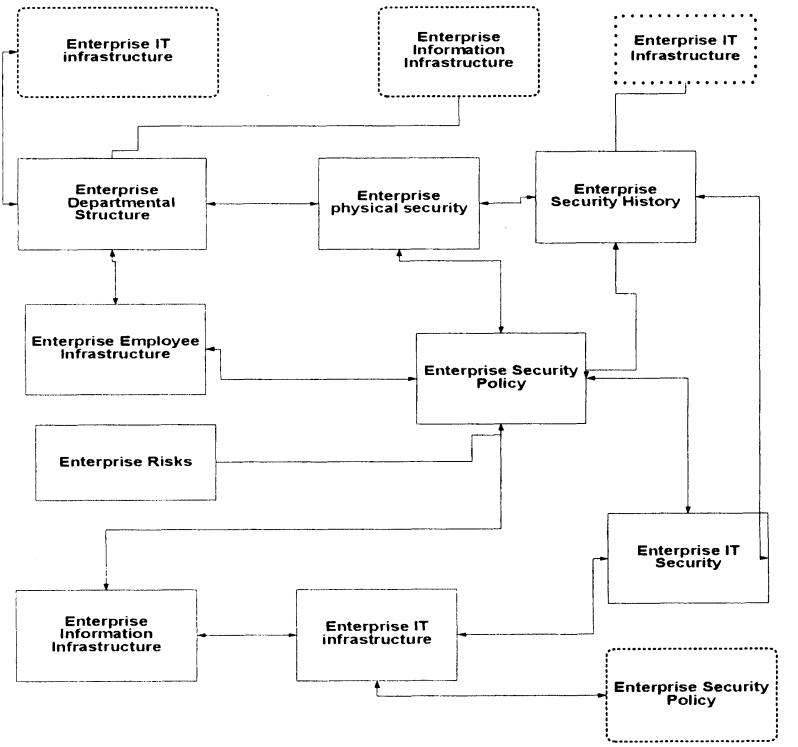

Figure 2 Context Model

During the decomposition of the proposed model the *Zachman framework* [7] is used to provide the next lower level model. In that way each entity will be analysed against most of the aspects that the Zachman framework includes. Describing such a decomposition process in one paper is impossible. Follows is one example of such decomposition for one of the entities the model includes:

Enterprise Departmental Structure: This entity provides a composite to encapsulate the organisational structure of the enterprise. The Data simply provides the lists of departments, the Function lists the tasks that each

department performs, the Network shows the interfaces between departments and for departments to the outside world, the People simply shows the posts and roles in the department and their general responsibilities (not the actual people in the roles), the Time shows the possible sequence constraints for task and data elements, the Motivation provides a statement of purpose for the tasks, interfaces, roles and data. The refinement of these elements relates to the Owner, Architect, Designer, and Builder Views

4. Enterprise Security Incident History.

Keeping records of the past security incidents is vital for every enterprise [8]. These records can assist security specialist to avoid incidents from happening again, to educate users, and assist management in assigning the appropriate funds for information security. Currently much research has been done in delivering data models able to store information coming from past security incidents [9-11]. Unfortunately these models store only the technical information associated with an incident neglecting any managerial information that could be of help to the management. These models have been developed to assist Computer Security Incident Response Teams (CSIRTs) and so do no include any clear links with the enterprise's models.
Decomposing further the proposed enterprise IT security data model, an incident model was created. This model is able to store information coming from the security incident that took place on the enterprise's information systems and correlate this information with the rest of the enterprise IT security data model. The model was first published in [12]. An illustration of this model showing some of the links of it to the rest of the enterprise security data model is given in figure 3.

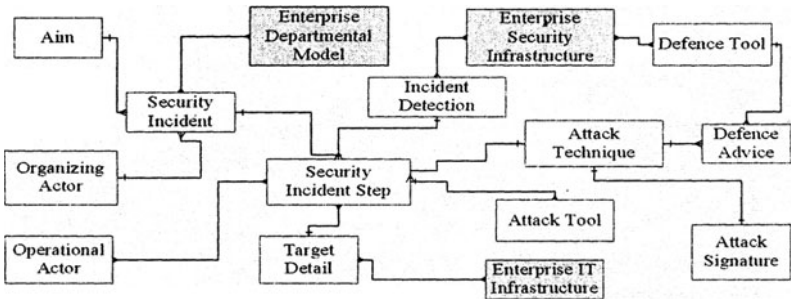

Figure 3 Enterprise Incident History Model

5. Implementing the proposed structure

Two issues regarding deployment of a security related database are the security of the data stored and the way this data will be accessed by the system's users.

Due to the nature of its data, such a database could be an invaluable tool for all kinds of hackers and/or criminals. Adversaries might be able to identify precisely the hardware and software that an enterprise uses. The database might be used as a hacking tutorial to advice adversaries on how to bypass specific systems. The problem becomes more apparent if the database is going to be accessed via the Web. In order to ensure the authorised use of the database, there must be security procedures in place to protect the stored data. The system that maintains the data model must be able to safeguard it against the *CIA* requirements.

The second problem concentrates on the way security related information are going to be accessed and is more difficult to handle. Current systems are localised for security specialists forgetting that managers are the ones that assign the budget for information security. Corporate managers need to identify the managerial information related to an incident. Examples of such are: an average cost to the enterprise; the time the company needed to recover from the incident, and, statistical data. The statistics will relate to the frequency of the attack and/or the type of companies this incident targets. This information will assist managers in identifying potential weak points and allow them to calculate a budget and/or extended the organisation *high level* security policy. For the security manager it would not be helpful to display a huge amount of technical information on the screen when data incidents are retrieved. The need for security, limits the utility of the current systems. At the same time security technicians are not interested in the architectural details of the security mechanisms. They are interested at the configuration information of the specific security tools they are assigned to. Enterprise employees would need an easy way to access their private security related information (i.e. passwords and encryption keys) as well as to identify specific parts of the corporate security policy. To enhance awareness users should be presented with an easy way of accessing some of the information coming from the past security incidents.

The above requirements raise issues in relation to the operation of such data structures. In addition to having a data model that provides sufficient scope, the way the content is accessed must be user friendly. Each user of the database must be able to see details that are closely related to the line of his work. The system supporting the model must allow for *smart queries* to be executed. Examples of smart queries that would be useful to a security expert include:

- Which incident targeted corporate confidential information?

Examples of smart queries that would be useful to a manager include:

- How many incidents cost more than $100?

Currently a number of research publications have proposed the use of the Common Object Request Broker Architecture (CORBA) to access Internet based databases [13-15]. CORBA with its security service can provide adequate security to fulfil the CIA requirements of the data stored in the incident database [16]. The system discussed here uses the CORBA model to allow registered users to fully access an incident database. The new system allows access through the TCP/IP protocol. In addition to this the new system automates the process of recording an incident by providing the ability to implement the client of the system as part of the overall company's security management console.

Every user of the system is assigned an X.509 digital certificate. This certificate can be the one that the enterprise had assigned when employed by the corporation.

Users will access the system by using the corporate intranet and authenticating with their digital certificate. They will then download a java applet. After setting up the applet, it will open a connection to the database server. From there the user will be able to update his security records and/or perform queries to the database (Figure 4). To allow more security the digital certificate will contain the privileges that this user has over the database.

To provide friendly access a Natural Language Interface DB (NLIDB) system [17-18] is used. Such systems provide the ability to use regular English expressions to search the database instead of SQL queries. The system is responsible for translating the English expression into an appropriate SQL statement and for formatting the search output into an acceptable form. Initial designs for the MS SQL Server and MS English Query have been constructed and the examples have been shown to be relevant to the proposed architecture. Using an NLIDB server provides a much more friendly way to search security related records than the traditional keywords search. It will allow non technical users to access and search the database easily. Along with that it allows the construction of smart questions that can be answered by the database.

The NLIDB server can create different views depending on the type of the user (i.e. manager or technical personnel). Using specific views, we avoid filling a manager's screen with lots of technical information or an administrator's screen with managerial information. This makes the output of a database search much more structured and readable. This also adds a

second layer of security to the system due to the fact that the server can be programmed to hide the search results from 'confidential' fields.

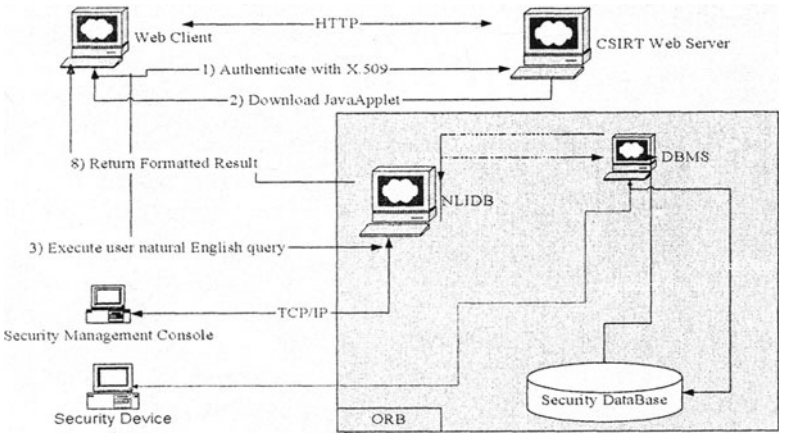

Figure 4 Proposed System

Security experts can use their existing security managing consoles or the intranet to access security related records. Due to the open architecture that the CORBA model provides security vendors are able to incorporate functions that will allow their product to access the database. This will enable security managers to maintain distributed records of their systems security history. This provides security systems with the ability of automatically registering a security incident when it occurs (i.e. intrusion detection sensors can record an anomaly as soon as the detect one). In addition to that security experts could update the intrusion detection sensors and firewalls of the enterprise to detect and stop the new anomaly. To be able to provide this functionality there are a number of problems that need to be solved first. Examples of such are: deciding on a common incident structure, and, ensuring that the detected incidents are not false.

The client software, either Java applets or embedded in security products, will be able to use CORBA's *DII* to identify and locate new services. CORBA will allow incident management teams to add new functionality on demand.

6. Conclusion

In this paper a novel contextual model of the enterprise security has been discussed. The CORBA based architecture for practical evaluation of the

model has been developed. From the overall model the security incident decomposition was provided. To retrieve or exchange the security incident related information the developed architecture incorporates a natural language interface to the data stored. By using such integrated approach the authors have attempted to make process of handling security related information in more efficient and secure way. We relay on the following important facts:

- Firstly, that CORBA standards are Web Consortium (W3C) controlled and no single software vendor (in comparison Java-RMI is proprietary Sun's technology and COM/DCOM is one of Microsoft technologies) or a governmental body are responsible for developing CORBA protocols. That could make the proposed architectural approach very reliable and secure – as specific as needs of a particular enterprise;
- Secondly, there major web sites or even vendor's portals dedicated to the describing security related information, incidents and vulnerabilities as well as supplying security updates and recommendations. We found that all of them are not easy to use, required continuous attention of security administrators, managers or simply too generic for the needs of a particular enterprise. The embedded natural language interface could significantly simplify and streamline the process of retrieving the related information.

Finally as all work in progress there is a certain element of future development involved. In particular, the idea to use Web services, based on XML-SOAP approach appears as very attractive one. The powerful feature to supply and maintain application-to-application communication may be used to develop a Web service containing the details on security architectural descriptions, security incidents, security updates, costs, risks, vulnerabilities etc working together with a group of intelligent autonomous agents to retrieve and supply the related information. The web client may present the information to the end-user and could be tailored to the specific corporative needs. We consider this as next step in our research and looking for possible collaboration.

7. References

1. Donald L. Pipkin, 200, *Information Security: Protecting the Global Enterprise.* Hewlett-Packard Professional Books.
2. Kostantin Beznosov, *Information Enterprise Architectures: Problems and Perspectives.* Florida International University technical report 2000-06.2000
3. Rimvydas Skytius, *Business Decision Making, Managerial Learning and Information Technology.* Proc. Of the Informing Science: Challenges to Informing clients: A Transdisciplinary approach Conference. 2001
4. Ethan Sanderson and Karen A. Forcht, 1996, Information Security in Business Environments. Information Management and Computer Security, 4/1, pp. 32-37.
5. D. Spinellis, S. kokolakis and S. Gritzalis,1999, *Security requirements, risks and recommendations for small enterprise and home-office environments,* Information Management and Computer Security, 7/3, pp.121-128.

6. Tonda R. Henning, 1996, *Use of the Zachman Architecture for Security Engineering*, 19th National Information systems Security Conference. Baltimore
7. Zachman, J. A., *A framework for Information Systems architecture*. IBM Systems Journal, vol.26, No.3, pp.276-292. 1987
8. Anderson R. *Why Cryptosystems fail*. Technical Report. University Laboratory, Cambridge University. January 1994
9. IDWG. *Intrusion Detection Exchange Format Data Model (IDEFDM)*. 15 June 2000
10. Commission of the European Communities Security Investigations Projects. Project S2003-Incident Reporting a European Structure "Final Feasibility and Strategy Report". Report No19733.Version 1.0. 1992
11. Demchenko Y. *Incident Object Description and Exchange Format Data Model and Extensible Markup Language (XML)*. Internet Draft. July 2001
12. Belsis A. Meletis, Godwin Nick and Smalov Leon, *A Security Incident Data Model*, Proceedings of the 17th International Conference on Information Security (IFIP/Sec 2002), Cairo, Egypt, May 2002
13. Athman Bouguettaya, Boualem Benatallah, Mourad Ouzzani and Lily Hendra. Using Java and CORBA for Implementing Internet Databases. Proceedings of the 15th International Conference on Data Engineering, 1999, pp.218-227.
14. Athman Bouguettaya, Boualem Benatallah, Lily Hendra, James Beard and Kevin Smith and Mourad Ouzzani. World Wide Database- Integrating the Web, CORBA and Databases. Proceedings of the SIGMOD Conference 1999 ,pp. 594-596.
15. Ebru Killic, Gokhan Ozhan, Cevdet Dengi, Nihan Kesim, Pinal Koksal and Asuman Dogac, Experiences in using CORBA for a Multidatabase Implementation. In Proc. Of 6th Intl. Workshop on Database and Expert System Applications, London, Sept. 1995
16. Belsis A. Meletis, Nick Godwin, Leon Smalov. *Delivering Secure Manufacturing IT Systems within the CORBA Security Framework*. 14th International Conference on Systems Engineering (ICSE), Coventry, UK, 12-14 September 2000
17. Androutsopoulos I., Ritchie G.D., and Thanisch P. Natural Language Interfaces to DBs - An Introduction. Natural Language Engineering, vol. 1, part 1. Cambridge University Press, pp.29-81, 1995.
18. Ott N., Aspects of the automatic Generation of SQL Statements in a Natural Language Query Interface, Information Systems, 17(2),pp.147-159,1992.