Chapter 7.13
Intrusion Detection and Vulnerability Analysis of Mobile Commerce Platform

Changhua Zhu
Xidian University, China

Changxing Pei
Xidian University, China

ABSTRACT

Intrusion detection and vulnerability analysis play the same important roles in wireless infrastructure as in wired infrastructure. In this chapter we briefly present the methods and technologies of intrusion detection and vulnerability analysis. Then we give the security issues in various wireless networking technologies, analyze the vulnerability of the enabling technologies for the mobile commerce platform, and propose a distributed wireless intrusion detection & vulnerability analysis (WID&VA) system that can help to address the identified security issues. Finally, we conclude this chapter and discuss the future trends.

INTRODUCTION

Combining with current wireless communications infrastructure, wireless computing infrastructure and mobile middleware, mobile commerce provides consumers with secure, faster and personalized services and is becoming one of the most important wireless applications. Mobile commerce is a vast area of activity comprised of transactions with monetary value conducted via a mobile device. These transactions may involve intangible goods, such as applications and information delivered to the mobile device in digital format, as well as tangible goods that are purchased using the mobile device but delivered separately. More and more people prefer m-commerce services and enjoy themselves by these prompt services.

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

On the other hand, compared with wired networks, wireless networks have no central control scheme and determinate boundary, which provide many chances for the intruders to attack the networks. Mobile data can be copied, sniffed, or lost. Wireless terminals and network platforms can also be deceived, and attacked passively (decryption) or actively (unauthorized communications).

Typical systems of wireless infrastructure for m-commerce platform include cellular networks (e.g., GSM), WLAN (wireless local area networks, e.g., IEEE 802.11), wireless MAN (metropolitan area networks, e.g., IEEE 802.16), HomeRF, WPAN (wireless personal area networks, e.g., Bluetooth) and the combination of them (e.g., GPRS (general packet radio service) /WLAN). In GSM circuit-switched data (CSD), GPRS and EDGE (enhanced data rates for global evolution), the A5 algorithm is applied to encrypt the radio link data and the A3/A8 algorithm is applied for the authentication. There exists a common weakness that has been reported that both A5 encryption algorithm and A3/A8 authentication algorithm can be easily broken. This means that the attacker can calculate the private key of a consumer and duplicate the SIM (subscriber identity module) card. In GSM, there is no authentication against networks, no end-to-end security scheme, and no explicit integrity protection on the air link. Barkan, Biham, and Keller (Barkan, Biham & Keller, 2003) from Technion Institute of Technology in Haifa (Israel) described a ciphertext-only attack on A5/2 that requires a few dozen milliseconds of encrypted off-the-air cellular conversation and finds the correct key in less than a second on a personal computer. They described new attacks on the protocols of networks that use A5/1, A5/3 or even GPRS. UMTS has explicit integrity protection on the air link, uses the publicly reviewed encryption algorithm (KASUMI), conducts the authentication between mobile terminal and network, and encrypts transmitted data within a base station. However, UMTS has not been widely implemented and will not be likely accepted worldwide in the near future. In addition, with the increasing capability of the intruders, new security weaknesses of wireless cellular networks may be discovered.

The wireless application protocol (WAP) offers additional and advanced layers of security, where wireless identity module (WIM) may carry asymmetric keys, certificates, and perform WTLS (wireless transport layer security) authentication and signature operations. The WAP has a special security layer, WTLS, in the WAP protocol stack, and it supports PKI (public key infrastructure). However, it is well known that decryption and re-encryption between WTLS and SSL/TLS (secure sockets layer/transport layer security) occur in the WAP gateway. This means that the data are exposed to intruders. The intruders can access private authorization information through packet sniffing (so-called WAP GAP).

WLAN is easy to be broken-in because the network must send beacon frame with information that can be used by hackers, and this provides necessary clues for intrusion. Intruders can penetrate into the WLAN anywhere by using high sensitivity antennas. Subscribers might be deceived by unauthorized APs (access points). Because of limited bandwidth, the resource of WLAN may be exhausted by non-authorized traffic, and APs can be blocked. This is a so-called DoS (denial of services) attack. Fluhrer, Mantin and Shamir analyze the weakness of RC4 stream cipher that is applied to traffic between wireless access points and stations by WEP (wired equivalent protocol) and declare that WEP can be cracked within 15 minutes (Fluhrer, Mantin & Shamir, 2001). On the other hand, WEP can merely protect the initial data of the subscriber and network. It cannot encrypt the supervision and control frames. Therefore, it provides chances of being deceived by fraud frames. In addition, many subscribers have not really implemented WEP although it is a default option in many WLAN products. This allows an intruder to easily puzzle the ARP table, to obtain the MAC address, to find the existence

15 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/intrusion-detection-vulnerability-analysis-mobile/9602

Related Content

Digital Rights Management for Mobile Multimedia
Sai Ho Kwok (2003). *Advances in Mobile Commerce Technologies (pp. 97-111).*
www.irma-international.org/chapter/digital-rights-management-mobile-multimedia/4874

The Affective and Cognitive Impacts of Perceived Touch on Online Customers' Intention to Return in the Web-based eCRM Environment
Hong-Mei Chen, Qimei Chenand Rick Kazman (2007). *Journal of Electronic Commerce in Organizations (pp. 69-91).*
www.irma-international.org/article/affective-cognitive-impacts-perceived-touch/3488

Opportunities and Challenges for B2B Manufacturing Firms: Moving from Products to Services-Case SKF
Esko Penttinenand Timo Saarinen (2008). *Electronic Commerce: Concepts, Methodologies, Tools, and Applications (pp. 1664-1671).*
www.irma-international.org/chapter/opportunities-challenges-b2b-manufacturing-firms/9576

Measurement of Grid Mobile Commerce Process Based on Users
Dan Chang, Xiaoling Jiand Yunfang Ma (2017). *Journal of Electronic Commerce in Organizations (pp. 24-38).*
www.irma-international.org/article/measurement-of-grid-mobile-commerce-process-based-on-users/188835

Delivering Superior Customer Perceived Value in the Context of Network Effects
Fan-Chen Tseng, Ching-I Tengand David M. Chiang (2008). *Electronic Commerce: Concepts, Methodologies, Tools, and Applications (pp. 1870-1880).*
www.irma-international.org/chapter/delivering-superior-customer-perceived-value/9592