A SECURITY APPROACH OF DISTRIBUTED FINANCIAL INFORMATION SYSTEMS IN GREECE

Dimitrios I. Maditinos[a], Željko Šević[b] and Nikolaos C. Kokkinos[c*]

[a] *Kavala Institute of Technology, School of Business and Economics, Department of Business Administration, Ag. Loukas, 65404 Kavala, Greece*
E-mail: dmadi@teikav.edu.gr

[b] *Glasgow Caledonian University, Business School, Cowcaddens Road, Glasgow G4 0BA, UK*
E-mail: Zeljko.Sevic@gcal.ac.uk

[c] *Kavala Institute of Technology, School of Technological Applications, Department of Petroleum & Natural Gas Technology, Ag. Loukas, 65404 Kavala, Greece*
E-mail: nikokkinos@mwpc.gr

Abstract

The importance and the sensitivity of financial data make the security of financial information systems a very significant prospect for every enterprise. A survey in fifty large enterprises of the private and public sector of Greece sheds light to the hidden points of view of security in distributed financial information systems. Thus, several in-depth interviews with the CIO (Chief Information Officers) and/or system administrators and also observations on the spot took place in order to examine the security policy of the FIS (Financial Information Systems) in distributed computer networks. User authentication policy, audit trails events, CIO's/system administrators' graduated studies are the mainly examined criteria in this study. The results show that the Greek companies need to realise and to take more seriously the fact that security is not something extra, but a normal part of performing business.

Keywords: Security, Financial information systems, Distributed networks.

1 INTRODUCTION

Nowadays, advances in network technology and the globalisation of markets and business processes have created a revolution in business and information systems (Calderon, Chandra and Cheh, 2006). The well-known term "business" is converted to "e-business" ("e-" refer to various technology-enabled business activities) upgrading its main infrastructure. The main infrastructure for e-business consists of corporate computer networks which compose the backbone of distributed financial information systems (Prabhu and Raghavan, 1996). Nevertheless, Bertolotti *et al.* (2007) underlined that computer networks are exposed to serious security threats (attacks from hackers, malicious users or even cyber-terrorists who use hi-tech abuse techniques and methods to commit computer fraud) that can even have catastrophic consequences from both the economy points of view and safety. Throughout history, successful business relationships have been fundamentally based on trust, so naturally a secured, comprehensive and trusted infrastructure is essential to the future success of the firm. However, how secure, reliable, consistent and valid are the distributed financial information systems? A survey in several large private enterprises and public organisations in Greece sheds light to the hidden points of view of security in distributed financial information systems (FIS). The

* Corresponding author

observation of the technical network specifications as well as the analysis of the security policies of the examined enterprises are the main targets of the current study.

In spite of the fact that the computer networks offer a lot of worthy of remark services and advantages, many expanded threats appear to the FIS and eventually to the whole enterprise. A computer-system threat has various types and effects. It is remarkable that the number of the threats is increasing while the technology is developing (Allen *et al.*, 2000). Therefore, system security is a very important issue, which the Chief Information Officers (CIO), system administrators, supervisors and managers ought to take it into serious consideration. System security also consists of many and various components. A user name and a password is only one of the known safety measures against expanded threats. Furthermore, there are a lot of other types of security such as data encryption, routing verification procedures, intrusion detection etc. Consequently, security issues deserve caution by any serious organization and especially, the security of FIS. That is why a survey takes place in order to examine specific factors that seriously affect the security of distributed FIS of several large enterprises. The password policy, audit trails events, the use of Kerberos system and CIO's/system administrator's graduated studies are examined in this work. Throughout this survey, primary data were gathered from fifty large private industrial plants and public national organisations in Greece (several interviews and observations took place).

2 THEORETICAL BACKGROUND

2.1 Financial Information Systems (FIS)

The main obligation of FIS is to keep updated and under control not only the revenue, the expenditure, the production and the human resources/payroll cycle of a firm, but also the general ledger and the reporting system of a firm (Romney and Steinbart, 2003). Thus, financial information systems offer: operational assist to a firm (keeping track of transactions), knowledgeable support (using computerized tools for quick and easy support in investments), managerial aid (controlling financial resources) and strategic development of the organization (establishing long-term investments goals and providing long-range forecasts of the firm's financial performance). The above features of FIS are achieved and integrated with the use of enterprise resource planning (ERP) system applications. ERP systems integrate all the operational aspects of a firm with the traditional accounting-financial functions. The corporate data are kept in databases and a database management system (DBMS) is responsible for the data exploitation and sharing. Romney and Steinbart (2003, p. 335) mentioned that "in response to the Y2K issue, many large organizations replaced their disparate stand-alone legacy systems with integrated information systems, such as enterprise resource planning (ERP) systems". Nowadays, it has been observed that there is a wide use of ERP systems by most of the contemporary enterprises.

2.2 Computer fraud and the necessity of information system security

The Securing Proprietary Information Committee of the American Society of Industrial Security observed that the value of a company's future lies not in its tangible assets, but in the "intellectual capital" of the business (Carter and Katz, 1997). In most businesses today, intellectual property is kept in computers by means of data, information and computerised processes. As a consequence, the computer has become the target -and many times the instrument- of e-crimes. Romney and Steinbart (2003) mentioned that many computer frauds go undetected and only 5 to 20 per cent of computer crime is detected. The reason for the above mentioned finding is the existence of many different kinds of computer threats using various and modern techniques. Trojan horses, virus hoaxes, adware, spyware, remote access programs, dialers, hack tools, e-mail threats, e-mail forgery, e-mail bombs, e-mail spamming, trap door, data diddling, data leakage, logic time bomb, round-down and salami technique are only few of the well-known computer frauds and abuse techniques. That is why Allen *et*

al. (2000) mentioned that while experienced intruders are getting smarter -as demonstrated by the increased sophistication in the types of attacks- the knowledge required on the part of novice intruders to copy and launch known methods of attack is decreasing (Figure 1).

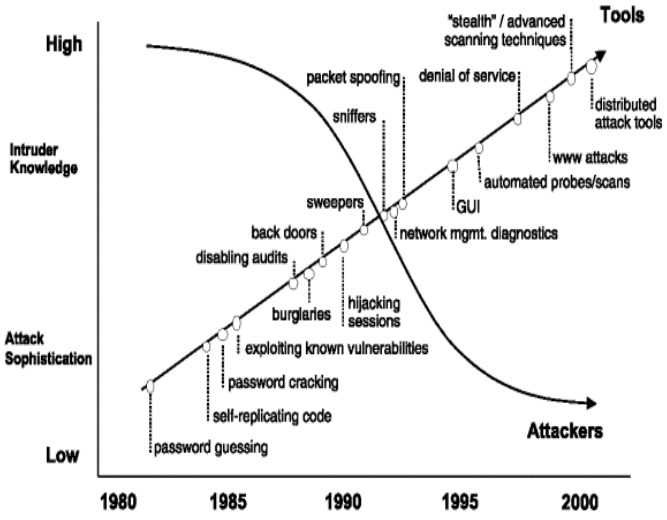

Figure 1. Attack Sophistication vs. Intruder Technical Knowledge (Allen et al., 2000).

Nevertheless, studies revealed that most employees don't even give a minute per hour of their workday for IT security (Luzwick, 2004). Most enterprises employ system administrators, information system security officers (ISSOs), physical security, operations security or other security professionals only when their network or applications do not respond. Looking to the facts, Microsoft's Millennium Edition was cracked before it was released, Microsoft Outlook was exploited, and without executable files in attachments, also Adobe Acrobat, Netscape Navigator, Microsoft's Internet Explorer, Word, Excel, Access and Cisco's gigabit Ethernet router family were exploited, too. Consequently, it is really wise and important for every company to organize security policies and use the proper security tools and techniques for achieving integrity, reliability, availability and accuracy to its information systems.

2.3 Secure password policies

Crume (2004) cited that according to a survey by Barron McCann, 92 per cent of IT managers prefer to use passwords as protection from possible data thieves. This means that information systems are only as secure as the weakest password (Schneier, 2000, p. 139). Hacking or cracking can be slowed down significantly or even defeated through the use of strong passwords. According to Microsoft Security Guidance Kit (2004) and to SANS Institute Password Policy (2005), a strong password is a password that includes characters from at least three of the five groups in the character classes table (Table 1). In addition, the longer the password the more difficult it is to break. Crume (2004, p. 1) stated that "a 4-digitnumeric password could be cracked on a modest PC in 0.02 seconds -faster than you can blink your eyes". However, the longer the passwords are the more difficult it is the users to remember them (Warkentin, Davis and Bekkering, 2004; Schneier, 2000). Furthermore, the length of a password depends also on the operating system. The maximum password size on many UNIX systems is eight characters and some newer versions of UNIX support 16-character passwords (Cooper *et al.*, 1995). In Windows NT 4.0 or earlier, Windows 2000, Windows XP, and Windows Server 2003, passwords up to fifteen or more characters are supported (Microsoft Security Guidance Kit, 2004). Consequently, creating passwords with both complexity and length makes it the most difficult of all to break.

Group	Example
Lowercase letters	a, b, c, …
Uppercase letters	A, B, C, …
Numerals	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Non-alphanumeric (symbols)	( ) ` ~ ! @ # $ % ^ & * - + = | \ { } [ ] : ; " ' < > , . ? /
Unicode characters	€, □, *f*, and ?

Table 1. Character Classes Table.

Choosing a secure password is mainly a matter of individual responsibility and training, too (Cooper *et al.*, 1995; Charoen, Raman and Olfman, 2005). Thus, a couple of secure password techniques have been developed in order to help end-users and system administrators to keep their passwords safe. One of the best secure password techniques is the use of smart cards (Hancock, 1999). These smart cards generate a new and unique password every minute. The information system uses the same algorithm and generates the same passwords, because it is time-synchronized with the smart cards. The specific password procedure requires a user to enter a value obtained from a smart card when asked for a password by the computer. Even though it is a better way of dealing with authorization than with the traditional password approach, it is more expensive and maybe a little bit inconvenient to carry the smart card. Moreover, an alternative password technique which is based on the confidentiality of the systematically repeated change of passwords is the password age. The system administrators ought to adjust properly the maximum password age (in days). This adjustment determines how many days a password can be used before the user is required to change it.

2.4 Audit trails

Another security technique, which has been developed for financial information systems since the inception of computers, is audit trails (Allinson, 2001). Although in the beginning the audit trails were used in accounting for the checking of financial reliability of a business, nowadays has become a process of recording a series of specific events occurred in an information system. Cooper *et al.* (1995) defined audit trails as any file that records the time users log in, from where they log in, what they try to do, and any other action a CIO might want to save for later analysis. In other words, audit trails can provide CIO with valuable information in tracking security violation and brake-in attempts. Therefore, audit trails seriously contribute to a process verification of an information system, as well as to fraud prevention. Despite the important contribution of audit trails to information system security, an Australia wide survey in the Australian Commonwealth and State Governments revealed that most organisations approach audit trails with inconsistently and incomprehensively (Allinson, 2001).

It is also worth mentioning that most of the current computer and network operating systems offer audit trails utilities. UNIX network operating system provides a large number of auditing and logging tools and utilities. Most of them are enabled by default system configuration and some others must be turned on and configured by the administrator. Some common UNIX logs are: lastlog (keeps track of each user's most recent login time and each user's originating destination), UTMP (keeps track only of online users), WTMP (keeps track of logins, logouts and normal system shutdowns, reboots), syslog (is a very powerful message-logging facility which keeps tracks of a variety of programs) and history (keeps a record of recent commands entered by user). In addition, Cooper *et al.* (1995) noticed that some UNIX versions include sniffing utilities such as tcpdump or snoop, which belong to Ethernet sniffer programs (they log all activity over the local Ethernet segment). On the other hand, Windows stores its log files in a special format that can be read using the Event Viewer Application from the Administrative Tools program group.

2.5 Data encryption

Due to the extraordinary growth of the Internet and technology-enabled business activities, many organizations rely on encryption to protect sensitive information transmitted over the Internet and other networks. In the field of on-line applications and client/server computing, where the communications medium is TCP/IP, Kerberos protocol is commonly used (the name comes from Greek Mythology). Kerberos is an authentication system that is part of project Athena at Massachusetts Institute of Technology - MIT (MiUen *et al.*, 1987). Pfleeger (2000) mentioned that Kerberos is a system that supports authentication in distributed information systems. The basis of Kerberos is a central server (authentication server-AS) that knows the passwords of all users and stores these in a centralized database; it also provides authenticated tokens, called tickets, to requesting applications. Thus, the user of a Kerberos enabled distributed FIS has the facility to log in once and uses a variety of services during a specific session, without the inconvenience of explicitly authenticating (Neuman and Ts'o, 1994). Kerberos has been adopted by many enterprises, universities and organizations, and implementations are available for all major operating systems (Butlera *et al.*, 2006).

3 METHODOLOGY

Taking into consideration the above mentioned theoretical and empirical background, an integrative survey was designed and took place in fifty Greek large private industrial plants and public national organisations. The main purpose of the survey is firstly, to examine thoroughly the infrastructure of each industrial plant and organisation, and then, to focus on the specific security issues of the observed distributed FIS, individually.

The survey was conducted by in-depth interviews with the CIO and/or system administrators and afterwards by several observations on the spot. Thus, a first contact type of e-mail with an attached automated-electronic form was sent to many CIO, system administrators and IT consultants in Greece. The particular electronic form informed the receivers about the subject, the questions and the purpose of the interview. Then, each enterprise and organisation filled the form and sent it back to the author by e-mail. After the first data gathering by e-mail, several interviews (some of them by telephone communication, due to the big distances) with the CIO of the firms/organisations were arranged in order to illuminate every obscure corner of the study. In addition, in some cases the final verification of the corporate data was achieved by author thorough observation of the current distributed network infrastructure of the examined FIS. Eventually, all the collected data (gathered by e-mails, interviews and observations) were structured, tabulated and encoded by two different statistical software applications.

The content of the above data gathering was orientated into two sections. In the first section, the technical specifications of the observed computer networks were identified in order to ensure the existence and the operational conditions of a distributed FIS. Thus, the geographical scope of the network, the network topology, the type of data communication cables, the nominal data network speed, the type of router, the number of corporate servers, the type of servers and clients depended on use, the CPU (Central Processing Unit(s)) and the NOS (Network Operating System) of the servers, the CPU and the OS (Operating System) of the clients were examined. In the second section of the collected data, a security approach of the above defined distributed FIS took place. Hence, the first factor that was investigated was the type of the password the users choose for accessing FIS resources. A sample of 30 per cent of the users within the examined organisations was participated in this survey (more than adequate for statistical analysis). Four types of password authentication were checked: simple passwords (insecure passwords, which have small length and homogeneous characters), complex passwords (passwords with both complexity and length), complex passwords with specific expiration date and the use of smart cards (one of the best modern password techniques). The second examined security issue was the audit trail events of the FIS. According to Allinson (2001), five

significant parameters were examined in this survey the audit trail generation, the audit trail retention, the audit trail storage, the existence of enhanced security mechanisms and the responsibility for audit trails. Another examined security parameter was the use of Kerberos protocol in the FIS network and the relation of CIO's/system administrator's graduated studies with Information Technology field. In point of the later parameter, it is noticeable that in some of the examined enterprises and organisations the CIO and the system administrator was the same person; and in other cases, there was only system administrator.

4 RESULTS AND DISCUSSION

The research modelling appealed to fifty Greek large private companies and public organisations that used distributed FIS. Twenty five private firms of the sample were large industrial plants and the rest of the sample consisted of public national organisations (Appendix 1). The main criterion of the sample selection was the FIS of every Greek large enterprise or organisation to be based upon a distributed computer network, which consists of a switched Ethernet type of local area network (LAN) with a gateway to the Internet (Figure 2). Thus, the first section of data gathering (concerning technical network specifications) took place in order to ensure that the sample follows the requirements of the study. According to the first section of data gathering, it was found that apart from the corporate LAN, ten of the fifty firms used also a wide area network (WAN) or a metropolitan area network (MAN). Nevertheless, the above isolated cases used separated gateways, which were dedicated for WAN or MAN use. Therefore, the above phenomenon did not affect the current survey. Though, there were several useful out coming information from the technical network specifications of the examined industrial plants and national organisations (first section of the survey), the main scope of this research paper is not computer science, but the security approach of distributed FIS (second section of the survey).

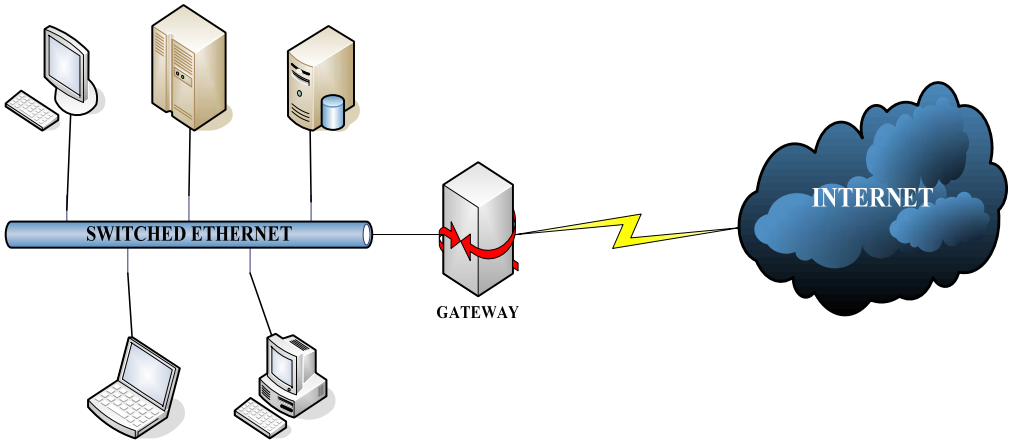

Figure 2. Network infrastructure of the examined distributed FIS.

The first examined security factor of the distributed FIS was the reliability of the password authentication, which was used by the 30 per cent of the users within the examined firms and organisations. The results revealed that the 32 per cent of the sample used simple password, 48 per cent used complex passwords and only the 20 per cent of the sample used complex passwords with specific expiration date (Figure 3). It is worth mentioning that 5 per cent of those who used simple password claimed that they knew how to make complex passwords, but they were afraid of forgetting them; and the rest of them (15 per cent) claimed that they had never been trained to use "strong passwords". Another important finding was that the 42 per cent of those who used complex passwords did not use password age, because this option has been disabled by the system administrator; and the other 6 per cent disabled it by their own for facility reasons. The lack of users' training and the lack of

time of IT support department to occupy with expired passwords are in line with the theoretical background (Warkentin, Davis and Bekkering, 2004; Schneier, 2000; Charoen, Raman and Olfman, 2005). Furthermore, Table 4 (Appendix 2) shows that there is a significant statistical association between the IT graduated studies of CIO/system administrator and the level of security of users' passwords [$x^2(2)=9.48$, $p<.01$]. For instance, 87.5 per cent of the users, who used simple passwords, work in companies or organisations with non-IT graduates CIO/system administrators and the 60 per cent of the users, who used complex passwords, worked in companies or organisations with IT graduates CIO/system administrators. The above observation reflects the fact that the users of the examined firms and organisations, whose CIO/system administrators were IT graduates, used more secure passwords than the users of the companies and organisations with non-IT graduates CIO/system administrators. Unfortunately, none of the examined enterprises or organisations used smart cards for password authentication; most of them believed that it is too excessive, expensive and also complicated technique.

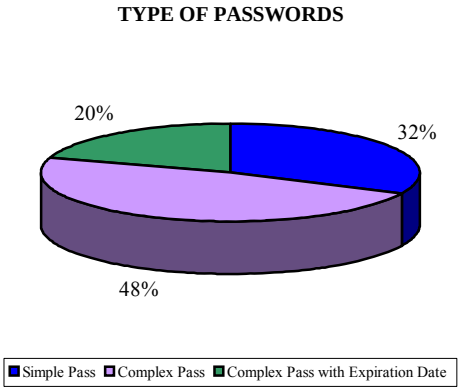

Figure 3. Type of password protection.

Audit trail was the next examined variable in the security of a distributed FIS. Five important parameters of audit trails were examined in this survey (Allinson, 2001). The generation of audit trails by the companies and the proper attention to them was the first examined parameter. In other words how many companies and organisations wittingly not only generate audit trails by the use of software tools, but also study them. According to Table 3 (Appendix 1) only 28 per cent of the companies and organisations generated audit trails and paid the proper attention to them. Many CIO/system administrators stated that they cannot undertake all the security-related duties they want due to the overwhelming daily FIS obligations. The next examined parameters (Table 3, Appendix 1) referred only to those companies and organisations that generate audit trails (i.e. 28 per cent of the initial sample). Thus, 50 per cent of the companies and organisations that generated audit trails retained them for up to 2 years and the rest of them for more that 2 years. Most of them (50 per cent) kept the audit trails on same the file server with the other corporate data, the 42.9 per cent used peripheral storage devices for audit trails retaining and only 7.1 per cent used a separated server for audit trails. Moreover, most of the firms and organisations (71.4 per cent) did not use security mechanisms (password authentication or data encryption) for protected the audit trails from unauthorised access; and only 28.6 per cent used password protection for accessing the folder of audit trails. The responsibility and the control for audit trails from a security perspective belonged equally to information system department (35.7 per cent) and to system administrator (35.7 per cent); the responsibility for the audit trails of the rest percentage belonged to the business owners, while neither a firm nor organisation had established an audit department. Comparing the results of the companies and organisations that generated audit trails with the IT graduated studies of their CIO/system administrators there is a significant relationship [$x^2(1)= 5.93$, $p<.05$]. This seems to represent the fact

that based on the odds ratio ($odds\,ratio = \frac{odds_{non-IT\ graduate\ doesn't\ use\ AT}}{odds_{IT\ graduate\ uses\ AT}} = \frac{\frac{24}{12}}{\frac{4}{10}} = 5$) (Field, 2005) CIO/system administrators were 5 times more likely not to be IT graduates if they did not used audit trails than if they used audit trails.

Based upon the results of the above security factors, it is easily understandable that IT graduated studies of the CIO/system administrators play a significant role in the security level of a distributed FIS. A CIO/system administrator aught to stand not only upon its experiences, but also upon its educational provision. In addition, a cross-tabulation of the sector (public or private) of the companies and organisations with the IT graduated studies of their CIO/system administrators (Table 6, Appendix 2) revealed that there is a significant statistical association [$x^2(2)= 5.19$, $p<.05$]. For example, 72 per cent of the CIO/system administrators who worked in public sector were non-IT graduates and 60 per cent of the CIO/system administrators who worked in private sector were IT graduates. Pedestal on the odds ratio ($odds\,ratio = \frac{odds_{non-IT\ graduate\ belong\ to\ public\ sector}}{odds_{IT\ graduate\ belong\ to\ private\ sector}} = \frac{2.57}{0.67} = 3.84$), it seems to be a sign of the fact that CIO/system administrators were 3.84 times more likely not to be IT graduates if they belonged to the public sector than if they belonged to the private sector.

Another important examined security factor of the distributed FIS was the adaptation of Kerberos authentication system by the Greek private industrial plants and national organisations. However, in spite of the fact that Kerberos is a system that supports authentication in distributed systems, only 12 per cent of the examined sample used it. It seems that Kerberos is not a popular system in Greece and most of the firms did not use it, because they did not know it. Consequently, though name Kerberos comes from Greek Mythology, the Greek private industrial plants and public national organisations did not prefer to use Kerberos authentication system in their FIS.

5 CONCLUSIONS

Taking everything into consideration, several useful and remarkable conclusions could be drawn from the current survey. The lack of users' training and the lack of time of IT support department to occupy with expired passwords are the main reasons that make users of a distributed FIS to use simple and insecure passwords. Moreover, the overwhelming daily FIS obligations force CIO/system administrators to be inadequate to their stern security-related duties as the audit trails generation and study. In addition, IT graduated studies of the CIO/system administrators play a significant role in the security level of a distributed FIS. On the other hand, smart cards for password protection and Kerberos authentication system are not popular systems in Greece and most of the examined companies and organisations did not use them, because they did not even know them. Consequently, the Greek enterprises need to realise and take seriously the fact that security is not something extra, but a normal part of performing business. A better allocation of the information system department's duties and also, the development of new IT departments that would be dedicated to specific duties, as audit trails, it would alleviate the CIO/system administrators' burden and make them more productive and efficient. Hence, it is really wise for every company and organisation to develop security policies and uses the proper security tools and techniques for achieving integrity, reliability, availability and accuracy to its financial information system.

References

Allen, J., Alberts, C., Behrens, S., Laswell, B. and Wilson, W. (2000), *Improving the security of networked systems*, Pittsburg: Carnegie Mellon University's Software Engineering Institute.

Allinson, C. (2001), 'Information Systems Audit Trails in Legal Proceedings as Evidence', *Computers & Security*, **20**(5), pp. 409-421.

Bertolotti, C. I., Durante, L., Maggi, P., Sisto, R. and Valenzano, A. (2007), 'Improving the security of industrial networks by means of formal verification', *Computer Standards & Interfaces*, **29**(3), pp. 387-397.

Butlera, F., Cervesatob, I., Jaggardc, D. A., Scedrovd, A. and Walstadd, C. (2006), 'Formal analysis of Kerberos 5', *Theoretical Computer Science*, **367**, pp. 57-87.

Calderon, T.G., Chandra, A. and Cheh, J. J. (2006), 'Modeling an intelligent continuous authentication system to protect financial information resources', *International Journal of Accounting Information Systems*, **7**(2), pp. 91-109.

Charoen, D., Raman, M. and Olfman, L. (2008), 'Improving end user behaviour in password utilization: An action research initiative', *Systemic Practice and Action Research*, **21**(1), pp. 55-72.

Cooper, J. F., Goggans, C., Halvey, J. K., Hughes, L., Morgan, L., Siyan, K., Stallings, W. and Stephenson, P. (1995), *Implementing Internet Security*, Indianapolis: New Riders Publishing.

Crume, J. (2004), *Inside Internet security - What hackers don't want you to know*, Addison-Wesley.

Field, A. (2005), *Discovering statistics using SPSS*, Second Edition, London: Sage Publications.

Hancock, B. (1999), 'Smart Card Security Users Group created to ensure highest standards of security', *Computers & Security*, **18**(8), pp. 653-654.

Luzwick, P. (2004), 'Security? Who's got time for security? I'm trying to get my job done', *Computer Fraud & Security*, Oxford: Mayfield Press, pp. 16-17.

Microsoft, Security Guidance Kit, CD-ROM edition, Spring 2004.

MiUen, S. P., Norman, C., Schiller, J. I. and Saltzer, J. H. (1987), *Kerberos authentication and authorization system, Project Athena Technical Plan, Section E.2.1*, Cambridge: MIT.

Neuman, C.and Ts'o, T. (1994), 'Kerberos: an authentication service for computer networks', *IEEE Communications*, **32**(9), pp. 33–38.

O' Mahony, A. and Doran, J. (2008), 'The Changing Role of Management Accountants; Evidence From the Implementation of ERP Systems in Large Organisations', *International Journal of Business and Management*, **3**(8), pp. 109-115.

Password Policy (2005) SANS Institute, http://www.sans.org/resources/policies/Password_Policy.pdf.

Pfleeger, P. C. (1997), *Security in Computing*, Second Edition, Upper Saddle River: Prentice Hall.

Prabhu, M. M. and Raghavan, S. V. (1996), 'Security in computer networks and distributed systems', *Computer Communications*, **19**(5), pp. 379-388.

Romney, B. M. and Steinbart, J. P. (2003), *Accounting information systems*, Ninth Edition, Upper Saddle River: Prentice Hall.

Schneier, B. (2000), *Secrets and lies*, New York: John Wiley and Sons.

Warkentin, M., Davis, K. and Bekkering, E. (2004), 'Introducing the Check-off password system (COPS): an advancement in user authentication methods and information security', *Journal of Organizational and End User Computing*, **16**(3), p. 41.

APPENDIX 1. FREQUENCY TABLES

Statistics

		Password	Kerberos Use	IT Graduate	Sector
N	Valid	50	50	50	50
	Missing	0	0	0	0

Password

		Frequency	Percent	Cumulative Percent
Valid	Simple	16	32.0	32.0
	Complex	24	48.0	80.0
	Complex with date	10	20.0	100.0
	Total	50	100.0	

Kerberos Use

		Frequency	Percent	Cumulative Percent
Valid	No	44	88.0	88.0
	Yes	6	12.0	100.0
	Total	50	100.0	

IT Graduate

		Frequency	Percent	Cumulative Percent
Valid	No	28	56.0	56.0
	Yes	22	44.0	100.0
	Total	50	100.0	

Sector

		Frequency	Percent	Cumulative Percent
Valid	Public	25	50.0	50.0
	Private	25	50.0	100.0
	Total	50	100.0	

Table 2. Frequency table of Password, Kerberos Use, IT Graduate and Sector security variables of the FIS.

Statistics

		Audit trail generation	Audit trail retention	Audit trail storage	Enchanced security mechanisms	Responsibility for audit trails
N	Valid	50	14	14	14	14
	Missing	0	0	0	0	0

Audit trail generation

		Frequency	Percent	Cumulative Percent
Valid	No	36	72.0	72.0
	Yes	14	28.0	100.0
	Total	50	100.0	

Audit trail retention

		Frequency	Percent	Cumulative Percent
Valid	<2Yrs	7	50.0	50.0
	>2Yrs	7	50.0	100.0
Total		14	100.0	

Audit trail storage

		Frequency	Percent	Cumulative Percent
Valid	Peripheral Storage Device	6	42.9	42.9
	Separate files on same server as data	7	50.0	92.9
	Separate server	1	7.1	100.0
Total		14	100.0	

Enchanced security mechanisms

		Frequency	Percent	Cumulative Percent
Valid	Not used	10	71.4	71.4
	Password protected folder	4	28.6	100.0
Total		14	100.0	

Responsibility for audit trails

		Frequency	Percent	Cumulative Percent
Valid	System Admin	5	35.7	35.7
	Information system Dept.	5	35.7	71.4

Business owner	4	28.6	100.0
Total	14	100.0	

Table 3. Frequency table of the five parameters of Audit Trails security variable.

APPENDIX 2. CROSS-TABULATIONS – CHI SQUARE ANALYSIS

			Password			
			Simple	Complex	Complex with date	Total
IT Graduate	No	Count	14	10	4	28
		% within IT Graduate	50.0%	35.7%	14.3%	100.0%
		% within Password	87.5%	41.7%	40.0%	56.0%
	Yes	Count	2	14	6	22
		% within IT Graduate	9.1%	63.6%	27.3%	100.0%
		% within Password	12.5%	58.3%	60.0%	44.0%
	Total	Count	16	24	10	50
		% within IT Graduate	32.0%	48.0%	20.0%	100.0%
		% within Password	100.0%	100.0%	100.0%	100.0%

(X^2=9.48, DF=2, p=0.009)

Table 4. Cross-tabulation and X^2 analysis of variables: "IT graduated studies of CIO/system administrator" and "Password".

			Audit trail generation		
			No	Yes	Total
IT Graduate	No	Count	24	4	28
		% within IT Graduate	85.7%	14.3%	100.0%
		% within Audit trail generation	66.7%	28.6%	56.0%
	Yes	Count	12	10	22
		% within IT Graduate	54.5%	45.5%	100.0%
		% within Audit trail generation	33.3%	71.4%	44.0%
	Total	Count	36	14	50
		% within IT Graduate	72.0%	28.0%	100.0%
		% within Audit trail generation	100.0%	100.0%	100.0%

(X^2=5.93, DF=1, p=0.015)

Table 5. Cross-tabulation and X^2 analysis of variables: "IT graduated studies of CIO/system administrator" and "Audit trails".

			Sector		
			Public	Private	Total
IT Graduate	No	Count	18	10	28
		% within IT Graduate	64.3%	35.7%	100.0%
		% within Sector	72.0%	40.0%	56.0%
	Yes	Count	7	15	22
		% within IT Graduate	31.8%	68.2%	100.0%
		% within Sector	28.0%	60.0%	44.0%
	Total	Count	25	25	50
		% within IT Graduate	50.0%	50.0%	100.0%
		% within Sector	100.0%	100.0%	100.0%

(X^2=5.19, DF=2, p=0.023)

Table 6. Cross-tabulation and X^2 analysis of variables: "IT graduated studies of CIO/system administrator" and "Sector".