IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

M-Commerce: Risks, Security and Mobile Banking Payment Methods

Akanksha Srivastav[1], Ajeet Bhartee[2]

Department of Computer Science, Galgotia's college of engineering and technology Gr. Noida[1, 2]

Abstract: Mobile commerce is more popular in present time just only because of their mobility. M-commerce is the electronic commerce using mobile device. Here discuss the use of security method for prevention of spy type attacks. Mobile phone security has turned into an imperative part of security issues in wireless multimedia communications. As the most mainstream mobile operating system, Android security has been widely contemplated by scientists. Be that as it may, few works have concentrated on mobile phone multimedia security. In this article, we concentrate on security issues identified with mobile phone cameras. In particular, we find a few new assaults that depend on the utilization of phone cameras. We actualize the assaults on genuine phones, And exhibit the achievability and viability of the assaults Besides, we propose a lightweight protection conspire that can successfully distinguish these assaults.

Keywords: M-commerce, mobile security, multimedia.

I. INTRODUCTION

M-commerce is known as mobile commerce. The development in wireless and mobile has brought too much opportunity in the field of m-commerce. Mobile commerce is the result of revolution in communication. Day by day m-commerce getting too much popular and demand of this is increasing.
Mobile communication provides instant connectivity with high speed data service anytime anywhere to the mobile user. Mobile payment is defined as services between two parties in which mobile phone play vital role in the payment realization. In a m- payment activity for banking or financial transaction payer need one or more step .mobile payment is easy and proportion the electronic payment. That's why security is very important.

FEATURES OF M-COMMERCE

1] UBIQUITY
2] IMMEDIACY
3] LOCALISATION
4] INSTANT CONNECTIVITY
5] PROACTIVE FUCTIONALITY

1] UBIQUITY: It offered user geographical location
2] IMMEDIACY: This feature is related with ubiquity where real time availment of services i.e. Stock market.
3] LOCALISATION: This is position localization technology such as GPS offers goods and services specific to customer location.
4] INSTANT CONNECTIVITY: Constant online facility connected with the dial up or boot procedure.
5] PROACTIVE FUCTIONALITY: This feature provides the right information at right time and place.

II. M-COMMERCE ARCHITECTURE

M-commerce is the three tier architecture
1] FRONT END (client)
2] MIDDLEWARE (server)
3] Back end (database)

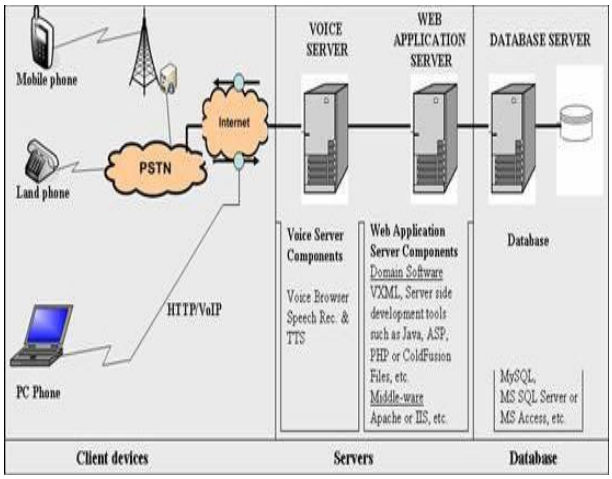

Fig-1[6] M-Commerce architecture

FRONT END- the cellphone are the client device and it's used to access different service to user. It provides front end interaction to the customer and server.
The base station will route and forward the services to the destination. The sms gateway/ WAP gateway support internet based communication.
MIDDLEWARE- The middleware constitute webserver keeps the business logic of the m-commerce system after successful authentication of user, the server will provide service request by client after charging.
BACKEND- at the backend database exit for further services which come from front end.

III. MOBILE BANKING

M-banking is important mobile commerce application [1]. Mobile commerce can be defined as E-commerce transaction, using mobile device through wired or wireless technologies [2].success of mobile commerce growing day by day because of its easy to use, convenience and trustable feature [3].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

The key player in mobile banking is bank and other financial institution and mobile operation.[4]. Day by day grow of m-commerce it must be ensure that end user must be confident in the financial institutions carrying out the transaction.

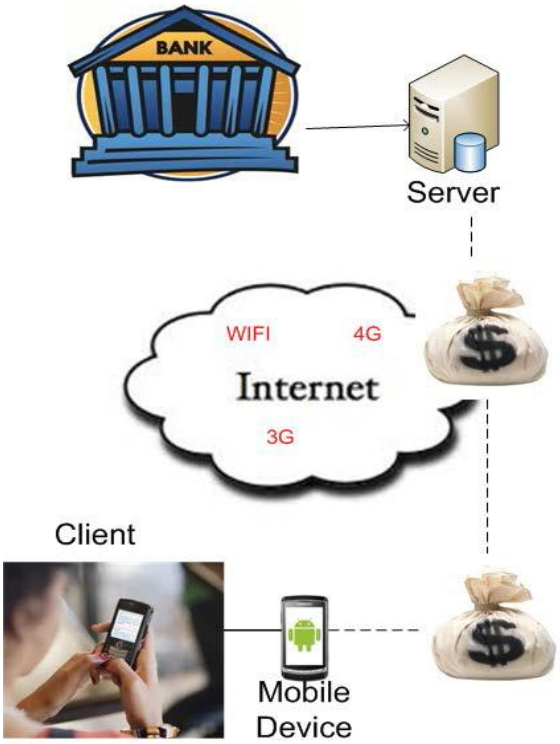

Fig-2 [7] M-banking structure

IV. MOBILE BANKING SECURITY ISSUES LITERATURE

The security issues in m-banking is much more needed when ratio of its uses rise dramatically [5]. Survey conducted by KPMG covering more than 5500 consumer in 22 countries. In the united nation 30% of house hold uses mobile phone to perform banking operation. Rather than in Asia (India, china, Korea) it's about 43%. In Australia 19%of household using m-commerce.

V. M-PAYMENT LIFE CYCLE

Mobile payment life cycle has main steps-
A] Registration
B] Transaction
C] Payment settlement

First of all for the mobile payment open the payment account through the registration process .and after that transaction comes under process, under this process we have some more steps through which we continue the process, the content provider forward the request to the payment service provider and this one connected with third party for authentication and authorization. after this if customer successfully authorize than payment provider inform to content provider and then its successfully deliver the goods. And then payment settlement process takes place during postpaid or prepaid mode.

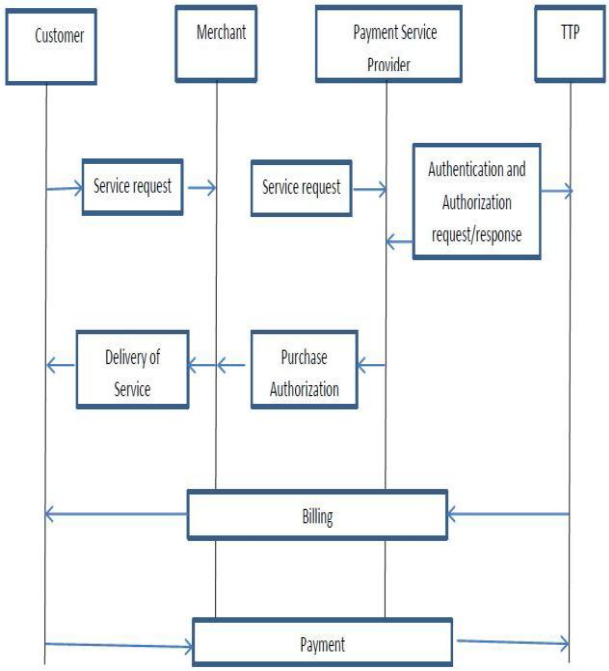

Fig-3 [8] m-payment cycle

VI. SECURITY IN MOBILE NETWORK

Security in mobile network in different modes-
1] Security in GSM
2] Security in CDMA
3] Security in UMTS
4] Security in 4G

VII. SECURITY ISSUES IN EXISTING SYSTEM

A few video-based attacks focused at keystrokes have been proposed. The attacks can acquire client information on touch screen Smartphone. Execute a programmed shoulder surfing assault against present day touch-empowered Smartphone. The assailant sends a video camera that can record the objective screen while the casualty is entering content. At that point client info can be reproduced exclusively basedon the keystroke input showed on the screen. Nonetheless, this assault requires an extra camera device, and issues like how to put the camera close to the casualty without getting a caution must be considered painstakingly.

VIII. CONCLUSION

In this article, we first lead a survey on the threats and advantages of spy cameras. At that point we exhibit the essential attack model and two camera-based attacks: the remote-controlled real-time monitoring attack and the password inference attack. We run these attacks alongside well known antivirus software to test their stealthiest, and behavior examinations to assess both sorts of attacks. The outcomes show the possibility and adequacy of these attacks. Finally, we propose a lightweight safeguard plan. In this work, we can conceal the entire camera app in Android. Also, we execute propelled types of attacks, for example, remote-controlled and real-time monitoring

attacks. We likewise use PC vision methods to examine recorded recordings and infer passwords from clients' eye developments.

REFERECES

[1] Ashok K Talukder and Roopa R Yavagal, "Mobile Computing", TaTa McGraw Hill Education, January 2005
[2] Hua Ye, "Design and Implementation of M-Commerce system applied to 3G Network platforms based on J2ME", IEEE International conference on Electrical and Control Engineering, 2010
[3] Hakima Chaouchi and Maryline Laurent maknavicius, "Wireless and Mobile Network Security", Second Edition, Wiley Publishers
[4] Anurag Kumar Jain and Devendra Shanbhaug, "Addressing Security and Privacy Risks Mobile applications", IEEE Computer society, 2012
[5] (2010), Mobile banking rising globally, but Australia yet to fully embrace
[6] The m-commerce architecture from "Security issues and challenges in mobile computing and m-commerce"International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015
[7] M banking architecture "Security issues and challenges in mobile computing and m-commerce"International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015
[8] M payment cycle "Security issues and challenges in mobile computing and m-commerce"International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015

DOI 10.17148/IJARCCE.2016.52135