A Security Framework Model for Mobile Computing

Kun Gao, Lifeng Xi, Jifang Li
Computer Science and Information Technology College
Zhejiang Wanli University
No.8, South Qian Hu Road Ningbo 315100, Zhejiang
P.R.China

Abstract: - In this paper, we present a framework model for E-commerce. We divide the framework model into three layers, discuss the problem related to security respectively, and defined the key research issues in each layer. we present some basic security problem at first, then discuss security issues in mobile networks, propose a brief classification of applications finally. This model can led to the further investigation of E-commerce security.

Key-Words: - Mobile Computing, Mobile Network Security, Security Model, Mobile Payment

1 Introduction

Mobile computing are emerging rapidly as exciting new paradigms to provide computing and communication services all the time, everywhere. According to the traditional way, it must come to the terminal to do some work on it. All devices, including workstation, server, hardware device, etc., connected to each other via cable. But in mobile computing environment, the situation has changed [1][2][3]. It is necessary to make mobile device small enough so as to be easily carried. The features of M-commerce, mobility and applications software break the barriers of geography and time. Such computing style creates unique value added attributes [4][5][6].

In the area of mobile computing, there is one problem that can not be avoided, that is the security issue. This problem is mainly due to the characteristics of application environment and requirement background in mobile computing [7]:

1. The cause of the security issues is caused by the characteristics of mobility and communication, for example high error rate and irregular behaviors;
2. Because the wireless signal is easy to be intercepted and captured, the hacker can have more chances to implement the hostile attack;
3. The application of mobile payment system will be more and more popular. Because of involving the commerce security problem, so the issue of the mobile payment is particularly important.
4. Mobile service may let out the individual privacy of customers;

Because of analysis described above, the traditional security mechanism is not suitable for the demand of mobile computing. A lot research has been concentrated on user authentication and data encryption, but security of mobile computing is not only involving these limited parts. We really need a more orderly method to accelerate to the study on mobile computing security.

In this paper, we present a framework model for the architecture research of mobile computing security. The study on mobile computing security in this framework model is partitioned into three different layers: Property Theory, Limited Targets, and Classified Applications. In each layer, we discuss main research issues in detail. The rest of this paper is organized as follows. In Section 2, we present some basic issues related to mobile computing security. We propose the mobile computing security model Section 3. Section 4 mainly discusses the key study issues in the framework model. Finally, we conclude this paper in Section 5.

2 Basic Issues Related to Mobile Computing Security

Regarding the issues of mobile computing security, we focus our attention on three respects, i.e., network architecture, network node and data processing. In fact, several respects described above are a simple abstract to mobile computing system, so we need to consider their background respectively.

The research of the network architecture can be divided into two category, i.e., infrastructure and protocol. Regarding infrastructures, the general classification is to divide into wireless(mobile network) and wired; As to protocol, the Open System Interconnection reference model is the theoretic concept, while the TCP/IP reference model is a standard in fact.

We focus our attention on main security issues for the aim of computation. The unified management that the data are collected has played an important role in network application, especially some data base management systems such as object-oriented database, multimedia database, parallel database, workflow database, active database and so on. Mobile computing gives full play to their potential ability in network application. Java has become one of the most important programming languages in the operation of this form. In addition, Grid technology has drawn common concern of people on the function in mobile computing.

3 MOBILE SECURITY MODEL for MOBIEL COMPUTING

The framework model that we propose is consist of three sections, that is, nature attribute layer, bounded goal layer, detailed application layer.

3.1 Nature Attribute

In the Nature Attribute section, what we discuss is some basic problem regarding the information security. And it is suitable for other two layers of this model.

- Target for security. It defined the safe goal that we want to make finally.
- Intrusion Detection. It offers the detection method for all goals that should be protected.
- Protection method. It can take precautions against and dissolve the risk of secutity in the mobile environment.
- Administration and maintenance. It defines and process the rule and strategy for mobile security.
- Estimation. It appraises the fragile key part and appraises, interfere with performance, personal secrets and stability and testing the inspections of the tactics and basic assessment determined.

3.2 Bounded Goal

On the basis of analysis to the restriction in mobile computing environment, we get the bounded goal layer as research area for mobile computing. It is the most important section in whole model framework that we proposed.

- Network. Include some network architecture and various relevant safety protocols, such as SSL,SET,NETBILL and so on.
- Computing. It mainly relates to mobile code and operating system.
- Data. It involves two respects, content and copyright. Data is considered for safe protection while transmitting and dealing with.

3.3 Detailed application

On the top layer, some applications are sorted out. Those applications must obtain support of security through network, computing and data processing. In these applications, though some are relatively independent, some is overlay in detail environment.

- Electronic messaging. Such as general electronic message, E-mail and Facsimile Amplitude modulation mode.
- Telephone. Such as Voice over Internet Protocol, Audio conference and IP Telephony, etc.
- Remote services. Such as Remote Diagnosis, Remote Consultation, Telecare, Distance Learning and Remote Medical Information Services, etc.
- Commerce. E-Commerce and E-business are typical representative of this kind of application.

4 Model Description

In this section, we describes the model in detail on every layer

4.1 Nature Attribute

We pay close attention to the technical field of security further, but in fact, safety management and estimation are equally important.

4.1.1 Target for Security

Into the bargain, the following three safe goals on the data will be reached:

Secrecy. An authorized account has authority of using the data.

- Wholeness. The rival can't revise the data in transmitting.
- Accessibility. The authorized account always has the authority of access to the data.

- Secrecy. Authorized account has authority of using the data.

4.1.2 Classification of Attacks

- Invade direction: outside and inside.
- Invade source: the person with evil intentions or without sense of responsibility.
- Invade goal: network device, database, password file and so on.
- Invade method: brute-force attack, trojan horse and remote control

4.1.3 Protection method

We can't enumerate all, because there are many kinds of protection methods.

- Means: we can protect the data using the methods of access, fire wall and security protocol, etc.
- Encrypt algorithm: cryptography, infrastructure of public & secret key and encrypt algorithm.
- Certification: personal identification number, weak or strong verification, and the intelligent card, etc.
- Monitor and control: intrusion detection, descry and supervisor.

4.2 Bounded Goal

4.2.1 Network

In previous generation's mobile network, the seacurity problem of mobile computing is unsatisfactory. The main shortcoming is related to authentication , repudiation and protocal. In the next generation wireless networks, more comprehensive examination will be considered, including wireless interface, mobile device association,mobile ad hoc networks and so on. Especially Wireless LAN, PAN and micro-cellular will be paid attention to.

The study on protocols mainly concentrates on ip protocol. The following ranges will also be developed: encrypting, registing and authenticating.

4.2.2 Computing

“Moving code”is an emerging computing technology and has been applied to various applications extensively. An agent can imagine it is a autonomy code. This code can start and take action, build the plan of taking action, form its own goal to the incident suitable, react the itinerary which plans, contact other agents, collect information,etc. It can sent the pieces of code to a remote host and withdrawn the results from the remote host.. When systematic resources are busy, an agent can dismiss, resume its action after being permitted. An agent can be send to others system and can be retracted to its origin location. It can be copied to process an action in parallel in a systems to enhance the whole performance. Finally, after stopping all its tasks, it can be arranged to leave. An agent can be classified based on the task type it is assigned. It can be able to migrate from one system to another, work with other agents in a system towards a common goal, communicate with other agents to gather information, or exhibit several other behaviors. There are two kinds of security mechanisms in agent environment, as follows:

- Agent Protection. The encrypted channel prevent the embedding of any untrusted third party intimidation to agents. As a part of the agreement, before they are sent, the host is demanded to sign on the agent's persistent state. This help during the course of analyzing, find that leads to the abnormal position of an agent's state.
- Host Protection. The special-purpose resources of the host computer are prevented from corruption and dealt with through Akenti by mistake. In order to confirm their ability, believe the agent, the appropriate access that Akenti carries out every one controls the decision.

4.2.3 Data

The advantage of the digital data has already led to the media of different digitization has been published through Internet and spread extensively, but unrestricted repetition and limitless replication brought the lost possibility at the same time. There are some methods, data encrypting and hiding information, to protect the author's intellectual property right.

A typical application with hidden information is a watermark. Watermarking is a special kind of encryption technolgy. A watermark often includes relevant datum origins and the information of the position or destination. This kind of method can be applied to very wide field, for example, text materials, image, video or audio data, fingerprinting and data authentication as well as embedded data labelling, etc. The stability of the watermark is a very important research direction.

4.3 Detailed Application

We introduce mobile E-business to present security issues for mobile computing in the detailed application layer. The mobile e-business is chosen as a case, because it may become one of the most promising applications of mobile computing.

Though the security question in mobile e-business is numerous, we can map these questions to three 3 goals which have been described in section 3.

In order to obtain the security, the mobile computing is also strict to the mobile device terminal, such as authentications of customer & merchandiser, functions of public key and private key, and so on.

5 Conclusion

In this paper, we propose a common security framework model for mobile computing. The model is consisting of three layers, and key research issues in each layer are defined. This model can led to the further investigation of mobile computing security.

References:

[1] Lassila, O., Adler, M.: Semantic Gadgets: Ubiquitous Computing Meets the Semantic Web. In Fensel, D., Hendler, J., Wahlster, W., Lieberman, H., eds.: Spinning the Semantic Web. MIT Press, 2003

[2] McGrath, R.E., Ranganathan, A., Campbell, R.H., Mickunas, M.D.: Use of Ontologies in Pervasive Computing Environments. Technical report, University of Illinois at Urbana-Champaign, 2003

[3] P. Rigole, Y. Berbers, and T. Holvoet. Mobile adaptive tasks guided by resource contracts. In the 2nd Workshop on Middleware for Pervasive and Ad-Hoc Computing, pages 117–120, Toronto, Ontario, Canada, October 2004.

[4] Y. Vandewoude and Y. Berbers. Run-time evolution for embedded component-oriented systems. In B. Werner, editor, Proceedings of the International Conference on Software Maintenance, pages 242–245, Canada, IEEE Computer Society, October 2002.

[5] A. Herzberg. Payments and banking with mobile personal devices. Communications of the ACM, 46(5):53–58, 2003.

[6] Niina Mallat, Matti Rossi, and Virpi Kristiina Tuunainen. Mobile banking services. Communication of the ACM, 47(5):42–46, 2004.

[7] K. Poutsttchi. Conditions for acceptance and usage of mobile payment procedures. In The Second International Conference on Mobile Business, pages 201–210. Giaglis, G.M. and Werthner, H. and Tschammer, V. and Froeschl, K.A. (Hrsg.), Wien 2003.