Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2013, Article ID 569562, 11 pages
http://dx.doi.org/10.1155/2013/569562

Research Article

Enterprise Information Security Management Based on Context-Aware RBAC and Communication Monitoring Technology

Mei-Yu Wu and Ming-Hsien Yu

Department of Information Management, Chung Hua University, Section 2, 707 WuFu Road, Hsinchu 30012, Taiwan

Correspondence should be addressed to Mei-Yu Wu; mywu@chu.edu.tw

Received 5 July 2013; Revised 11 October 2013; Accepted 15 October 2013

Academic Editor: Jung-Fa Tsai

Information technology has an enormous influence in many enterprises. Computers have not only become important devices that people rely on in their daily lives and work, but have also become essential tools for enterprises. More and more enterprises have shifted their focus to how to prevent outer forces from invading and stealing from networks. However, many enterprises have disregarded the significance of internal leaking, which also plays a vital role in information management. This research proposes an information security management approach that is based on context-aware role-based access control (RBAC) and communication monitoring technology, in order to achieve enterprise information security management. In this work, it is suggested that an enterprise may, first, use an organizational chart to list job roles and corresponding permissions. RBAC is a model that focuses on different work tasks and duties. Subsequently, the enterprise may define a security policy to enforce the context-aware RBAC model. Finally, the enterprise may use communication monitoring technology in order to implement information security management. The main contribution of this work is the potential it provides to both reduce information security incidents, such as internal information leakage, and allow for effective cost control of information systems.

1. Introduction

Nowadays, in the workplace, information technology has an enormous influence on many enterprises. Computers have not only become important devices that people rely on in their daily lives and at work, but have also become essential tools for enterprises. However, while advantages come with the prevalence of information technologies, disadvantages also present themselves. More and more enterprises have had to shift their focus to how to prevent outer forces from invading and stealing from their networks. However, a number of firms have disregarded the significance of internal leaking, which plays a vital role in information management [1]. According to a network security survey, most information security threats occur internally, and not externally. A threat is a potential cause of an unwanted incident that could result in harm to a system or organization. Different types of information threats include computer viruses, spyware, operating system vulnerabilities, malicious Web sites, malware, worms, and other attacks. Some employees are only slightly aware of information security and transmit sensitive and unencrypted information across networks. Some corporate staff use external storage devices to bring important data files home, and malicious users could take critical data to competitors. If an enterprise underestimates the implications of internal network security, it could suffer from the loss of many valuable core technologies, technical information, and patents. Therefore, the enforcement of information security management, policies, and regulations is an important and imperative issue.

With the development of information technology, more and more information products have been developed. With the advent of new information equipment, system administrators should have the ability to improve information security management policies. Each modification of an information security management policy will take a lot of time. Defining a management approach is therefore necessary for

any enterprise [2, 3]. However, the defined approach cannot be applied across the board to each user. That is, different users should have different permissions or blocking functions in order to reduce information security incidents.

Role-based access control (RBAC) has become a widely accepted access control mechanism for security management [3–6]. In a role-based access control model, a user can play several roles and a role can be assigned to several users. Permission assignments are not assigned to users but rather to roles. For different roles, enterprises should define corresponding information security management policies. For example, users in the sales and purchasing department may be able to use the Internet. However, there are relatively few users in the human resources or manufacturing departments who need to use the Internet during work. According to the different requirements and operational situations of each role, the enterprise should define different information security management policies. For example, in the manufacturing department, production line workers are not allowed to own individual computers, so the security management policy for production line staff does not need to include information equipment control. That is, in terms of the information security management issue, the level of threat is lower. In the sales departments, most staff members have mobile devices, such as notebook computers, smart phones, external storage devices, and tablet computers, due to the requirements of their jobs. A security management policy for sales staff, then, should focus on permissions for, and the control of, removable devices.

However, the funds that are able to be invested in information security monitoring control equipment are limited for small and medium enterprises. Given this, this research proposes an information security management approach that is based on context-aware role-based access control (RBAC) and communication monitoring technology. This research adopts RBAC in order to use limited resources to achieve comprehensive planning and save unnecessary waste and expenses. According to our information security management policy, the system gives different permissions to different roles and adopts different information monitoring devices to control those with different roles. The main objective of this work is to use minimal resources for the deployment and implementation of an information security management policy in order to achieve effective management.

The remainder of this paper is organized as follows. Section 2 reviews related work on information security management, the concept of access control, context-aware control, and communication monitoring technology. Section 3 introduces the proposed enterprise information security management system based on a context-aware RBAC and communication monitoring technology. System architecture and relevant discussions are shown in Section 4. Finally, in Section 5, conclusions are presented.

2. Related Work

The related literature covers information security management, access control models, context-aware control models, and communication monitoring technology.

2.1. Information Security Management. Information security refers to the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to ensure confidentiality, integrity, and availability [7]. Due to higher transmission speeds and the growing popularity of the Internet, data transmission across networks is common. The need for information security has become more and more important. Networks provide convenient data transmission but also, indirectly, result in information security concerns. Therefore, information security management is an important issue that cannot be ignored by enterprises. An information security management system (ISMS) is one part of the overall management system and is based on a business risk approach, in order to establish, implement, operate, monitor, review, maintain, and improve information security [8]. ISMS is a set of policies concerned with information security management or IT-related risks. An information security policy is the foundation of any successful security system. However, it does not comprehensively guarantee the avoidance of external or internal attacks. Despite this, information security policies provide the basis for all information security planning and establish the rules for auditing user network behavior and access control privileges.

2.2. Access Control Models. Access control determines whether a user has permission to access a service when he or she requests this service. The most common access control policies contain discretionary access control (DAC), mandatory access control (MAC), and role-based access control (RBAC) [9, 10]. The National Institute of Standards and Technology (NIST) adopts RBAC as the standard, called NIST RBAC [11]. In this model, users are assigned to the appropriate role, and their access to resources is determined according to this role. The RBAC model provides relevant security policy objectives, such as least privilege, separation of duty, and data abstraction [3, 6, 9, 12, 13]. Separation of duty (SoD) is a security principle used to spread responsibility and authority for a complex action or task over different users or roles, in order to prevent fraud and error. Under this principle, conflicting (mutually exclusive) roles are authorized to different users. For example, "purchaser" and "cashier" are mutually exclusive roles and therefore should not be authorized to the same user. There are two kinds of separation of duty, that is, static separation of duty (SSD) and dynamic separation of duty (DSD). SSD restricts a user from possessing two mutually exclusive roles, while DSD allows a user to possess up to two mutually exclusive roles as long as these are not active at the same time.

Access control avoids unauthorized access to information or information processing facilities in order to reduce threats. A role-based access control model more efficiently manages a large number of users. RBAC is a practical solution to the distributed environment [14]. However, because of advances in technology, today's users are no longer affected by time and space constraints, and traditional RBAC does not take into account the suitability of the user's environment using the original set of roles and permissions. Dynamic adjustment

permissions according to the contextual information are therefore necessary for today's environment.

2.3. The Context-Aware Control Model. Dey and Abowd define context as any information that can be used to characterize the situation of an entity [15]. An entity is a person, place, or object that is considered relevant to the interaction between a user and an application, including the user and applications themselves [15, 16]. They focus on the context of the entities described according to the user's environment, social status, emotional status, and information status. Ryan considers context as location, environment, identity, and time [17]. Beika and Bernd regard the user's devices as different contexts, such as personal computers, personal digital assistants (PDA), and smart phones [18]. Although different researchers explore different cognitive contexts, the main target remains the same.

Bill and Marvin propose context awareness as application software that can be used depending on its location near staff and objects, as well as objects made according to time changes [19]. In other words, application software is able to change with people, matter, time, and place in the environment, leading to corresponding action. Dey and Abowd claim that a system is context aware if it uses context to provide relevant information and/or services to the user, where relevancy depends on the user's task [15, 16]. There are several roles in an enterprise. Before authorizing permissions to roles, the system should consider related context information and dynamically adjust privileges.

2.4. Communication Monitoring Technology. According to the 2007 electronic monitoring and surveillance survey conducted by the American Management Association (AMA) and the ePolicy Institute, more than one-fourth of employers have fired workers for misusing e-mail, and nearly one-third have fired employees for misusing the Internet [20]. Organizational staff may use computers, e-mail, or the Internet to leak internal critical information. Employers have gradually increased monitoring power to monitor employees. In order to achieve information security, the privacy of employees has become increasingly narrow.

Legal, organizational, social, and technical methods are often taken by enterprises to prevent information leakage [2, 21, 22]. In order to avoid information leakage, enterprises usually adopt a communication monitoring technology. Communication monitoring technology is one kind of technical methods and can be divided into several approaches, which include the logging and blocking of instant messaging (IM) messages, web mail content, and web browser content, as well as file licenses and USB device authorization. Through several communication monitoring technologies, all information within the enterprise is filtered, recorded, or even blocked in order to reduce the occurrence of internal leakage. Even when confidential information is leaked through improper channels, logged messages can be used as valid evidence.

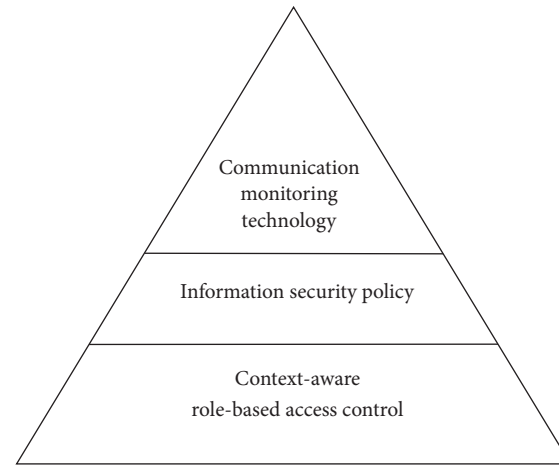

Figure 1: Research design.

3. The Proposed Approach for Enterprise Information Security Management

The research design of this work is illustrated in Figure 1. The design of the proposed approach is based on a context-aware role-based access control model. In a role-based access control model, a user can play several roles and a role can be assigned to several users. The permissions of a user are determined by authorized roles and related context information, such as location, time, and communication devices. The authorized permissions are enforced by an information security policy as defined by the enterprise. The information security policy will outline the implementation specification of security control and management. Finally, this research adopts communication technology to monitor or control equipment in order to achieve effective enterprise information security management.

3.1. Context-Aware RBAC Model. In this section, an enterprise information security management model is described. The enterprise information security management model is based on context-aware role-based access control and communication monitoring technology. The context-aware role-based access control (RBAC) model for enterprise information security management includes the users, roles, control groups, permissions, sessions, context information, and information security policy, as shown in Figure 2.

What follows is a detailed description of each component.

(1) Users: General Users. They are either an interactive human or an agent. In the enterprise environment, employees, contractors, or third party users are all regarded as users.

(2) Roles: Assigned to Users. Roles refer to the set of task functions or job positions. Users obtain permission and responsibility based on their roles and control groups.

(3) Control Groups: The Mapping of Roles and Communication Monitoring Technology. Several roles may adopt the same communication monitoring technology in order to control

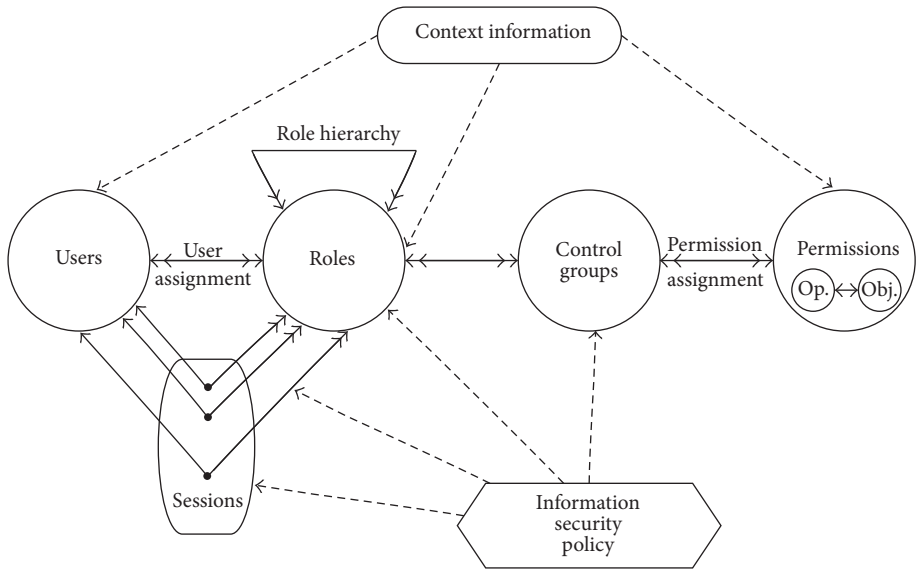

Figure 2: Context-aware RBAC model for enterprise ISMS.

privileges. For example, sales, procurement staff and R&D department personnel will use the Internet. An enterprise may define a control group, named web browser control group, to constrain permissions.

(4) Permissions: Operation of the Information Resource or Objects in the Access Control Model. Permission may involve a simple right, such as read, write, or execute, or complex rights, such as issue check, receive payment for a bank clerk, or use mobile devices.

(5) Sessions: The Time Necessary for the User to Take on a Role. A user can dynamically choose a role and execute the related work in a session.

(6) Context Information: The User's Environment Status. His device type, IP address, MAC address, current time, location, and so on.

(7) Information Security Policy. The rules, policy, and strategy defined by the enterprise in order to achieve information security management, such as all browsed web pages should be recorded and available times and locations to use wireless.

3.2. Information Security Policy and Communication Monitoring Technology. This study proposes an information security management model that is applicable to all kinds of enterprises, rather than only to the information technology industry. Because the threat of information security does not only exist in some specific industries, there is a demand for information security in various industries. Therefore, this research classifies all common roles/job positions in current industries. According to the job category of 104 Job Bank in Taiwan, this work divides roles into two types, that is, roles that require the use of IT equipment and roles that do not require the use of IT equipment. Roles that do not require information equipment are beyond the scope of our study. Therefore, this study only defines an information security policy in order to reduce information leakage for roles that require the use of information equipment.

The proposed context-aware RBAC model for enterprise ISMS is an extension of the RBAC model, and the main difference is the combination of context information, information security policy, and a novel element, that is, a control group, to allow various enterprises to improve information security management. Whether a user has the right to operate certain resources or objects is based on their respective roles. In addition, the information security policy should be satisfied and in compliance with related communication monitoring technology. A flowchart of the proposed architecture is shown in Figure 3.

The research analyzes common ways in which information is leaked in enterprises. In general, a user wants to bring files out from the enterprise. The available ways are through USB flash disks, file transfer protocol (FTP) transmissions, instant messaging (IM) software, e-mail, peer-to-peer (P2P) approaches, and web or cloud systems, CD writers, and so on. Therefore, this work defines several information security polices to avoid information leakage and proposes some related communication monitoring technologies to achieve effective information security management.

Based on related communication monitoring technologies, this research defines twelve control groups. Each control group contains a variety of roles, and the permissions for each role should be satisfied by the communication monitoring technology. A detailed description of each control group and its corresponding communication monitoring technology is described in the following.

(1) Network Behavior Control. For web browsing permission control, this research defines a control group, named the Web Behavior Control Group, which groups all users that need to

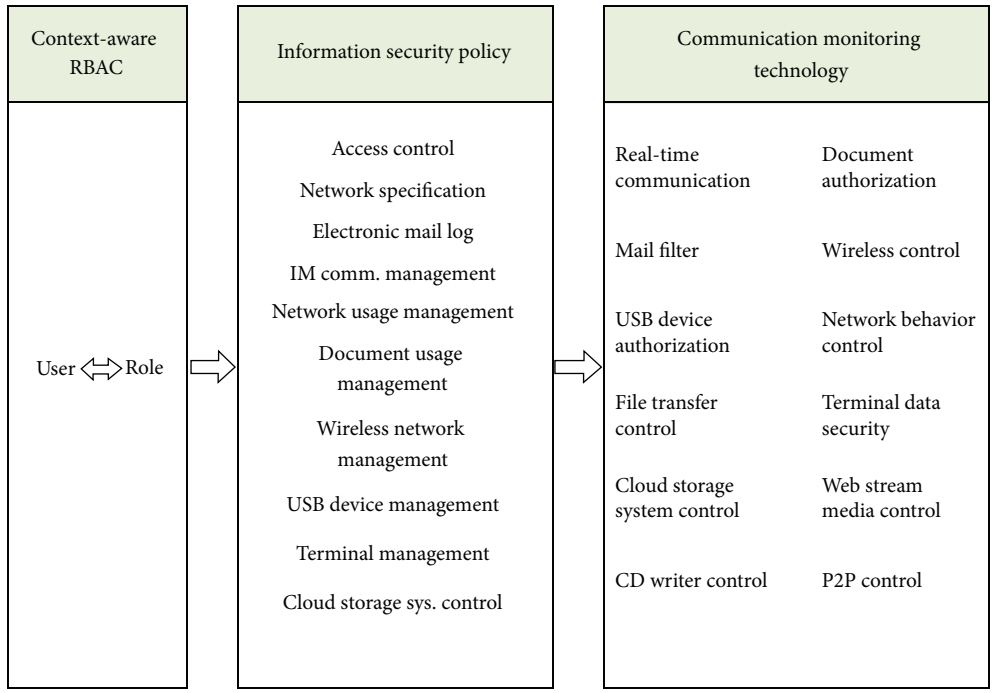

Figure 3: Flowchart of proposed architecture.

Table 1: Permissions for web browsing.

Control group	Roles		Communication monitoring technology
Web behavior control	Operations staff	System development staff	Webpage browsing/record/block
	Human resource staff	Maintenance staff	
	Administrative staff	Logistics staff	
	General staff	Drawing staff	
	Legal staff	Design staff	
	Marketing staff	Text staff	
	Planning staff	Media dissemination staff	
	Project management staff	Research staff	
	Sales staff	Financial staff	
	Trade staff		

use the Internet. Details related to permissions for the web behavior control group are shown in Table 1.

(2) IM Communication Management. Instant messaging (IM) software is the most difficult to control and the most frequently used communication tool. Enterprise users use IM software to communicate with others whether this communication is official or private, business related, or merely gossip. In addition to social networking sites, users use IM software to share personal information. Due to the convenience of IM software, it easily becomes one of channels used to leak information. The instant messaging software management policy is shown in Table 2.

(3) Mail Filtering Control. A mail server is an absolutely necessary system in the enterprise. Because of the presence of the mail server, the enterprise can communicate with outsiders in order to successfully carry out business-related tasks. However, the mail server often becomes an attack target. Hackers can use mail servers as springboards to attack other businesses or send spam.

This research adopts a firewall or antivirus strategy to defend against external attacks. However, internal information leakage cannot be protected in the same way as the previously mentioned approaches. If a user uses mail to send confidential data out, the hard work developed over years may be vital information for competitors. The system manager can adopt mail filtering management technology in order to avoid this situation. The system administrator can define specific keywords, sender accounts, receiver accounts, function variables, mail subjects, or content to block users from sending mail. Detailed permissions for mail filter control groups are shown in Table 3.

(4) Document Usage Management. All management policies, technical documents, management forms, contracts,

Table 2: Permissions for IM software.

Control group	Roles		Communication monitoring technology
IM communication management	Operations staff	Sales staff	Record instant messaging content/block file transfers
	Human resource staff	Trade staff	
	Administrative staff	System development staff	
	General staff	Text staff	
	Legal staff	Research staff	
	Marketing staff	Financial staff	
	Project management staff		

Table 3: Permissions for mail.

Control group	Roles		Communication monitoring technology
Mail filtering management	Operations staff	Project management staff	Mail auditing/record/release/block
	Human resource staff	Sales staff	
	Administrative staff	System development staff	
	General staff	Trade staff	
	Legal staff	Research staff	
	Marketing staff	Financial staff	
	Planning staff		

Table 4: Permissions for document usage.

Control group	Roles	Communication monitoring technology
DRM management	Marketing staff Sales staff	Read/bring out/open/ print/control and audit

quotations, and so on are archived and this is likely to be accessed. It is therefore essential to ensure that borrowing staff do not leak this information. The best way to educate and train users as well as to define borrowing rules is to use document management software. When enterprises adopt document management software, such as digital right management (DRM) software, this research can limit the number of documents that are allowed to be open at any time, cancel printing functions, read only functions, and available dates and times. Detailed permissions for document usage management control groups are shown in Table 4.

(5) Wireless Network Management. The wireless network privilege should be rigorous and prudent. For most enterprises, users should not be authorized to use notebooks in addition to sales and secretaries. Smart phones and tablet PCs are popular at present. If an enterprise does not have an effective control for wireless networks, users may misuse the wireless network resource and cause further information leakage. Enterprises should have a clear definition of acceptable wireless network usage. Detailed permissions for wireless network management control groups are shown in Table 5.

(6) USB Device Management. USB flash disks are convenient plug and play devices. Due to their convenience, USB devices often cause information leakage. Therefore, USB devices should be strictly controlled such that all USB devices should be shut down in the office. The right to use USB devices should only be given to staff that really needs them. Detailed permissions for USB device management control groups are shown in Table 6.

(7) P2P Usage Control. Peer to peer network technology is facilitated in order to search for and share files across the network. Given the convenience of network sharing, it is able to bring about greater disasters and so copyright is even more necessary. Through P2P software, users can obtain files that should not be shared over the network. Government agency files and internal documents of the enterprise can be downloaded or browsed by anyone. As a result, this not only seriously affects network bandwidth, but also causes information leakage. Detailed permissions for P2P usage control groups are shown in Table 7.

(8) File Transfer Control. When a file exceeds the limitations of the mail server, users must transfer the file through the Internet. FTP transmission is usually the primary way in which system administrators transfer files. Users can transfer larger files across the FTP server and the receiver downloads these files through FTP or HTTP transmission. In this way, large files can be exchanged in a short period of time. However, if certain users have bad intentions, then information leakage can happen. Detailed permissions for web behavior control groups are shown in Table 8.

(9) CD/DVD Read and Write Control. CD-ROM or DVD-ROM is at present a standard device in information equipment. For ease of use, suppliers provide simple functions that

Table 5: Permissions for web browsing.

Control group	Roles		Communication monitoring technology
Wireless network management	Operations staff Marketing staff Project management staff Planning staff	Sales staff Text staff Media dissemination staff	Allowed to use the wireless network

Table 6: Permissions for USB device.

Control group	Roles		Communication monitoring technology
USB device management	Operations staff Marketing staff Project management staff Sales staff System development staff	Drawing staff Design staff Research staff Financial staff	USB device read/write/query permission control

Table 7: Permissions for P2P usage.

Control group	Roles		Communication monitoring technology
P2P usage control	Operations staff Human resource staff Administrative staff General staff Legal staff Marketing staff Planning staff Project management staff Sales staff Trade staff	System development staff Maintenance staff Logistics staff Drawing staff Design staff Text staff Media dissemination staff Research staff Financial staff	Block P2P related software

Table 8: Permissions for file transfer.

Control group	Roles		Communication monitoring technology
File transfer control (HTTP/FTP)	Operations staff Human resource staff Administrative staff General staff Legal staff Marketing staff Planning staff Project management staff Sales staff Trade staff	System development staff Maintenance staff Logistics staff Drawing staff Design staff Text staff Media dissemination staff Research staff Financial staff	File transfer block/record

Table 9: Permissions for CD/DVD read and write.

Control group	Roles		Communication monitoring technology
CD/DVD read and write control	Operations staff Marketing staff Project management staff Sales staff System development staff	Drawing staff Design staff Research staff Financial staff	CD/DVD rom read/write control

Table 10: Permissions for web browsing.

Control group	Roles		Communication monitoring technology
Cloud storage system control	Operations staff	System development staff	Block cloud service connections
	Human resource staff	Maintenance staff	
	Administrative staff	Logistics staff	
	General staff	Drawing staff	
	Legal staff	Design staff	
	Marketing staff	Text staff	
	Planning staff	Media dissemination staff	
	Project management staff	Research staff	
	Sales staff	Financial staff	
	Trade staff		

Table 11: Permissions for terminal data control.

Control group	Roles		Communication monitoring technology
Terminal data control	Operations staff	System development staff	Backup data of computer equipment
	Human resource staff	Maintenance staff	
	Administrative staff	Logistics staff	
	General staff	Drawing staff	
	Legal staff	Design staff	
	Marketing staff	Text staff	
	Planning staff	Media dissemination staff	
	Project management staff	Research staff	
	Sales staff	Financial staff	
	Trade staff		

burn data. Users drag files to the drive and the CD-RW/DVD-RW will burn the data directly. The capacity of a DVD disk is increasingly bigger and burn speeds are becoming faster. Therefore, the information security policy should specify that these devices should not be installed in information equipment. Detailed permissions for web behavior control groups are shown in Table 9.

(10) Cloud Storage System Control. With a significant leap forward in network bandwidth, a large number of cloud technologies have arisen. The most popular cloud service is cloud storage space. Operating systems on both PC and MAC provide cloud backup mechanisms. Cloud storage also has universal application. Detailed permissions for web behavior control groups are shown in Table 10.

(11) Terminal Management. Local data protection may be given according to user permissions based on authorized roles. There are several mechanisms, such as identification, directory privileges, and watermarks, applied in the terminal. Detailed permissions for terminal data control groups are shown in Table 11.

(12) Web Streaming Media Control. Web streaming media may lead to serious network bandwidth overload and can directly lead to loss of business productivity. Although some system administrators completely block any type of streaming media, extreme limits often lead to more users accessing a proxy server in order to bypass content security filtering control. The result of this can be an even greater security threat. Detailed permissions for web behavior control groups are shown in Table 12.

4. System Architecture and Discussion

This section, first, demonstrates the proposed model, which combines a context-aware role-based access control model with communication monitoring technology for enterprise information security management and, second, presents the system's architecture. Moreover, a relevant discussion between traditional management approaches and the proposed information security auditing system will be presented.

4.1. System Architecture. The research simulates an information security management system (ISMS), the system architecture of which is shown in Figure 4.

Most of the operation systems of information systems used in current enterprises involve Microsoft Windows Software. In order to manage user accounts and privileges effectively, system administrators usually adopt domain management in order to manage domain computers. When a domain user logs on, a domain account, that is, a user ID, is required. This study adopts a unique domain account with

Table 12: Permissions for web streaming media.

Control group	Roles		Communication monitoring technology
Web stream media control	Operations staff	System development staff	Setting usage time of stream media block/release
	Administrative staff	Maintenance staff	
	General staff	Text staff	
	Legal staff	Media dissemination staff	
	Marketing staff	Research staff	

Table 13: Comparisons between traditional ISMS and proposed ISMS.

Item	Approach	
	Traditional ISMS	Proposed ISMS
Management approach	Passive	Active
System management	More complicated	More convenient
Strictness of security	Loose	Strict
Permission management	Complex	Simple
Audit trail setting	To be set in different monitoring devices	Simply define needed control items as per roles
Licensed count of equipment	Unable to effectively control	Able to use limited number of licenses in required control

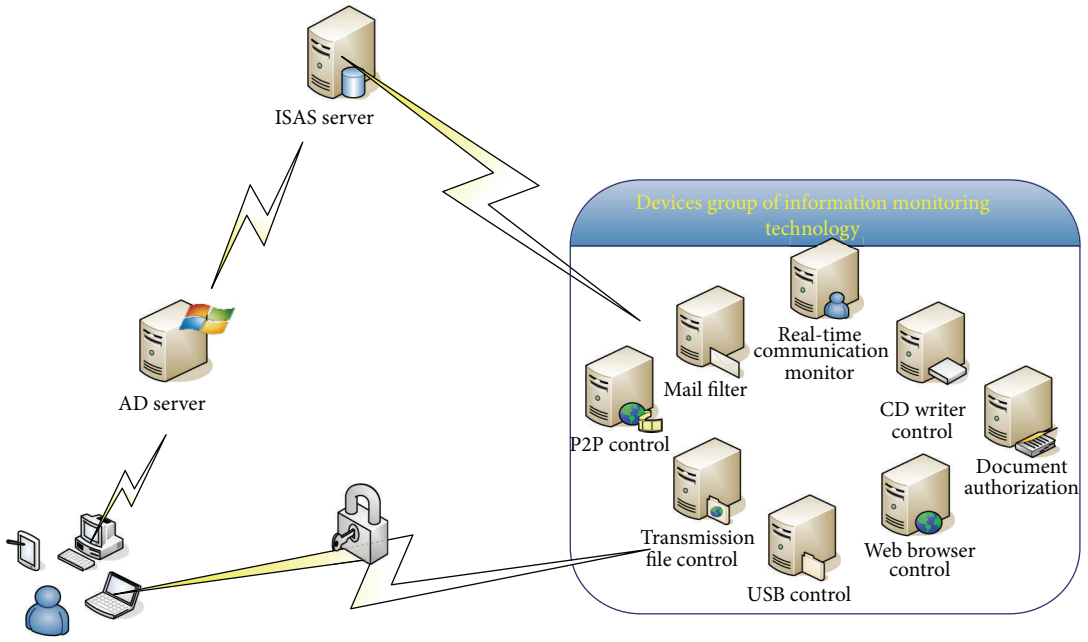

Figure 4: System architecture of enterprise ISMS.

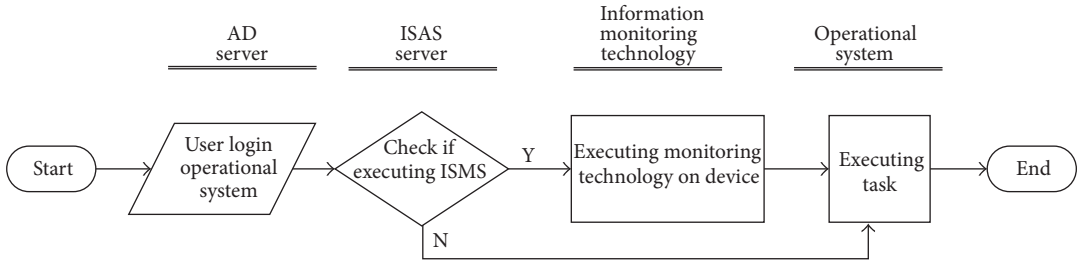

Figure 5: System flow of enterprise ISMS.

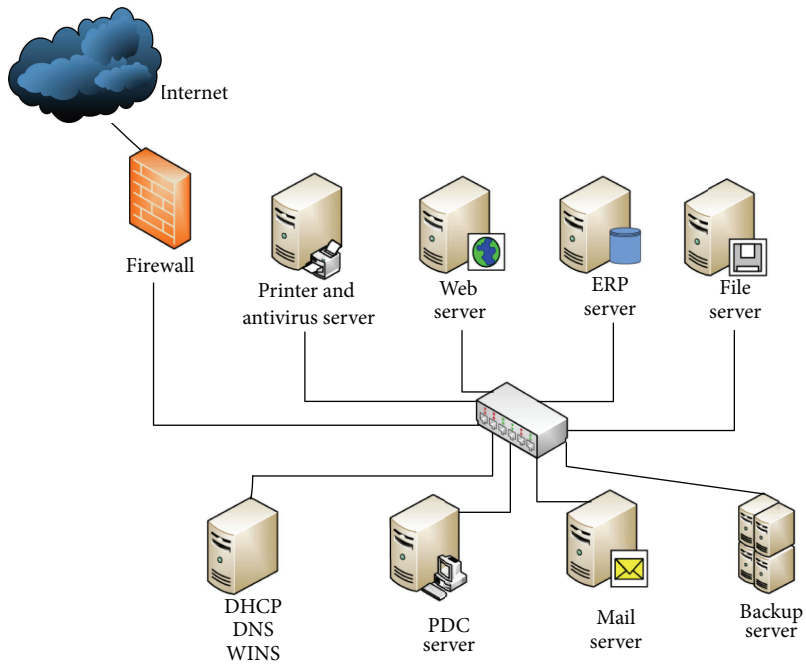

Figure 6: Network architecture of case company M.

group policy object (GPO) to the log in system. When a user logs on to the system from an active directory (AD) server, the proposed control model mentioned in Section 3 previously will determine the relevant permissions according to the current context information, information security policy, and communication monitoring technology. When a user is logging on to the system, the system will execute an authentication process in the information security auditing server (ISAS). The ISAS server will determine whether the user needs to process information security monitoring. The detailed system flow of enterprise ISMS is illustrated in Figure 5. In the proposed system, the system administrator does not need to define various security controls in several information pieces equipment nor define other permissions or audit trails. A user will not know that their behavior will be monitored and audited. For the system administrator, the proposed system can provide efficient information security management.

4.2. Related Discussion. Traditional information security management is passive. The system administrator must define different control rules for all information equipment in various systems. Typically, the system administrator spent a lot of time defining various permissions and auditing methods. However, given this, incorrect permissions settings or missing control items would often occur. For this reason, traditional information security management presented complicated work for system administrators. For example, the network architecture of case study of company M is illustrated in Figure 6.

Company M is a small and medium enterprise (SME) and only has one factory in Hsinchu Science Park in Taiwan. There are 80 PCs and 10 Servers in company M. The case company adopts "TrendMicro OfficeScan" as the antivirus software and "Scanmail For Exchange" for mail server. The security policy of case company is server control, antivirus software, and firewall. The security administrator defined various permissions and auditing methods on different servers. Besides, the company did not implement other policy, such as IM communication management, USB device management, and P2P usage control.

The proposed enterprise information security management system is a comprehensive framework based on context-aware RBAC and communication monitoring technology. Based on the characteristic of context-aware RBAC, the proposed enterprise information security management would significantly reduce the work load of system administrators. In place of the complicated work described previously, managers would confirm user-role assignments and the proposed system would automatically import the information security policy. Given that each role is assigned to certain control groups, the system would adopt, enforce, monitor, and audit the relevant communication monitoring technologies. Moreover, the monitoring equipment required for information security management can be purchased effectively and implemented in certain controlled roles. Other roles, which do not need to be monitored because they do not present a threat in terms of information leakage, would not require monitoring equipment. For this reason, an enterprise can reduce the cost spent on information security implementation and thereby reduce the load of system computing. Comparisons between traditional information security management approaches and the proposed approach are shown in Table 13.

5. Conclusion

With the progress of information technology, more and more systems, software, and technology are able to break through in the control of information security monitoring devices. Given this, a significant challenge for system administrators is the effective management of information equipment and assurance of all information assets in an enterprise. This research proposes a novel enterprise information security management model based on context-aware role-based access control and communication monitoring technology. According to the defined information security policy and implementing this policy with monitoring technology, enterprises will be able to effectively achieve information security management.

The planning of system architecture demonstrates the effectiveness of simply defining the needed control items based on roles. The main contributions of this work lie in its ability to reduce information security incidents, such as internal information leakage and reach the effective cost control of information systems. Furthermore, given that different organizations have different information security policies, objectively defining a complete information security policy allows for the implementation of the proposed model in various enterprises. Future research could take more information monitoring technologies into account.

References

[1] S. Besser, "Stopping information leaks: why traditional content filtering is no longer enough," White Paper of Portauthority Technologies, 2005.

[2] N. N. A. Molok, S. Chang, and A. Ahmad, "Information leakage through online social networking: opening the doorway for advanced persistence threats," in *Proceedings of the 8th Australian Information Security Management Conference*, pp. 70–80, 2010.

[3] D. Unal and M. U. Caglayan, "A formal role-based access control model for security policies in multi-domain mobile networks," *Computer Networks*, vol. 57, no. 1, pp. 330–350, 2013.

[4] D. F. Ferraiolo, J. Cugini, and R. Kuhn, "Role-Based Access Control (RBAC): features and motivations," in *Proceedings of 11th Annual Computer Security Application Conference*, pp. 241–248, IEEE Computer Society Press, 1995.

[5] D. F. Ferraiolo and R. Kuhn, "Role-based access control," in *Proceedings of 15th NIST-NCSC National Computer Security Conference*, pp. 554–563, 1992.

[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, "Computer role-based access control models," *IEEE Computer*, vol. 29, no. 2, pp. 38–47, 1996.

[7] R. Kissel, "Glossary of Key Information Security Terms," NIST IR 7298, Revision 1, 2011.

[8] ISO IEC 27001, Information technology—Security techniques—Information security management systems—Requirements, 2005.

[9] D. F. Ferraiolo, J. F. Barkley, and D. R. Kuhn, "A role based access control model and reference implementation within a corporate intranet," *ACM Transactions on Information and System Security*, vol. 1, no. 2, pp. 34–64, 1999.

[10] X. Huang, H. Wang, Z. Chen, and J. Lin, "A context, rule and role-based access control model in enterprise pervasive computing environment," in *Proceedings of the 1st International Symposium on Pervasive Computing and Applications (SPCA '06)*, pp. 497–502, August 2006.

[11] R. S. Sandhu, D. F. Ferraiolo, and D. R. Kuhn, "NIST model for role-based access control: towards a unified standard," in *Proceedings of the 5th ACM Workshop on Role-Based Access Control*, pp. 47–63, July 2000.

[12] A. Gupta, M. S. Kirkpatrick, and E. Bertino, "A formal proximity model for RBAC systems," in *Proceedings of the 8th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing*, October 2012.

[13] Z. Luo, N. Heilili, and Z. Lin, "A flexible applicable RBAC model and its administration," in *Proceedings of the 18th International Workshop on Database and Expert Systems Applications (DEXA '07)*, pp. 192–196, September 2007.

[14] E. Celikel, M. Kantarcioglu, B. Thuraisingham, and E. Bertino, "Managing Risks in RBAC Employed Distributed Environments," in *Proceedings of the OTM Confederated International Conferences CoopIS, DOA, ODBASE, GADA, and IS (OTM '07)*, vol. 4804 of *Lecture Notes in Computer Science*, pp. 1548–1566, 2007.

[15] A. K. Dey and G. D. Abowd, "Towards a better understanding of context and context-awareness," GVU Technical Report GITGVU-99-22, 1999.

[16] A. K. Dey, "Understanding and using context," *Journal of Personal and Ubiquitous Computing*, vol. 5, no. 1, pp. 4–7, 2001.

[17] N. Ryan, "Mobile Computing in a Fieldwork Environment: Metadata Elements," *Project working document*, version 0.2, 1997.

[18] Z. -Beika and K. Bernd, "A multi-context visual web page authoring tool," in *Proceedings of the 3rd Annual Communication Networks and Services Research Conference*, 2005.

[19] S. Bill and T. Marvin, "Disseminating active map information to mobile hosts," *IEEE Network*, vol. 8, no. 5, pp. 22–32, 1994.

[20] American Management Association, "2007 Electronic Monitoring & Surveillance Survey," 2008, http://press.amanet.org/press-releases/.

[21] S.-C. Chou, A.-F. Liu, and C.-J. Wu, "Preventing information leakage within workflows that execute among competing organizations," *Journal of Systems and Software*, vol. 75, no. 1-2, pp. 109–123, 2005.

[22] D. Y. Zhang, Y. Zeng, L. Wang, H. Li, and Y. Geng, "Modeling and evaluating information leakage caused by inferences in supply chains," *Computers in Industry*, vol. 62, no. 3, pp. 351–363, 2011.