

Chapter 4.22

Security Issues and Possible Countermeasures for a Mobile Agent Based M-Commerce Application

Jyh-haw Yeh

Boise State University, USA

Wen-Chen Hu

University of North Dakota, USA

Chung-wei Lee

Auburn University, USA

ABSTRACT

With the advent of wireless and mobile networks, the Internet is rapidly evolving from a set of connected stationary machines to include mobile handheld devices. This creates new opportunities for customers to conduct business from any location at any time. However, the electronic commerce technologies currently

used cannot be applied directly since most were developed based on fixed, wired networks. As a result, a new research area, mobile commerce, is now being developed to supplement existing electronic commerce capabilities. This chapter discusses the security issues related to this new field, along with possible countermeasures, and introduces a mobile agent based solution for mobile commerce.

INTRODUCTION

The Internet has been steadily growing at a rapid speed since its commercialization. The fast and convenient characteristics of the Internet attract a wide variety of users all over the world. Because of its ability to reach more potential customers, the Internet is changing the nature of business from a traditional model based on face-to-face negotiations to a more advanced model utilizing electronic commerce (e-commerce). People all over the world can sell, buy and trade goods online as long as they can access the Internet. As a result of recent advances in wireless and mobile network technology, accessing the Internet has become even more convenient. Users can now access the Internet with a handheld device from any location at any time they choose. This wireless technology evolution further broadens the scope of business from e-commerce to mobile commerce (m-commerce). Most major companies have foreseen this and devoted a significant effort to developing new m-commerce systems to facilitate this trend. However, the migration from e-commerce to m-commerce is not as easy as it first appears because all the existing e-commerce technologies were developed for wired networks, which are more reliable, more secure and faster than wireless and mobile networks. Therefore, without major revisions the current e-commerce technologies cannot be applied directly to m-commerce. This chapter addresses this issue by discussing possible solutions based on the use of mobile agent technology to overcome the underlying hardware limitations of m-commerce.

In order to fully deploy m-commerce for business, there are two levels of security requirements that must be satisfied. The lower level requirement is the need for a secure wireless infrastructure to protect each individual wireless communication and the higher level requirement is for a secure protocol with which to conduct mobile payment and business transactions, thus protecting the legitimate security concerns of the three parties

involved, namely the customer, the merchant, and the bank. Wireless communication security is a serious problem for all wireless applications that must transmit data securely through an open airwave communication medium. IEEE 802.1x (IEEE, 2001) defines the standard for wireless authentication, key distribution, network monitoring, and similar issues. This standard uses EAP (Extensible Authentication Protocol) (Blunk & Vollbrecht, 1998) and its supported algorithms to authenticate exchanged messages. The algorithms supported by EAP are MD5 (Message Digest 5), TLS (Transport Layer Security) (Aboba & Simon, 1999; Dierks & Allen, 1999), TTLS (Tunneled TLS) (Funk & Blake-Wilson, 2002), LEAP (Lightweight EAP), and PEAP (Protected EAP) (Hakan, Josefsson, Zorn, Simon & Palekar, 2002). The security community has agreed that cryptography is the only solution to the problem of ensuring authenticity, privacy and integrity for communications through insecure media and many encryption algorithms have been developed over the past few decades. However, in a wireless environment with limited physical resources, most existing encryption algorithms are too computationally intensive. A lightweight encryption algorithm with an acceptable degree of security strength is a possible solution to this dilemma. Although the lower level security requirement, wireless communication security, is the topic of considerable ongoing research and is a vital preliminary to the deployment of all wireless applications, this chapter will instead focus on the higher level security requirement, mobile payment and transaction security.

A business transaction is likely to involve a secure negotiation made up of many back and forth messages. However, due to their limited bandwidth, mobile handheld devices cannot afford to receive and respond to those messages individually. To resolve this problem, the use of mobile software agent technology could provide a possible solution. The handheld device launches a smart mobile agent containing all the necessary

17 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/security-issues-possible-countermeasures-mobile/23220

Related Content

Paradise to Peril: Humanistic Uncertainty during Hurricanes Isaac and Katrina

Scheljert Denas (2013). *International Journal of Risk and Contingency Management* (pp. 67-70).

www.irma-international.org/article/paradise-peril-humanistic-uncertainty-during/76658

Re-Evaluation of On-Line Hot Topic Discovery Model

Hui-min Ye, Sushil K. Sharma and Huinan Xu (2009). *International Journal of Information Security and Privacy* (pp. 1-10).

www.irma-international.org/article/evaluation-line-hot-topic-discovery/3998

Wearable Devices and Privacy Concerns: Data Collection, Analysis, and Interpretation

Ersin Dincelli, Xin Zhou, Alper Yayla and Haadi Jafarian (2021). *Research Anthology on Privatizing and Securing Data* (pp. 208-230).

www.irma-international.org/chapter/wearable-devices-and-privacy-concerns/280175

Risk Management Research Design Ideologies, Strategies, Methods and Techniques

Kenneth David Strang (2013). *International Journal of Risk and Contingency Management* (pp. 1-26).

www.irma-international.org/article/risk-management-research-design-ideologies/77903

Planning for Hurricane Isaac using Probability Theory in a Linear Programming Model

Kenneth David Strang (2013). *International Journal of Risk and Contingency Management* (pp. 51-66).

www.irma-international.org/article/planning-hurricane-isaac-using-probability/76657