Infrastructure-Based Protection of Unauthorized Access on M-Commerce

Theint Zarni Myint, Su Su Win
University of Computer Studies, Hinthada
chutpit@gmail.com; susuwin.most@gmail.com

Abstract

Recent technological innovations such as mobile computing have enabled new facility of buying and selling using mobile devices such as Laptops, PDAs mobile phones and other handheld devices which can support the wireless communication. Consequently, these devices will play an increasing role in M-Commerce (Mobile Commerce) technology. M-Commerce offers the possibility of an entire new level of financial flexibility, taking advantages of both social and technological developments. As M-Commerce platforms mature, grow in popularity and store valuable information, hackers are also stepping their evil efforts on these field. This paper focuses on security aspects to protect against threat of M-Commerce and since M-Commerce is based on infrastructure mode and all the important data are passed through on air medium, it has lots of vulnerabilities which can be a chance for an unauthorized user to attack the valuable data of M-Commerce. Therefore, this paper specifies how to care for the above aspects by using WPA (Wi-Fi Protected Access) protocol.

Keywords: WPA, wireless, threat, vulnerabilities, Mobile Commerce

1. Introduction

Mobile phone and other small and powerful portable gadgets have revolutionized personal communication and affected, considerably, the lifestyles of the people in the industrialized world. The trend in technology is such that small lightweight low complexity devices will become one of the predominant computing platforms. M-Commerce can be described as the act of performing an electronic transaction that has financial implications from a mobile device. The shift from physical payments to virtual payments has brought enormous benefits to consumers and merchants. In spite of getting the advantages from M-Commerce, security is a crucial requirement of an M-Commerce system on account of the fact that the sensitive information which travels over unreliable networks.

The concern about how to make M-Commerce secure go beyond the authentication processes, since a stolen or cracked password may gain authentication and access even if it is being used by an unauthorized one. In this paper, its design is for the book publisher who wants to improve his/her business and make an efficient way to access from the customers who are long time ago partners with this book publisher. All these long times ago partners are the pre-registered users for this system. WPA is applied for Mobile Purchase which is one of the services of M-Commerce. Whoever comes and asks the request to access the M-Commerce services, they have to pass through the WPA protected network. And the implementation of this system will be demonstrated about that how to protect the unauthorized access on M-Commerce by using WPA.

2. Related Work

Scarlet Schwiderski-Grosche [2] identified the special characteristic of M-Commerce and reflected on some important security issues. Ali Grami [1] stated the future trends in major aspects of M-Commerce. Moreover, the author also presented the M-Commerce services such as highly-personalized, context aware, location-sensitive, time-critical, pin-point information presentation forms the basis upon which promising applications can be built. The final one is that the author mentioned about privacy concerns, trust issues and security challenges in wireless area. Jari Veijalainen [5] discussed about the Transaction Manager (TM) design that can be called “Ontological Transaction Monitor”. The author

described that this acts as intelligent component between the application and the server accessed during M-Commerce transactions as well as of security and privacy. Francois Kritzinger [3] implemented as Secure End-to-End M-Commerce system. The author showed that this system satisfied to all of the fundamental requirements of secure computer systems as well as six out of the seven requirements of Secure Electronic Transaction. Seema Nambiar [4] studied the security measures in mobile security technologies which employed in the current M-Commerce market.

3. Wi-Fi Protected Access (WPA)

Making a dedicated communication between the specific nodes is the most significant fact in WPA. If the third party wants to join this communication, they have to submit the Network key which is generated by WPA.

Wi-Fi Protect Access (WPA) [7] is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined the protocol in response to several serious weakness researchers had found in the Wired Equivalent Privacy (WEP).

3.1. Wireless Network Standards

The Institute of Electrical and Electronic Engineering (IEEE) has defined 802.11 standards for wireless networks. Significantly, a wireless network is of great advantage compared to wired network. Wired network usually consumes a lot of time in order to set up in a building or house. In some instances, there is a need to route wires through thick wall or ceilings. Wireless network can deploy easily and is less expensive. More clients can be added to the network without necessity for extra materials. There are two types of operation mode in wireless local area network (WLAN) such as Ad-hoc Mode and Infrastructure Mode.

3.1.1. Ad-hoc Mode

This mode is also called the peer-to-peer mode or Independent Basic Service Set (IBSS) mode. Because it is a peer mode, the wireless stations communicate directly among themselves without using an access point.

3.1.2. Infrastructure Mode

This mode is called the Basic Service Set (BSS) infrastructure mode. Wireless stations and one access point are included in this mode.

3.2. Mobile Commerce (M-Commerce)

Mobile Commerce [6] also known as M-Commerce is ability to conduct commerce using a mobile device, such as mobile phone, PDA, or other emerging mobile equipment. M-Commerce is linked with wireless Internet and large number of Internet ready telecom terminals such as GSM. The idea is to serve the customer better by providing up-to-date information anywhere, anytime, anyhow using the mobile telephone. Using the mobile devices, the technology facilitates access to information that is on-line and up-to-date.

3.2.1. Threat (Security Risks) of M-Commerce

The success of M-Commerce depends much on the security of the underlying mobile technologies. Wireless communications rely on open and public transmission media that raise further security vulnerabilities, in addition to the security threat generally found in wired network. The treats of M-Commerce relate to user's mobile device, the wireless access network, the wired-line backbone network and M-Commerce applications.

Security threats in M-Commerce may be passive (such as information monitoring and release for fraudulent purposes) or active (such as the modification of information through denial-of-service and unauthorized access).

3.2.2. Vulnerabilities of M-Commerce

M-Commerce has lots of vulnerabilities because it is based on the wireless medium. Among them the most significant point of vulnerabilities is that protection of the data is not enough in the WLAN since wireless network can be accessed remotely from a distance without the need for a physical connection; anyone who is using compatible wireless equipment can potentially access the resources of LAN.

4. System Implementation and Design

4.1. Proposed System

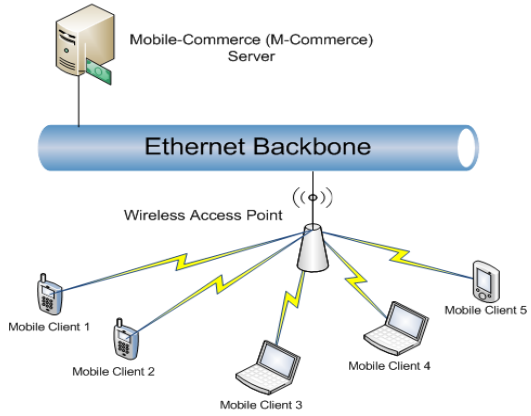

Figure 1. Wireless Infrastructure of the Proposed System

In this paper, only a pre-registered user can access the information from M-Commerce server to protect the attackers by using the significant point of WPA which is mentioned at the above. Based on this significant fact, we can create the dedicated communication between the M-Commerce server and all the pre-registered users as the specific nodes so that the proposed system can provide the highly security rate for active threat of M-Commerce because an unauthorized party cannot access the valuable information from server.

4.2. System Implementation

Figure 2. Pre-registered User Log-In Page

When a pre-registered user wants to access the information from M-Commerce server using a mobile phone, he/she has to fill up the log-in page as shown in the figure 2. The left arrow indicates about that the log-in page and the right arrow shows that the pre-registered user can log-in successfully.

If the requested user is an unauthorized user, there will be displayed the unsuccessful log-in page which is shown in the figure 3. After the pre-registered user had logged-in successfully, he/she can see the main category of available books. The main category page is shown in the figure 4.

Figure 3. Unsuccessful Log-In Page

Figure 4. Main Category Page

And then, a pre-registered user can search the books he/she wants to order from M-Commerce site. Order successful page is shown in figure 5.

Figure 5. Successfully Ordered Page

If a pre-registered user uses the laptop to access the information from server, they have to submit the network key which is provided by wireless infrastructure using WPA. After entering the network key, a pre-registered user has passed through the access point and they also has to log-in to access the web page from M-Commerce. The log-in page will be described figure 6. If the requesting user is an unauthorized user, that user cannot reach the web page because the WPA creates a dedicated communication which is only for the server and all the pre-registered users.

Figure 6. Pre-registered User Log-In Page Via Laptop

After a pre-registered user had successfully logged-in to the web site, he/she can choose any book he/she wants to order from the main category. This main page is shown in the figure 7.

Figure 7. Main Category Page for Using Laptop

Today, the threat to sensitive corporate information is greater than ever. End-users with multiple devices and making more decisions only serve to increase the risk. In this paper, step-by-step procedures for the infrastructure-based protection of an unauthorized access on M-Commerce and this procedure is described as figure 8.

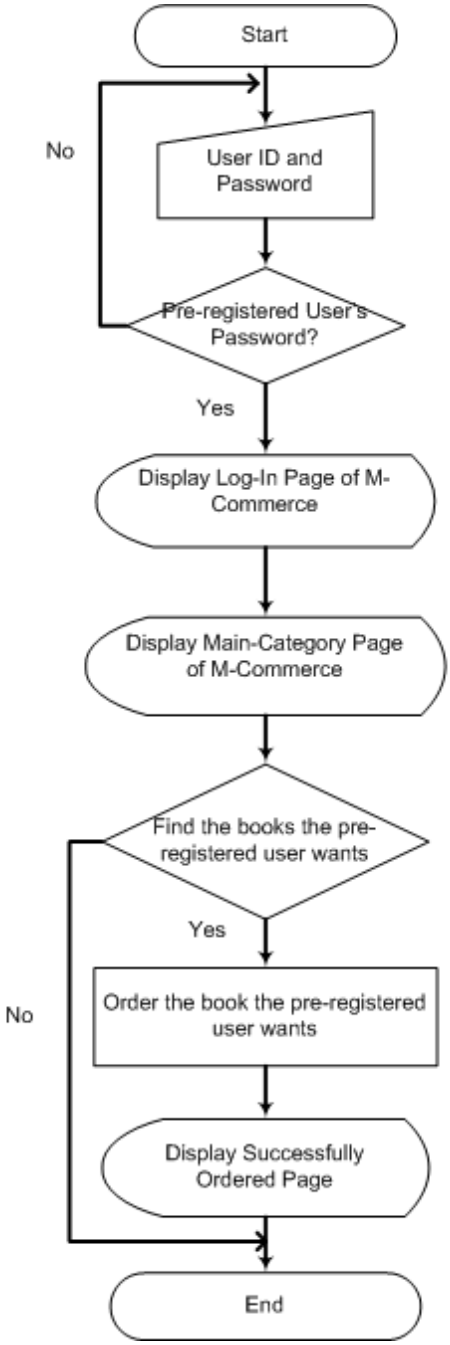

Figure 8. System Flow Diagram

5. Conclusion

Because of creating a dedicated communication between the specific nodes, this system can protect the access of unauthorized user and make a shelter for vulnerability of M-Commerce. This system provides the protection from the unknown users who can be an ordinary user or an attacker. Even though

they are the ordinary users, this system cannot give permission to access the information from M-Commerce. If the attackers get a chance to access the information, they can make many ways of attacking methods, for example, one kind of attacking is DoS (Denial-of-Service) and it can make the M-Commerce server responses too slow and cannot access the information from the other users.

In this system, we have discussed about WPA which is a kind of security mechanism for M-Commerce and used a significant point of WPA as an improvement way to protect the valuable information from M-Commerce server. The architecture suggested that WPA security module is a kind of barrier and to protect the unauthorized access on infrastructure-based M-Commerce.

References

[1] A. Grami, B.H. Schell, "Future Trends in Mobile Commerce: Service Offerings, Technological Advances and Security Challenges", Faculty of Business and Information Technology, University of Ontario

[2] S.S.Grosche, H.Knospe, "Secure M-Commerce", Information Security Group

[3] F..Kritzinger, D.Truter, "A Secure End-to-End System for M-Commerce: Research Paper", CS03-24-00, October 12, 2003

[4] S.Nambiar, C.T.Lu, "Analysis of Payment Transaction Security in Mobile-Commerce", IEEE International Conference on Information Reuse and Integration 2004 (IEEE IRI-2004)

[5] J.Veijalainen, V.Terziyan, H.Tirri, "Trasaction Management for the M-Commerce at a Mobile Terminal", '03 Proceedings of the 36th Annual Hawaii International Conference on System Science (HICSS '03) – Track3 – volume3A

[6]http://en.wikipedia.org/wiki/Mobile_commerce.htm

[7]http://en.wikipedia.org/wiki/WiFi_Protected_Access.htm