Design and Simulation of Mobile Commerce Identity Authentication Protocol Based on OTP

Qin Wang, Beijing Union University, Beijing, China
Huifeng Li, School of Application and Science, Beijing Union University, Beijing, China

ABSTRACT

With popularization and development of mobile commerce, the security of mobile commerce has drawn more and more attentions. Identity authentication is the first safety barrier, as communication security almost starts from its handshake process. Authentication protocol based on cipher technology is the safest method to realize identity authentication, and therefore identity authentication protocol is necessary to ensure communication security in mobile commerce. Combined One-time password (OTP) with Elliptic Curve Cryptosystem (ECC), a mobile commerce identity authentication (MCIA) protocol is presented. The two procedures of user registration and bidirectional authentication are designed. In order to verify its operation efficiency in the actual network environment, the simulation model of MCIA is set up through Opnet. The MCIA performance is analyzed from the statistics variables, including scheme time, server queuing delay, channel utilization and throughput. The results verify that MCIA has better feasibility in mobile commerce environment.

Keywords: ECC, Identity authentication, MCIA, Mobile Commerce, Opnet, OTP

1. INTRODUCTION

Abroad, the research point about identity authentication in mobile commerce is mainly focused on Wireless Public Key Infrastructure (WPKI). Public-key encryption, open and standard technology are used to construct a trustable and secure architecture in WPKI (Karl Felder, 2004). It could provide all sorts of secure services based on WPKI architecture for mobile users, realize real peer to peer security in data transmission process, secure user identity authentication and trustable trade, protecting data transmission integrity and confidentiality, and realize non-repudiation of transaction participants, so as to establishment secure mobile commerce environment effectively. However a study claims that is higher computation ability...
for mobile terminals in WPKI authentication mechanism, and it isn’t suitable for mobile commerce environment with limited computation ability (Zhao, W., & Dai, Z., 2005). At the same time, it has disadvantages such as high expenditure, complicated technology, lack of unified standard and better interoperability, especially it has no legal and authoritative third authentication institution - Certification Authority (CA). Because of these factors, WPKI hasn’t had a better application for domestic mobile commerce environment.

Presently, identity authentication in domestic mobile commerce is mainly implemented by static password mechanism based on UserID (user name)/UserPW (user password). The mechanism has some advantages, such as easier implementation and simpler operation. But its security is only depended on secrecy of UserPW (Zhang, Z., 2004). Once UserPW is lost, its security is completely lost. One-Time Password (OTP) authentication mechanism has higher security by one time padding. It is implemented simply, it costs less and needs no third-party notarization, and therefore it is more suitable for mobile commerce environment, but it couldn’t resist decimal attack and realize bidirectional authentication (Ye, X.-J., & Wu, G.-X, 2002). The main reason is that random number is generated one time password and authentication information are transmitted by plaintext, hence cryptosystem is used to encrypting these above information. Public-key cryptosystem has the higher security intensity, and Elliptic Curve Cryptosystem (ECC) has the best security, the fastest speed and needs no third-party notarization among all the public-key cryptosystems (Xiao, Y., 2006). It has some characteristics, including smaller storage space and taking-up bandwidth, lower computational complexity and faster processing speed, and thus more suitable for mobile commerce.

Combined OTP mechanism with ECC, it is presented a mobile commerce identity authentication (MCIA) protocol based on OTP. Bidirectional authentication and key agreement are realized in the mechanism, and simultaneously decimal attack and man-in-middle attack are resisted effectively.

2. RELATIVE THEORY

2.1. OTP and Its Safety Analysis

OTP main authentication thought is that some uncertain factors are added in the login procedure and therefore digest password isn’t the same in the every login procedure, to improve the security of login procedure (Chen, L., 2008). OTP authentication procedure is shown in Figure 1.

In OTP, user’s password transmitted on network is used only once, thus preventing aggressors from accessing through stealing user’s password (Gao, X., Zhang, H.-G., & Sun, X.-M., 2006). OTP authentication is digest authentication (Sui, Z., 2005), which adds uncertain factors during the login course to make every time password different and so improving login security. After accepting the login password, Server adopts the same algorithm verifying user’s legitimacy.

OTP authentication mechanism has some characters:

1. OTP is implemented simply and more suitable for mobile terminal with relatively low computational capabilities.
2. OTP has the certain safety because it is produced by connection user’s own secret pass phase with challenged information (random seed and iterations) through a unidirectional function (Long, Y., Zhou, Z., & Liu, Q., 2006).
3. Because OTP doesn’t need the third-party notarization, it is particularly suited to mobile environment without the authoritative third-party notarization organizations and related laws.

Therefore, OTP is feasible to be used in immature mobile authentication environment. Although OTP has some advantages, it has some security risks:
Innovation Scope and the Performance of the Firm: Empirical Evidence from an Italian Wine Cluster
www.igi-global.com/chapter/innovation-scope-and-the-performance-of-the-firm/119751?camid=4v1a

Emergence of Familiness and Family Owned Business Performance: The Case of Myanmar
www.igi-global.com/article/emergence-of-familiness-and-family-owned-business-performance/233578?camid=4v1a