User Authentication Techniques for Mobile Payment: A Survey

Pushpalatha.M[1] Anand.R[2] Dr Rajshekhar M Patil[3]
[1]II Semester PG Student, Department of CSE, BMS Institue of Technology,Avalahalli
[2]Assistant Professor, Department of CSE, BMS Institue of Technology,Avalahalli
[3] Associate Professor, Department of CSE, BMS Institue of Technology,Avalahalli,
Yelahanka,Bengaluru-560064,Karnataka,India.

Abstract- **Mobile authentication system for moblie payment can be used either the web or mobile channel indiviually to confirm the identity request of a remote user. Most common user activity in mobile commerce is done through mobile devices .The mobile phones are invloved to numerous security threats due to presence of valuable financial and personal datasets . To provide a secure web transcation using mobile phones, multifactrolial authentication technique preferred.User authentication technology using mobile phones ,one of the mutifactroial authentication technique, can be potentially copied to an another device. This paper proposes Transaction Certificate Mode(TCM),a software tokens, by which supports mutual authentication considering a stolen,borrowed, and infected mobile phones for mobile payments.**

Keywords- Mutual authentication; mobile payment protocol; mobile phones; transcation certificate; software token;multifactroial authentication

1 INTRODUCTION

Security Risks are of great concerns. Many companies are comfortable with protecting their confidential information and transactions with a password. A simple password security may be effective for protecting the noncritical data. But passwords, administrative issues and password hacking tools render a password-only authentication policy inadequate for protecting confidential information and transacations.

There are different strategies proposed for making authentication mechanism more and more secure. The secure passwords can be hacked in different ways such as Hashing, Guessing, Default Passwords, Brute Force and Hashing. Generally, a password containing both uppercase & lowercase characters, numbers and special characters be guessed. But still is not much secure way of authentication.

Authentication using mobile phones is one way to bring such devices into the realm of security. Use mobile devices for authentication purposes, have employed weak authentication (i.e., only a username and password pair) using input and output features of such devices. Weak authentication is known for its vulnerability to several attacks, including shoulder sur_ng, phishing, and key logging.

Many password-based schemes use static identity, which can easily leak information to an attacker. Many papers have proposed a number of techniques for preserving the user’s anonymity by employing a random value or time-stamp, to vary user identity for each session. These schemes provide a smart card for each user and assume that the contents of smart card for each user cannot be disclosed.

One way to strengthen your authentication roles is by adding factors such as tokens, smart cards, digital certificates and biometrics. The most common form of multi-factor authentication is to two-factor authentication using a tokens or smart cards as the second form of identification. For the two factor authentication, mobile phones can be a good choice to everyone carries a mobile handset.

Many user authentication schemes for mobile client-server environment were proposed, these schemes are subjected to an inherent design weakness, namely, the server knows all users’ private keys.For this problem, these schemes cannot provide insider attack resistance or mutual authentication. Some of these schemes cannot simultaneously provide user anonymity, perfect forward secrecy, or leakage of session temporary secrets resistance.

Remote user authentication allows a remote user and a server authenticate the identity with each other over insecure networks. Mobile devices are widely and popularly used in many electronic transaction, such as online shopping, Internet banking, e-payment, e-voting and pay-TV. Considering the limited energy resources and computing ability of mobile devices, it is inappropriate for remote user authentication schemes to be realized in traditional public key cryptography because most cryptographic algorithms require much expensive computation and it suffers from heavy certificate burden.

Mobile phones are most common devices to do business and commerce due to involvement of huge financial and personal data transferring such as Personal Identification Number (PIN), Bank Account Number (BAN) etc. Mobile commerce demands the means for secure mobile payment. The security issue of mobile networks challenges more efficient protocols and authentications. Authenticating users on mobile devices can be challenging, and many solutions currently being used by mobile applications either compromise security or usability. Two common solutions that are often used are:

Requiring the user to enter a password every time the application is started. Complex passwords are difficult to enter on mobile devices, and requiring frequent password entry typically results in users either saving the passwords on their devices in plain text files (so they can be copied and pasted), or in users choosing weak passwords that they can easily enter on their devices.

Requiring the user to enter a password once, and storing it on the device for subsequent authentication. Even if the password is stored encrypted/obfuscated, the key required to decrypt/decode the password needs to be stored in one of two locations: Somewhere on the device: the device decrypts the password and sends it to the server if the device is lost or stolen, the user's password is compromised.

The device transmits the encrypted password to the server. The encrypted password is as good as the user's actual password for authenticating to the server. If the device is lost or stolen, the user's password may be protected, but the user's account is compromised. This compares various approaches for authenticating users on mobile devices and highlights their pros and cons in terms of security and usability.

Risks

A mobile device, user authentication solution must address three main security risks.

Stolen devices

If a user's device is lost or stolen, the attacker can generally get access to everything stored on the device. This is generally true because currently, most mobile devices either do not support disk encryption, or do not have disk encryption enabled by their users. If a user's device is stolen, the attacker can access plaintext data on the device, brute force passwords used to encrypt data, etc. The attacker can perform both software attacks and physical attacks against the device

Borrowed devices

The likelihood of this risk is much greater for mobile devices than for other computers (laptops, desktops, etc.). Users often allow others to borrow their mobile devices to make a phone call, send a SMS, etc., and mobile devices currently only support a single user account/password. Users cannot create a "guest" account on their devices that only offers access to a limited subset of functionality.

The risk is different than that of a stolen device because in this case, the user provides the device in an unlocked state to somebody else. Therefore, full disk encryption is an ineffective control in this case. On the other hand, the types of attacks that can be conducted with a borrowed device are limited as the user borrowing the device will have access to it for a limited amount of time and may be under the device owner's supervision.

Infected devices

Mobile devices are at least as likely to get infected with malware as any other type of computer. In fact, there are several reasons why mobile devices may be more likely to get infected.

Users download applications for many purposes on their mobile devices from potentially untrusted sources. Most users do not have separate devices for corporate e-mail, online banking, media streaming, gaming, etc. Most mobile platforms allow users to download applications from large "application stores" containing hundreds of thousands of applications. Although some application stores have stricter controls than others, there is no way for the application stores to guarantee that the applications they are providing do not contain something malicious.

Currently supported desktop and server operating systems generally receive frequent security updates; however, due to several reasons, mobile devices' operating systems do not receive frequent security updates. Many mobile devices receive updates every few months, and many run operating systems that are several years old. Many mobile devices run operating systems with known exploitable vulnerabilities.

Anti-virus software for mobile devices is not as mature as anti-virus software for desktop and server operating systems. This is due to a combination of several factors including a lack of operating system support, limited battery life on mobile devices, etc.

II THE RELATED WORKS

Two factor authentication programs that combine both security and convenience using QR (Quick Response) code with smart phone users can login to the website without to put 6 to 8 digit code such as OTP(One Time Password). Users can happy with both security and convenience. They encourage further research into technological development within internet security systems because of the significant role security systems play in the growth of online shoppings.

A strong authentication mechanism that exploits the use of mobile devices to provide a two-factor authentication method. Their approach uses a combination of one-time password, as the first authentication factor, and credentials stored on a mobile device, as the second factor, to provider a strong and secure authentication approach. They also provides a analysis of the security and usability of this mechanism. The security protocol is analyzed against an adversary model this evaluation proves that their method is safe against various attacks, most importantly key logging, shoulder surfing, and phishing attacks. A security token may be a device that an authorized user of system services is given to ease authentication. Security tokens are used to prove one's identity electronically .We have two types of Tokens- Hardware Token and Software Tokens. The token is used in addition to or in place of a password to prove that the customer is who they claim to be. The token acts like an electronic key to access something. Hardware tokens are typically small enough to be carried in a pocket and often are designed to attach to the user's keychain. Software Tokens are type of security device that may be used to authorize the use of system services. Software tokens are stored on a general-purpose electronic device such as a desktop computer, laptop, PDA, or mobile phone.

Singhal and Tapaswi a method of implementation of Two Factor Authentication using Mobile handsets. This two factor authentication is based on Time Synchronous Authentication using the RFC1321 MD5 Message Digest Algorithm of Epoch Time, Personal Identity Number (PIN) and Init- Secret. The password generated would be One Time Password (OTP) which would be valid for 60 seconds only after which it expires and the user can not login through that password.

III. TRANSACTION CERTIFICATE MODE(TCM)

Many protocols came begin into successvily to meet the requirement of operations in low power roming environment with the fast advance of communication technologies. Unfortunately,these protocals are not suffient for special requirements in automobile roming system such as low power consumption, high performance and convenience so these protocols are pay more attention to the common network environment.

To provide a security of encryption algorithm is very important,they are limited to the mobile phones resources such as processor capabalities and memory capacity The proposes a TCM software which provides a mutual authentication considering limited mobile phone resources

III TCM construction

TCM is software for certificates which confirms the valid user and merchant accessing their accounts.TCM composes TCM1 and TCM2,Customer Bank (CB) has issued TCM1 and Merchant Bank (MB) has isssued TCM2

TCM algorithm uses the following terms:

1)International Mobile Equipment Identity(IMEI) number

IMEI is a number and unique to identify to Global System for Mobile communication (GSM) or Code Division Multiple Access (CDMA) mobile phones . It is found at the battery compartment of the phone

2) *one time password*

Password for every transaction will be generted using IMEI number which is unique.Same password is stored on server, which uses the same software genertor program where it can be crosschecked for authentication.

3)Call Back Technique

When ever user connects to a server and confirms user ID and password, and server disconnects the user connection and tries to connects the user directly.This technique is used in windows server operating system for confirming the identity of dial up users

IV CONCLUSION

Now a days,Two Factor Authentication becomes more and more popular. But on the other hand, there are disadvantages of T-FA also. The drawback of strong authentication is that every user has to be provided with a token device. This can be quite expensive.This paper has proposed a new security algorithm for mobile phones based on the mutual authentication
communication techniques and developed mobile payment protocol using TCM

It can be used to encrypt a counter value and send it to the server each time it needs to authenticate to the server. This will require the server to maintain a counter value for each device that connects to it.

V REFERENCES

[1] S manav and T.shashikalla “software token based two factor aunthtication schema “International Journals Information and Electonics Engineering vol2. NO3 2012.

[2] Li-Hua Li,Iuon-Chung LIN and Min-shing Hwang,”A Remote password Authentication Schema for Multi –Server Architecture using Neutral Network ,vol.12,pp 1498-1504,2001.

[3] Jau-Ji Shen, Chih-Wei Lin and Min-Shiang Hwang, “A Modified Remote User Authentication Scheme Using smart cards”, IEEE *Transactions on Consumer Electronics vol.49* pp.414-416, May 2003.

[4] K. Nima, H. Kirstie and B.konstantin,” A Two-Factor Authentication Mechanism Using Mobile Phones”,2008