SECURITY LOOPHOLES AND PASSIVE ATTACKS FOR M-COMMERCE IN PKI-BASED INFRASTRUCTURE

Pramit Kumar Samant[1], Sandeep Kumar Viswakarma[2], Preeti Yadav[3]

[1,2]Computer Sci.&Engg Dept. Dr. KNMIET. Ghaziabad, (India)

[3]Computer Sci.& Engg Dept, M.J.P. Rohilkhand University, Bareilly,(India)

ABSTRACT

This paper presents attacks in a PKI-based architecture for m-commerce. Here, different types of attack will be designed and simulated. In addition, some loophole has been discussed in m-commerce for these attacks. Therefore, to analyze the performance, here developed and tested an application that implements the proposed method in a simulated environment. The results exhibit improvements in security aspects on both parts, the client as well as service provider.

Keywords: ARP Poisoning Attack, IP Address Attack, M-Commerce, PKI-Based System Architecture, Request/Response, Session Side Jacking Attack, Time Delay.

I. INTRODUCTION

Electronic and mobile commerce is now a major factor in modern economy. With no human- to- human contact, it has become crucial to strongly authenticate both the seller and the buyer. Lack of strong authentication has been a great obstacle for applications where payment is made through the phone. This is mainly due to the fact that the buyer cannot be authenticated reliably. The resources of handheld devices with wireless capability have also increased tremendously in recent years. However, security over mobile platform is more critical due to the open nature of wireless networks. Most of the existing techniques use PKI-based authentication [1, 2]. In the existing literature, a set of key exchange and authentication protocols that can run on a thin client model are presented in [3-5]. Wireless links are more vulnerable to security threats. Therefore, it is much easier for malicious users to gain access to the wireless network and perform fraudulent activities such as eavesdropping and impersonation [6]. However, this work does not address other possible attacks like session side jacking attack, IP address attack etc. [7], [8]. In this paper, we design different types of attacks and simulated with protocol. In addition, we propose a protocol for secure messaging with PKI. This protocol is a combined time-delay technique along with the request-response approach [9] in order to detect the delay, replay and forgery attacks. Afterwards, the calculated time delay will be compared with a reference time. The reference time is defined as the average value of round trip time and hacker processing delay. Finally, if the time delay [13-16] is greater than given reference time, the User Authentication Server (UAS) session will be aborted. Otherwise, the session will continue. The protocol has been simulated for attacks from false base station and clone of the cookies. The simulated results have been compared between delay of false base station and delay of actual base station calculated through ARP poisoning and session side jacking. Moreover, some loophole has been discussed in m-commerce due to some attacks can be performed.

II. PKI-BASED SYSTEM ARCHITECTURE

A typical PKI-based infrastructure for m-commerce is shown in Figure 1. The Short Message Service (SMS) gateway acts as a boundary between the wireless and wired networks

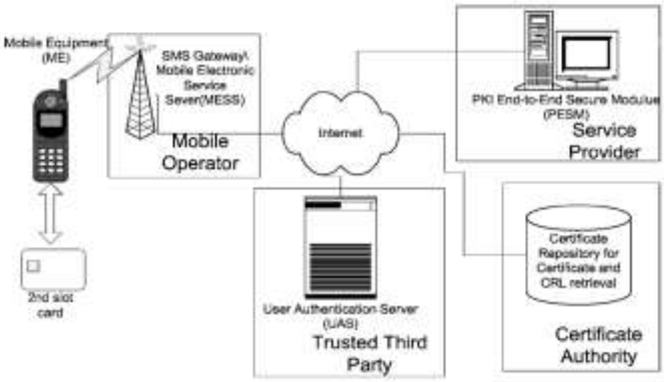
Mobile Equipment (ME)
SMS Gateway\ Mobile Electronic Service Sever(MESS)
Mobile Operator
Internet
PKI End-to-End Secure Module (PESM)
Service Provider
2nd slot card
User Authentication Server (UAS)
Trusted Third Party
Certificate Repository for Certificate and CRL retrieval
Certificate Authority

Figure 1: Typical PKI-Based System Architecture for M-Commerce [4]

Mobile Electronic Service Server (MESS) interprets the header of the message packets and routes the packets to the proper Mobile Equipment (ME) and servers. It is not capable to read the message contents since they are encrypted at source. The UAS is a centralized server that is operated by trusted third party. Its function is to assist the ME to verify the party to which it is communicating. Mutual authentication is performed first between ME and UAS. Its function is to assist the ME to verify the party to which it is communicating. Mutual authentication is performed first between ME and UAS. Then, UAS verifies the PESM on behalf of ME. Following, a PESM session key is exchanged between the ME and PESM to set up an end-to-end secure communication channel. PESM is a server operated by the service provider. It is accountable for ensuring security at the application level, includes authentication, confidentiality, and integrity. For authentication, it performs the handshake protocol to verify the UAS or optionally verify the mobile client and establishes a session key. For confidentiality, it encrypts and decrypts messages sent and received from the mobile client using the recognized session key. Furthermore, it verifies the message authentication code of each message to guarantee integrity. For non-repudiation, it verifies the digital signature of a message, if present. The certificate repository is a service provided by the Certificate Authority (CA), which allows the public to right to use the issued digital certificates. The UAS and PESMs will right to use this server from time to time to retrieve digital certificates for authentication purposes [4].

III. PREVIOUS WORK

Some mobile phone operators, such as Sonera in Finland, have their own secure system for mobile authentication. These systems have been sold mainly for businesses, where these systems have been used for authentication and authorization in back office systems [17]. PKI-based system architecture is described in [4]. This system uses a dual slot phone, where PKI-based application used for authentication is located in another card as the SIM card. An enhancement with a single slot was also proposed. However, the system needs several servers in the internet. Moreover, this paper does not discuss the attacks of the application. A system for end- to- end encryption of messages was described in [5]. It uses a symmetric algorithm and shared key. Furthermore, integrity of messages is guaranteed by using message authentication codes.

IV. SECURITY LOOPHOLES IN M-COMMERCE FOR THE DIFFERENT ATTACKS

This section presents some loopholes that are present in the m-commerce. While most of these also apply to e-commerce this is not because the same risks are present, but also because of the nature of wireless that has made it more vulnerable than wired networks. Therefore, some security loopholes in m-commerce for the different attacks are discussed below:

4.1 Wired Equivalent Privacy (WEP)

The main risk is that m-commerce network does not provide a way to secure data in transit against eavesdropping. Frame headers are always unencrypted and are visible to anyone with session side jacking attack. Security against eavesdropping was supposed to be provided by WEP. WEP protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving a session side jacking attack to disrupt transmissions with clone of the cookies. If the m-commerce network is being used for sensitive data, WEP may be insufficient. Consequently, WEP is the loophole in m-commerce for session side jacking attack.

4.2 IP Forwarding

The ARP poisoning attack turns on an operating system feature called IP forwarding. This feature enables the hacker’s machine to forward any network traffic it receives from Computer A to B. Consequently, IP forwarding is the loophole in m-commerce for ARP poisoning attack.

4.3 Operating System Weakness

Another security problem lies in the operating system. For instance, NetBIOS and SMB services allow unauthenticated users to create NULL sessions. Thus, IP address attack to gain access to information about the machines they exploit. These services are enabled by default on Windows systems. Windows 2000 and Windows XP port 135 through 139 and port 445. When improperly configured, NetBIOS. Consequently, operating system weakness is the loophole in m-commerce for IP address attack.

4.4 Rough Access Point Installation

Easy access to m-commerce network is coupled with easy deployment. Any users can purchase an access point and connect it to the corporate network with easy deployment. Any user can purchase an access point and connect it to the corporate network without authorization. Afterwards, rough access point deployed by end users poses great security risks. Many end users are not security experts and may not be aware of the risks posed by m-commerce network. However, hacker can easily pretend to be an access point because nothing in 802.11 requires an access point to prove it really is an access point. At the point, the attacker could potentially steal credential and use them to gain access to the network trough a man in middle attack (ARP poisoning, session side jacking and IP address attack).

V. RESULTS AND DISCUSSION

In order to emulate the proposed attacks, Back-Track 5 Penetration Testing System and J2ME toolkit [10, 11] have been used in PKI-based network for m-commerce for simulation. ARP poisoning with session side-jacking have been performed on Back-Track 5 system. However, delay and replay attacks have been detected by the given protocol [5] which is developed in J2ME toolkit. Wire-Shark Network Analyser [12] is used to validate the simulated result.

5.1 ARP Poisoning Attack

An attack allows us to capture traffic between mobile and router. This is done by poisoning the ARP of the two machines, making mobile believe that router's MAC address is our MAC address. Thus, all the traffic sent by mobile and router will come to our machine. We will subsequently reroute it to the appropriate destination, so the entire process is transparent to them. A potential way to discover if a man-in-the-middle attack is under way is to check our local ARP cache and see if it contains two machines with the same MAC address. The attack is simple from our machine. We send fake ARP reply packets to both hosts. These replies inform mobile that router's MAC address is our MAC address. Thus, all subsequent traffic sent by mobile to router will actually be received by our machine. We send a constant flow of ARP reply packets to mobile and router with the following contents:

Mobile: ARP reply informing that 192.168.187.130 has MAC address 00:0C:29:15:2B:3C

Router: ARP reply informing that 192.168.187.1 has MAC address 00:0C:29:15:2B:3C

From now onwards, all packets coming from mobile and router will be routed to us. Once captured, we have to reroute them to the intended recipient, depending on who the sender is: Packets coming from Mobile: forward to 00:0A:BC:1A:2B:1E Packets coming from Router: forward to 0F:AB:0D:0C:A1:0A For implementation, a computer running Back-Track 5 penetration testing system [9] has been connected to a network hub, which also has an option of Wi-Fi access point to it. A program to carry out an ARP poisoning attack is shown in Figure 2(a).

In first given horizontal screen, arpspoof program sends ARP reply informing that mobile 192.168.187.130 has MAC address 00:0C:29:15:2B:3C. And in second horizontal screen, it sends ARP reply informing that router 192.168.187.1 has MAC address 00:0C:29:15:2B:3C. From now on, all packets coming from mobile and router will be routed to us. Once captured, it has to reroute them to the intended recipient. This attack can be detected by proposed protocol.

5.2 Session Side Jacking Attack

In this case computer running Back-Track 5 penetration testing system [9] was connected to a network switch, which also has an option of Wi-Fi access point to it. The network interface on the computer is set to eth2, which allows the device to see all traffic on the network switch. The urlsnarf program is run which intercepts the traffic on the network interface (eth2). And inspects it for URLs If a URL is found, it is printed to screen. Bear in mind, all network traffic is intercepted so any encrypted data such as user names or passwords could be similarly captured and viewed. A program to carry out an ARP spoofing attack with session side-jacking attack is shown in Figure 2(b):

In first given horizontal screen, arpspoof program sends ARP reply informing that mobile 192.168.187.130 has MAC address 00:0C:29:15:2B:3C. And in second horizontal screen, it sends ARP reply informing that router 192.168.187.1 has MAC address 00:0C:29:15:2B:3C. From now on, all packets coming from mobile and router will be routed to us. Now, session cookie has been captured using urlsnarf program shown in second vertical screen for performing session hijacking.

5.3 IP Address Attack

In this case computer running Back-Track 5 penetration testing system [9] was connected to a network switch, which also has an option of Wi-Fi access point to it. The network interface on the computer is set to eth2, which allows the device to perform IP address attack on the network switch. Consequently, a program for IP address attack has been shown below:

- set payload windows/shell/reverse_tcp
- Use exploit /windows/smb/ms08_067_netapi
- set lhost 192.168.187.128
- set rhost 192.168.187.128
- set rhost 192.168.187.201
- show options
- exploit
- It has entered victim machine for testing

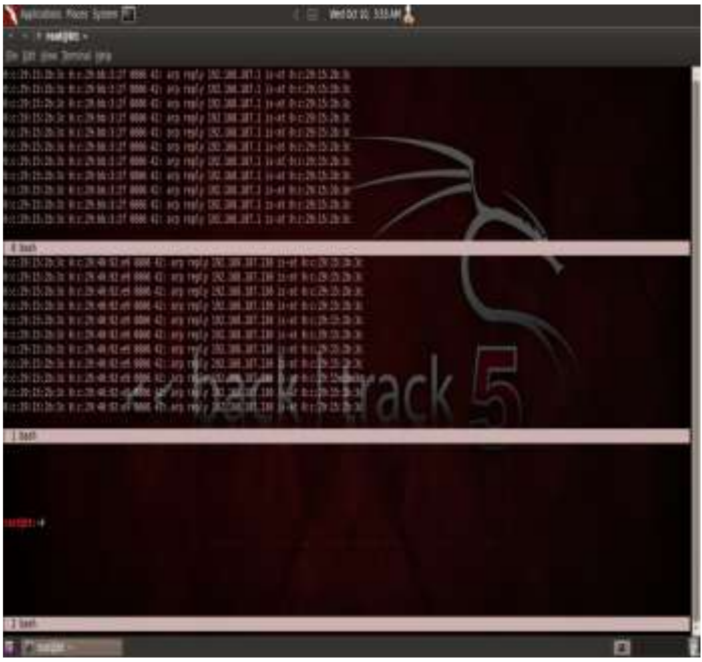

Figure2 (a):ARP Poisoning Attack

A program to carry out an IP address attack is shown in Figure 2(c) & 2(d).A program to carry out an IP address attack is shown in Figure 2(c) & 2(d).Consequently, the results are shown in Figure 2(e), 2(f) & 2(g).

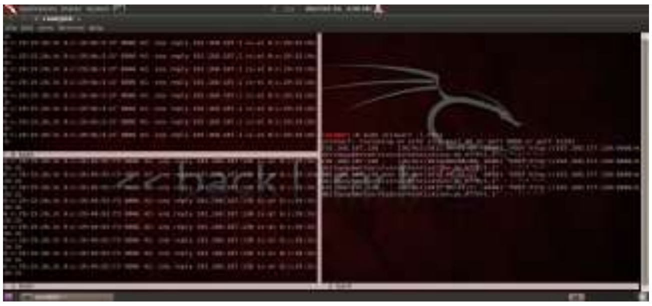

Figure 2(b) Session Side-Jacking Attack

i.e., in Figure 2(e), where the time delay is shown by X - axis and the number of packets are shown by the Y- axis. which describes the time delay with respect to the number of packets of received. Firstly, in the absence of hacker’s setting, *i.e.*, in Figure 2(e), where the time delay is shown by X - axis and the number of packets are shown by the Y- axis.

Figure2(c): IP address Attack

Figure2(d): IP address Attack

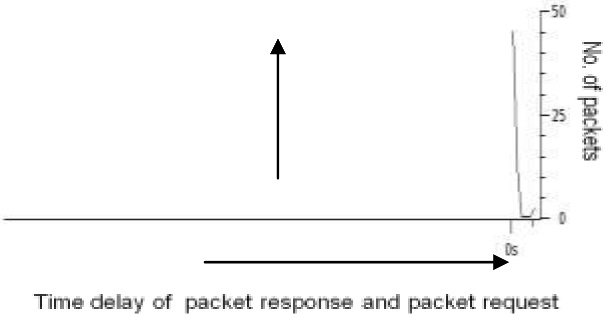

Figure 2(e) Time delay before ARP poisoning Attack

to its minimum level. Therefore, it is observed that time delay of request/response message becomes minimum with number of packets that are moved between mobile and router. Here, the time delay is round trip time (RTT) of the packets with mentioning no attack is there. Second, in the presence of hacker setting, *i.e.*, in Figure 2(f), this determines that there is little activity on the PKI-based network for the first 54 seconds of the packet capture, which increased to rate approximately to 45 packets per seconds for 2 seconds before activity returned to minimum level. So, it is observed that time delay of request/response message becomes maximum with number of packets that are moved between mobile and router through the interface of hacker. Here, the time delay is processing time (54 seconds) of hacker with RTT (2 seconds) of packets with mentioning ARP poisoning.

Third, in the presence of session side jacking setting, *i.e.*, in Fig. 2(g), by default, plots the time delay on the X axis and the number of packets on the Y axis. This allows us to determine that there is little activity on the PKI-based network for the first 78 seconds of the packet capture, which increased to rate approximately to 45 packets per seconds for approximately 2 seconds before activity returned to minimal level. So, it is observed that time delay of request/response message becomes maximum with approximated number of packets that becomes maximum with approximated number of packets that are moved between mobile and router through the interface of hacker. Here, the time delay is processing time (78 seconds) of hacker with RTT (2 seconds) of packets with mentioning session side jacking attack.

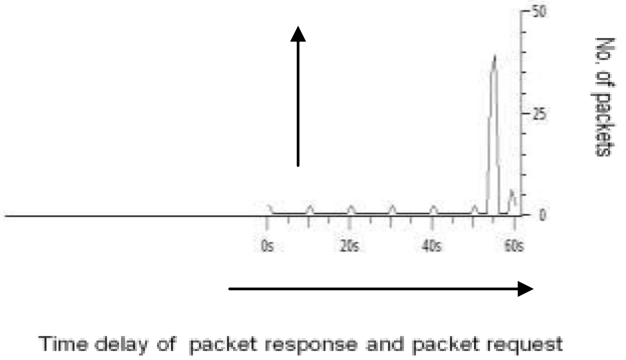

Figure 2(f) Time delay after ARP poisoning attack

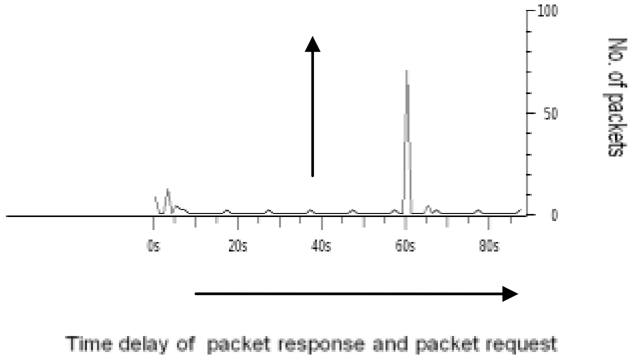

Figure 2(g) Time delay after Session side jacking attack

VI. CONCLUSION

The use of PKI-based system architecture can significantly increase trust in modern electronic commerce, to the benefit of both service providers and their customers.

In this paper, we have shown ARP poisoning, session side jacking and IP address attacks along with Back-Track 5 penetration testing system in order to make false base station ,clone of the cookies, computer hijacking. Consequently, some loophole has been discussed in m-commerce for these attacks. It has been shown that simulated results i.e., time-delay enable to detect ARP poisoning with session side-jacking attacks resulting in a more unsecure architecture for m-commerce applications.

.

REFERENCES

[1] S. Blake-Wilson, D. Johnson, and A. Menezes , "Key Agreement protocol and their security analysis," Sixth IMA International Conference on Cryptography and Coding, Vol. 1355, pp. 30-45, December 1997.

[2] C.H. Lim, and P. J. Lee, "Several practical protocols for authentication and key exchange," Information Processing Letter 53, pp. 91-96, 1995.

[3] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks," IEEE Personal Communications, Vol. 1, pp. 25-31, 1994.

[4] Wu Yanyan, "Design of a PKI-Based Architecture for Mobile E-Commerce," Third International Conference on Information and Computing (ICIC), Vol. 1, pp. 97-100, 2010.

[5] Pramit Kumar Samant, Poonam Saini, and C. Rama Krishna, "A Combined Request/Response and Time Delay Technique to detect Attacks in a PKI-Based Architecture for M-Commerce," in the proceeding of 3rd IEEE International Advance Computing Conference, (IACC-2013), held on Feb 22-23, 2013, Ghaziabad (UP), India. Catalog Number: CFP1339F-CDR, ISBN: 978-1-4673-4528-6.

[6] Scarlet Schwiderski-Grosche, and Heiko Knospe, "Secure M-Commerce," Electronic & Communication Engineering Journal, Vol. 14, pp. 228-238, 2002.

[7] Crtiana L. Abad and Rafael I Bonilla, "An Analysis on the Schemes for detecting and Preventing ARP Cache Poisoning Attacks," 27th International Conference on Distributed Computing Systems Workshop (ICDCSW'07), pp. 60-67, April 2007.

[8] Xiaobo Long, and Biplab Sikdar, "Wavelet Based Detection of Session Hijacking Attacks in Wireless Networks," Global Telecommunication Conference, IEEE Communication Society (GLOBECOM'08), pp. 1-5, 2008.

[9] Wenlan Ying, Aiping li, and Liyun Xu, "Research on the Authentication Strategy of ASP Mode-based Networked Manufacturing System," Proceeding of the 2008 ieee/asme international conference on advanced intelligent mechatronics, pp. 1014-1017, 2008.

[10] Vivek Ramachandran, "Back Track 5 Wireless Penetration Testing," PACKT publishing, 2011.

[11] James Keogh, "J2ME: The Complete Reference," Corel VENTURA, 2007.

[12] J.F. Kurose, and K. W. Ross, "Computer Networking: A Top Down Approach," 4rth Edition, Version 2.0, 2007.

[13] Albert Treytl, and Bernd Hirschler, "Practical Application of 1588 Security," Precision Clock Synchronization for Measurement, Control and Communication, 2008. ISPCS 2008. IEEE International Symposium on, pp. 37-43, 2008.

[14] Cheng-Chi Lee, Te-Yu Chen, Chun-Ta Li, Chi-Tung Chen, and Ping-Hsien Wu,"A New Key Exchange Protocol with Anonymity between STB and Smart Card in IPTV Broadcasting," Wireless Communications, Networking and Mobile Computing (WiCOM),7th International Conference on, pp.1-4, 2011.

[15] Bogdan Groza, "Broadcast Authentication Protocol with Time Synchronization and Quadratic Residue Chain," Availability, Reliability and Security (ARES), the Second International Conference on, pp. 550-557, 2007.

[16] Kalid Elmufti, Dasun Weerasinghe, M Rajarajan, Veselin Rakocevic, Sanowar Khan, "Timestamp Authentication Protocol for Remote Monitoring in eHealth," PervasiveHealth 2008. Second International Conference on, pp. 73-76, 2008.

[17] Marko Hassinen, Konstantin Hypponen, "Strong Mobile Authentication," Wireless Communication Systems, 2005. 2nd International Symposium on, pp. 96-100, 2005.

	Pramit Kumar Samant received Master of Engineering in Computer Science and Engineering from the National Institute of Technical Teacher's Training and Research, Chandigarh, India. His research interest in the field of Network Security, Algorithm and Mobile Ad-hoc Network.
	Sandeep Vishwakarma received Master of Engineering in Computer Science and Engineering from the National Institute of Technical Teacher's Training and Research, Chandigarh, India. His research interest in the field of Network Security, Artificial Intelligence and Automation.