Volume 1, No. 4, Nov-Dec 2010

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Dynamic user Dependent Security Policy Framework for Mobile Commerce Applications

V. Shanmugasundaram*
Asst. Prof., Dept. of MCA,
J.J. College of Engg. & Technology,
Tiruchirappalli - 620 009
Tamilnadu, India
ss7433@gmail.com

M. Jawahar
Asst. Prof., Dept. of MCA,
J.J. College of Engg. & Technology,
Tiruchirappalli - 620 009.
Tamilnadu, India
mjawahar2009@gmail.com

Abstract: Mobile-commerce is the ability to perform commercial transactions using mobile phones or other wireless devices on the move. It is a major application domain for mobile devices where applications require a high level of security. Generally, either server operating system or application authority for the specific user about its behavior to access the applications after authentication enforces security policies. In this proposed framework, users submit their policy through its mobile device to the policy server (PS) after preliminary authentication assigned by the application authority. The trust of user device is analyzed using authentication protocol in addition to the feasibility of user submitted policy to the application. The levels of security are also changed depending on the user type accessing the applications. User types are identified using the ip addresses that are stored in the database on the server side. User can change its policy any time from its location as well as increases its levels of security after mutual concern from the application authority. In this paper, user policy submission protocol is developed for the m-commerce applications.

Keywords: M-Commerce, Security, Authentication, Policy Server, Protocol, Repudiation

I. INTRODUCTION

M-Commerce has been growing rapidly in the recent years with the development of the mobile communications and e-business. Mobile e-commerce is the ability to perform commercial transactions from mobile phones or other wireless device on the move [4].

It is a major application domain for mobile devices where applications require a high level of security. The two main areas of m-commerce that are relevant to security namely network technology and m-payment [1]. Each mobile device has certain characteristics that influence its usability such as size and color of display, memory and CPU, network connectivity, bandwidth capacity and support Operating System. There are different security challenges depending on the point of view of the different particular participants in m-commerce scenario. These challenges related to the mobile device, the radio interface, the network operator infrastructure and the kind of m-commerce application [3]. The confidential data on the user accessed mobile device should also be protected from unauthorized use using security mechanisms such as user authentication [PIN or password], secure storage of confidential data and security of the Operating System. Generally, Security policies are enforced by either Server OS or Administrator [5].

A security policy is a formal statement of the rules through which users privileges can be measured with respect to technology, information assets and access to the system [2]. It is an effective and comprehensive program, which provides feasible, understandable, realistic, consistent procedural tolerable and provides reasonable protection relative to the goals and objectives of an application for developing security architecture. The security policies developed must establish a consistent notation of what is and what is not permitted with respect to control access to the data and processing resources. A new framework is designed in which user can submit its security policy as its demand from anywhere and any time using mobile device. Policy is updated for the specific user after authorization from the policy server. Policy Server is one, which contains the security policy of each user. Initially, security policy or default policy is assigned for each user by the application authority. In this paper, user assigned security framework, its simulation and feasibilities are discussed.

II. MATERIALS AND METHODS

A. Framework for M-Commerce

The fundamental requirement for m-commerce is secure environment for transaction but there are different security challenges depending on different participants in m-commerce circumstances. The new security framework provides legal environment within which users can confidently perform commercial transactions. The proposed framework integrates several existing security techniques in order to achieve enhanced secure transactions for mobile applications. The proposed framework architecture for m-commerce applications is shown in Figure 1. At the beginning, user received USERNAME and PASSWORD from the application authority. In each admissible range of transmission, there is one Authenticated Server (AS). AS check the validity of the user-accessing device with the application. User can submit its security policy to the AS in its admissible range. After authentication of user accessing device, submitted policy is

forwarded to the PS. PS collects the history of the user from other ASs, update the policy to that specific user and inform through message to the user. Users can increases their levels of security depends on its category.

The format of the user submitted policy is as shown in Figure 2.The application authority assigns distinguished *User Name* to the each user at the beginning. The *Context* is the list of location from where the user accessed the *application*. *Authenticated-ID* is assigned by the AS in connection with validation of the user-accessing device. This ID is an unbroken one-time pad encrypted type key. *Level-ID* specifies the security level, which is a number. The level of security depends on the user category. The mobile number that is stored in the database at the server side determines the user category. *History* tells about the user previous footprint in the accessed authenticated servers say *context*.

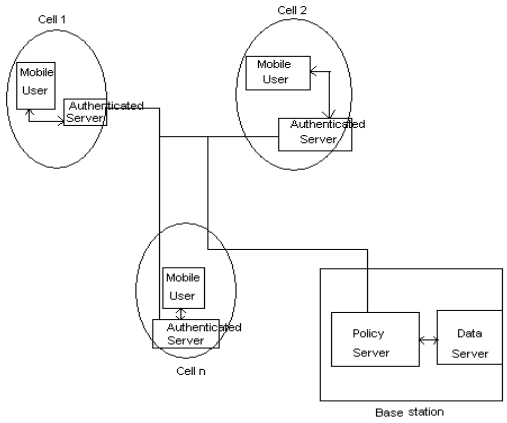

Figure 1: Framework architecture for M-Commerce applications

At the beginning, it is *Nil*. The previously accessed authenticated servers assign it. *Passwd* is the assigned by the application authority. The challenges in the proposed framework are outlined

User name	Context	Authentic ated – ID	Level -ID	History	Passwd
2 Byte	3 Byte	2 Byte	1 Byte	6 Byte	2 Byte

Figure 2: Format of User submit policy

[a] Protocol which authenticates the user accessing device involving AS and user.
[b] Developing communication protocol between ASs and PS.
[c] User level categories, identifying the levels of security to the user.

B. Security of the Protocol

The following subsections justify the protocol, which satisfies the general security requirement.

Confidentiality: This is achieved by encrypting the message using a symmetric secret one-time password. This password is shared between the ASs and user. The strength of the confidentiality depends on the security strengths of the password-generating algorithm used and the strength of the ciphering algorithm used.

Integrity: The message digest is the hashed value of the message content calculated by the server and client application. If the content is altered during transmission, the hash algorithm will generate different digest value at the receiving side. If the digest value is mismatch, the receiver knows the integrity of the message has been compromised.

Authentication: The authentication process is performed by validating the A*uthenticated- ID* when the users register for an account in the application.

Non-Repudiation: Only the account holder and the servers are supposed to have the one-time password. The servers do not generate the same one time password more than once. There fore, every time password is unique in the database server.

Availability: The availability of this protocol depends on the availability of the network. The time it takes for a message to be delivered depends on the density of the network operator base towers. The number of transactions that the server can handle at once depends on the hardware capability. The protocol has no restriction on the type of hardware needed.

III. EXPERIMENTAL RESULTS AND DISCUSSIONS

This work was carried out in small-scale client and server environment. Client side applications were running in Laptops. IP addresses of the Laptops were stored in the database at the server side for identifying the user category. Incoming requests are classified into either valuable or Non-valuable category. Valuable category requests are those having more than 2 lakhs in the account. Initially, application authority assigns policy for the user. Later, it is changed by the user itself depends on their category and its demand.

In this simulation, there is only one AS and PS. User submitted policy is received by the local AS. It is then forwarded to the PS after checking the trust of the user-accessing device. Policy is submitted in the form of text file. PS broadcasts *User Name* to all ASs and collects the previous footprints of the user for authentication.

The level of security depends on the user category. User security levels have been dynamically updated by the application. The level of security considered in this simulation namely *PASSWORD,* last transaction date and amount in the account etc. This work was implemented.

IV. CONCLUSION

In this paper, we introduce a user assigned security policy framework; discussed how the communication takes place between user, ASs and PS and feasibility of the proposed model.

V. REFRENCES

[1] Dominik Haneberg, Alexander kreibich, Wolfgang, "Design for Trust: Security in M-Commerce Applications", Proceedings of LIT, PP 24-28, 2003.

[2] Joel Weiss, Charles R. Martin, " Developing a security policy " available from http://www.sun.com/blueprints

[3] Li-sha he, Wing Shang "An asymmetric authentication protocol for m-commerce applications", Proceedings of the 8th International symposium on computers and communication (ISCC'03), pp 30-38, 2003.

[4] Woo young Kim, Akhil saha, "A secure platform for per-to-peer computer in the Internet" proceedings in the 35th Annual Hawaii International conference on system and communication.

[5] Kelvin choom, Ming ki chong, Alapan Arab, Andrew Hutchison, " Security of Mobile banking "Security of Mobile banking " , Proceedings of Fast software Encryption workshop, 2000.

[6] Mustafa A. Ally and Mark Toleman,"Towards a Theoretical Framework of Determinants for the Adoption Diffusion of Buyer Authenticated Credit Card Payment Programs: The Online Merchant's Perspective." Proceedings of the IEEE International Conference on E-Commerce Technology, 2004.

[7] Wagner D. and Schneider B., "Analysis of the SSL 3.0Protocol", The Second USENIX Workshop on Electronic Commerce Proceedings, pp.29-40, November 1996.

[8] Visa and MasterCard, Secure Electro nic Transaction (SET) Specification, Book2: Technical Specifications found at http://www.setco.org/download/set-bk1.pdf

[9] Hsiao-Cheng Yu, Kuo-Hua His and Pei-jen kuo,"Electronic payment systems: an analysis and comparison of types", Technology in Society, Vol.24, Issue 3, pp.331-347, August 2002.

[10] Andrea Bottoni and Gianluca Dini,"Improving authentication of remote card transactions with mobile personal trusted devices", Computer communication I press, corrected proof, available online, 16th February-2007.

[11] Wn-Sheng Juang,"D-cash:A flexible pre-paid e-cash scheme for date-attachment", Electronic Commerce Research an d Applications, Vol.6, Issue 1, pp.74-87, 2007.

[12] Tolone W., Ahn G-J, and Pai T., "Access Control in Collaborative Systems", ACM Computing Surveys, Vol.37, No.1, pp. 29-41, 2005.

[13] Lee Y.E., and Benbasat I., "A Framework for the study of Customer Interface Design for Mobile Commerce, 1086-4415/2004, Vol.8, No.3, pp.79-2, 2004.