CORPORATE SECURITY IMPLEMENTATION FOR MOBILE INFORMATION SYSTEMS

Tuncay ERCAN
Yasar University, Department of Computer Engineering
Universite cad. No:35-37 Bornova 35100-İzmir
E-mail: tuncay.ercan@yasar.edu.tr

Murat KOMESLI
Yasar University, Department of Software Engineering
Universite cad. No:35-37 Bornova 35100-İzmir
E-mail: murat.komesli@yasar.edu.tr

Ibrahim ZINCIR
Yasar University, Department of Computer Engineering
Universite cad. No:35-37 Bornova 35100-İzmir
E-mail: ibrahim.zincir@yasar.edu.tr

Abstract

Mobile Information Systems (ISs) have an important effect in organizations. They are not limited to the office, people can use mobile devices that they carry with them and access the network resources. They do not replace traditional information systems, but they are planned and designed with the unique features of wireless communication. With the increasing level of different information technologies, corporate level systems have the potential to change how business people efficiently work together. The need for a mobile user to have uninterrupted and secure access to information on the network should be considered and the necessary policies should be established for regular information flow in the organization. Our paper reviews the overall benefits of the mobile systems in the business since it has a critical value for the diversity of ISs. It also explains how mobility works and how organizations can extract maximum value from the mobile services in a secure way.

Key Words: *Mobile Information Systems, diversity, mobile devices.*

JEL Classification: D80, L86, L96, M15

1. INTRODUCTION

Mobile networking, mobile computing and wireless communications are the parts of today's current technology terminology that mean enabling different types of information at any time and place. Pervasive computing refers the same thing with the mobile computing concept which uses computers in a dynamic environment With the only exception of having wireless communications capability, devices used in mobile networking no matter they are owned by individuals or organizations, are personal portable devices like notebook computers, Personal digital assistants (PDAs), and smart phones. They may use different communications technologies like 3G, EDGE, Wi-Fi, Bluetooth, and dial-up services.

E-business is again today's major business innovation that most companies should have to adopt. Because, economic benefits of companies begin with a strong financial background, and maintain

with the necessary market share in their sector. Transaction and integration capabilities to improve production and management are mainly based on web based marketing which covers the big percentage of the technology trends. What we see in today's technological personal devices in our environment, they are all enriched with information processing capabilities. They have embedded processing and communications features for interaction and networking. Their additional capabilities with sensor technologies give them flexibility and responsiveness while communicating with their surrounding for mutual information share. While sensing is done through the hardware features and its evaluation of collected data is made through software processing, another type of software processing can be handled by software agents located and installed in the devices. If we think from the point of using these software agents in mobile devices, they can be renamed as mobile agents and travel from one mobile device to another with wireless transactions to run/monitor/audit their previously assigned functions.

Traditional network security measures do not cover the experienced problems mobile networking. The main changing threat is the dynamic environment of users' devices. Because many of the users are not able to keep their mobile devices up to date with antivirus programs, software patches or some other personal or corporate security features. Even they fail to follow the security policies requiring them to maintain what is mandatory. However, system administrators and network managers' biggest concern is to keep all mobile devices secure in place according to the corporate security policies.

In this study, we will focus on the corporate security implementations using content-based and trusted-based policies that become increasingly more important in recent years, in accordance with the appropriate technological infrastructure Here, the first factor we will face is the semantic approach since content-based applications are directly related with the semantic meaning of the shared data which is also the current content for the proper information. If we assume that many of the applications we used in mobile environments are mainly web-based and their related source files containing words and phrases, a content-based mechanism will always be useful.

The rest of the paper is organized as follows. We've reviewed and evaluated the current studies and tried to analyze uncovered or slightly covered issues in the next section. Section 3 explains the main differences between traditional and mobile security applications and describes why corporate mobile security policies are difficult to handle. In section 4, we propose an applicable model by improving content-based and policy-based approaches through our practical experience and knowledge in developing networking solutions. The paper concludes with a summary of the results and suggestions for future research.

2. LITERATURE REVIEW

Since mobile networking and computing tools have been increasingly used in the last decade, many of the features and standards in personal and corporate use must be identified. Considerable research on how companies benefit mobility in their business activities and how mobile devices securely execute different applications and what the right mix of current technology in the security of mobile networking are summarized with the following topics.

- Business benefits of mobile devices and a spectrum of mobile usages
- Different methods of user applications
- How to secure mobile networking

- Mobile agents and security with mobile agents
- Context-based and policy-based approaches

March et al (2000) addressed the challenges of globalization, interactivity, high productivity, and rapid adaptation in heterogeneous and distributed environments. They focused on three major capabilities such as Mobile Computing, Intelligent Agents, and Net-Centric Computing. The adoption of mobile technologies by the companies follows a technology-driven approach without knowing the potential benefits of these systems. Especially in larger an organization with complex business processes, a systematic procedure is required if a verifiable economic benefit is to be created by the use of mobile technologies. Kohler and Gruhn (2004) defined and introduced a similar procedure for this systematical analysis of the distributed use of mobile technologies. They both redesigned of the business processes and the requirements engineering of mobile information systems. Thurnher (2007) identified major business metrics which are influenced by mobile tool integration into mobile business processes.

Some of the authors (Barnes et al, 2006; Du et al, 2006; Apostolos et al, 2007; Bulander, 2008) investigated the impact of wireless and mobile networking on field force automation (FFA) in trade services organizations, Mobile Interactive Learning System (MILS) project, financial systems and Customer Relation Management (CRM) projects respectively.

Gebauer and Shaw (2004) assessed success factors of mobile business applications in different user groups. They found that functional mobile applications complemented existing information systems to design and manage different business applications. Schierholz et al (2006) aimed at providing different service levels to different customer groups especially in mobile contexts where mobile communications were widely used. The authors addressed some research questions on 1) How can the customer base be segmented for different mobile service levels? 2) Which characteristics qualify mobile services for service level differentiation? 3) How can mobile services be designed for service level differentiation? Holzinger et al (2008) provided an overview about the design, development and implementation of mobile applications within the clinical domain because of the problems with software applications, user interface designs and back end development (software engineering) to decide for the most optimum development path and to select the most appropriate environments.

Ivancic et al (2003) described a conceptual architecture for wide-scale deployment of secure mobile networking in operational environments. They explained some infrastructural issues such as link costs, placement of encryption engines and running routing protocols. Raghunathan et al (2003) presented an introduction to security concerns in mobile appliances for system architects, HW engineers, and SW developers. They also highlighted recent innovations and emerging commercial technologies. Schwiderski-Grosche et al (2004) discussed particular problems involved in securing mobile environments and established a series of requirements for the mobile infrastructures. Kappes et al (2004) presented new security challenges for the networks of mobile users. They discussed that future threats to the network would come from inside the network; specifically, from legitimate devices and users that roam and reconnect to the enterprise. Therefore, they worked on to authenticate the content of a device instead authenticating the user or mobile device. They expected that this approach should have been in line with the enterprise's security policies. Gallery et al (2004) worked on the secure download of content protection software, Bonnefoi et al (2005) focused on the security of mobile ad hoc networks by using smart

cards. Borselius et al (2002) provided a detailed security architecture and a specification of security services for particular agent applications.

Mobile Agents (MAs) are able to support distributed applications in open and heterogeneous environments. However, they lack of dispensable security mechanism. Hu et al (2005) proposed a solution for protecting the data from malicious behavior of execution sites for the integrity of the collected data especially in the situation that MA moves into an untrustworthy host or environment. Bernardos et al (2008) identified some descriptors such as personal, physical or activity related features for context-aware applications. The features of these descriptors have been evaluated for specific services resulting automatically perceived applications due to their functionalities, location aware services and mobile social networks.

3. MOBILE NETWORKING SECURITY

Mobile service providers look for necessary developments to their 2G and 3G cellular systems. With significant technological improvements and enabling new services, they provide substantial technological and economic benefits to customers. Powerful mobile solutions (Cellular and Wi-Fi) can connect employees directly into the office network while working offsite. Apart from necessary security features, most of the mobile devices have improved specifications that provide robust configuration parameters and applications to enable different security options (Fang et al, 2005).

3.1. Corporate policies

We should first look at where mobile devices may be used in our business and what new opportunities may lead. On the other hand, the increased flexibility in the work environment makes employees to train themselves for necessary skills and understand the security issues. Corporate policy begins with the definition of business models, components, classifications and of course the descriptive frameworks. The goal is the integration of them and the added values in different business models. Every organization should have their written policy which is brief, easy to read, feasible to implement and effective. So that, all of employees participate that they can communicate well and rules of specific requirements are met. Corporate security policy is a collection of system specific and functional requirements and assumes the rules below:

- Mobile devices belong to the organization,
- Mobile software is loaded by System administrators,
- Centralized management tools are necessary,
- Authentication methods should be carefully selected among the alternatives,
- Hardware and software security tools installed,
- Connect only to the authorized networks.

3.2. Mobility need and mobile business applications

Mobile Information Systems are decomposed in three main portions, hardware, software and communications. Mobile applications can support handheld devices owned by the employees. They provide availability and ease of use for out-of-office users. They can support offline and online (internet connected) scenarios. They provide better responsiveness, rich functionality and

improved user experience. It is nice to have mobile networking equipment for the ability to download business data, access and retrieve corporate information, and communicate anytime from anywhere. Mobility becomes important to many customer facilities like enterprises, government agencies, and service providers due to its success to reduce operational expenses.

3.4. Mobile Device Diversity

Different levels of mobility provide different degrees of flexibility and extendibility of the information. Support of multiple platforms, multiple programming languages and business processes is a business necessity. Differences in the business partners and technologies should have the common interoperable standards. Diversity also brings some critical design issues while deciding for a complete description and balancing the management tradeoffs to determine the corporate security policies. Table 1 shows some examples of design challenges and necessary actions taken how to balance them.

Table 1: Design challenges for mobile diversity

Design issues	Problems	Tradeoffs
Employees' profiles	How to define	User and customer access
Overall mobility benefit	Real value for end	Technological possibilities and user
Customer satisfaction	Usage of the service	Ease of use and abuse
Mobile device brands	Maintenance	Service provider and device seller
Trust	To whom	Security and privacy
Security	Secure access	Ease of use and privacy
Pricing	Budget	Quality of service and budget shortage
System Integration	How to integrate new	Flexibility and cost

4. PROPOSED SECURITY INFRASTRUCTURE

While dealing with the corporate uses of mobile devices, the main issue is to take care of rich variety in application domains. If we select an application from the necessary service offerings, there should be a predetermined context-based description for mobile services in the business model. Corporate users query the semantic agents to build a request in the server. For this reason we need to establish a services ontology that will provide an indexing mechanism for the corporate systems' data and content. In order to ensure optimal security solutions specifying adaptable security implementation, there are five key components to mobile corporate policy: *business environment, corporate policies, business applications, mobility* and *security* as seen in Figure1.

Corporate policies should need to be written and distributed for organization's practices in order to put them into action after each have been customized to the needs of our organization. Context-based semantic approach senses and adapts the users' context, application capabilities and preferences to deliver reliability over the network. Maintaining the users' personalized interface means that communications content are felt and necessary changes are done. Context is related with the well defined business service semantics called as corporate ontology; therefore all the transitions from one user to the corporate servers are pattern based.

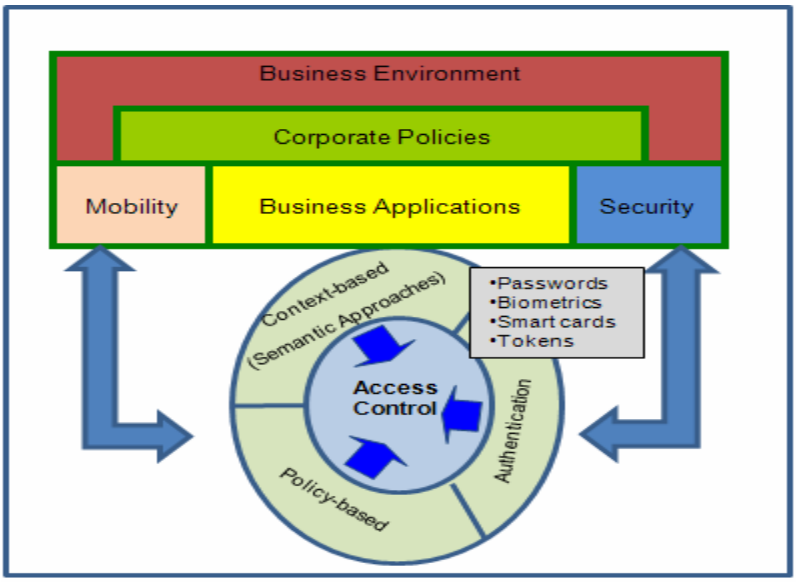

Figure-1: Overall Mobile Security Infrastructure

This provides contextually constrained business security composition. The difficulty is addressing different sets of complex corporate requirements such as existing infrastructure, business workflows, market performance, scalability and security. Authentication factors like passwords, biometrics, smart cards and tokens are fundamental security functions. They are presented by an individual and validated with the person's identity in the authorization servers. This is typically done for the purpose of granting or denying authorization to access secured files or applications.

5. CONCLUSION

Mobile IT devices change the way you do business since they all lead to new ways of working. This study explains how your organization can benefit from mobile computing and introduces the key security applications. Organizations need to take proactive look not just at the technologies of mobile networking and computing, but also the policies regarding their use. Since there are so many diverse technological systems that work for business benefits, there is no suitable recipe for developing successful business models.

It is necessary to define some parameters for corporate policies and security professional should be focused on what measures or controls to put into operation. Regardless of the application, predetermined context-based and policy-based constraints establish the limits of operation. This type of security feature will provide a higher level security and integration across multiple heterogeneous environments (different companies). System administrators maintain the local database where the semantic ontology has been built. They check the names of the service agents and inform the customers of the availability or unavailability of the required service. Enabling relationships between different companies, improved user experience and better corporate policy enforcement to improve security are very important. Using certificates for data integrity and

enabling cryptographic applications for confidentiality is a higher level request and determined by the policy.

The problems of which programs accessed over the Internet and different applications no matter who requested them will be run are determined by the corporate policies using content-based and semantic ontology approaches. Determining the differences between users and certain attributes are executed by trusted policy-based and attribute-based applications.

BIBLIOGRAPHY

Apostolos, K., George, P., & Theodore, A. (2007), Mobile financial services: A scenario-driven requirements analysis.

Barnes, S. J., Scornavacca, E., & Innes, D. (2006). "Understanding wireless field force automation in trade services", *Industrial Management & Data Systems,* 106(1-2), pp.172-181.

Bernardos, A. M., Marcos, D., & Casar, J. R. (2008). An analysis of context-awareness in commercial mobile services.

Bonnefoi, P. F., Poulingeas, P., & Sauveron, D. (2005). MADNESS: A framework proposal for securing work in ad hoe networks.

Borselius, N., Hur, N., Kaprynski, M., Mitchell, C. J., & IEEE. (2002). "A security architecture for agent-based mobile systems", T*hird International Conference on 3G Mobile Communication Technologies,* pp. 312-318.

Bulander, R. (2008). A research model of Customer Relationship Management systems for mobile devices - Description of a research model about Customer Relationship Management projects.

Du, H. S., Hao, J. X., Kwok, R. C. W., Wagner, C., & Pacis. (2006). Can Lean Media Enhance Large Group Learning? An Empirical Investigation of Mobile Information and Communication Technology.

Fang, X. W., Chan, S., Brzezinski, J., & Xu, S. (2005). Moderating effects of task type on wireless technology acceptance. *Journal of Management Information Systems,* 22(3), 123-157.

Gallery, E., Tomlinson, A., & IEEE Comp, S. O. C. (2004). Conditional access in mobile systems: Securing the application.

Gebauer, J., & Shaw, M. J. (2004). "Success factors and impacts of mobile business applications: Results from a mobile e-procurement study", *International Journal of Electronic Commerce*, 8(3), 19-41.

Holzinger, A., Holler, M., Bloice, M., & Urlesberger, B. (2008). Typical problems with developing mobile applications for health care - Some lessons learned from developing user-centered mobile applications in a hospital environment.

Hu, J. L., Wang, J. Z., Liu, A. Z., & Peng, D. Y. (2005). Solution for securing data integrity in the mobile agent system.

Ivancic, W. D., Shell, D., & IEEE, I. (2003). Securing mobile networks in an operational setting.

Kappes, M., Krishnan, P., & IEEE. (2004), "Content authentication in enterprises for mobile devices", *2004 IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication,* pp. 127-129.

Kohler, A., & Gruhn, V. (2004), "Analysis of mobile business processes for the design of mobile information systems", In K. Bauknecht, M. Bichler & B. Proll (Eds.), *E-Commerce and Web Technologies,* Vol. 3182, pp. 238-247.

March, S., Hevner, A., & Ram, S. (2000), "Research commentary: An agenda for information technology research in heterogeneous and distributed environments", *Information Systems Research,* 11(4), 327-341.

Raghunathan, A., Ravi, S., Hattangady, S., Quisquater, J. J., & IEEE Computer Society, I. C. S. I. C. S. (2003), "Securing mobile appliances: New challenges for the system designer"

Schierholz, R., Glissmann, S., Kolbe, L. M., Brenner, W., & Pacis. (2006), Mobile Systems for Customer Service Differentiation the Case of Lufthansa.

Schwiderski-Grosche, S., Tomlinson, A., Goo, S. K., Irvine, J. M., & IEEE. (2004), Security challenges in the personal distributed environment.

Thurnher, B. (2007). The impact of mobile technology on business processes - Results from 5 case studies.