Password Authentication System in Two Way Mobile Communication using image as a secrete Key

Nupur Shah, Prof. Pankaj Pandey

Abstract— During the transmission of message from sender to receiver in mobile communication needs various security protocols which prevents these messages from various types of attacks. Although there are various protocols implemented to check the authenticity of the sender and receiver so that the chances of attacks can be reduces. Here in this paper an efficient technique of two factor using OTPK and image based authentication is proposed to prevent from various attacks in mobile communication.

Index Terms— OTPK, PAKE, PRNG, Authentication, Signature.

1 INTRODUCTION

ne of the major areas of security improvement is the way in owhich authentication of users is carried out. Although various private and government organizations still rely on static ID and password authentication system. One of the solutions for this issue is the two factor authentication technique as a fundamental security function. Providing secure communication over insecure open networks has been a great concern for researchers. During recent years, cryptographic approaches have been applied to remove these problems. Hence password authentication system is required to validate the trust of communicating parties. Password can be a word combination of letter, characters and numbers that is used to identifying or confirming the right person. This process is known as authentication.

Security in computers is information protection from unauthorized or accidental disclosure while the information is in transmission and while information is in storage. Authentication is a process of determining whether a particular individual should be allowed to access a system or an application [1].

Two-factor authentication method is implemented in two main phases. In the first phase, the authenticator gets a request generated by the application to authenticate a specified user. As soon as the request is received, it generates a one-time password and sends it through a SMS to a GSM cell phone registered for that specified user [2] It proposes a secure, convenient and user friendly two factor authentication scheme and discusses its applications to online banking.

In present, the security enabling verification codes send through the SMS to the corresponding user mobile. These types of verification codes are generated in one way communication that is, the codes are received from the server then the user enter the codes in corresponding server application window. The verification codes are best approach to protect the applications or systems but in these one way verification codes lots of limitations are there. The users easy to access the codes but the codes enter the server application window. But these passwords schemes are mostly affected from network congestion and other technical issues. Hence it is less reliable with time constraints.

Mobile is a common electronic gadget that is used beyond the calling and messaging. Due to high availability and connectivity it is commonly used other purposes also like banking (Mobile Banking), social connectivity (Facebook, Twitter etc.) and many mobile based applications. It is also used for authentication using OTP. OTP stands for one time password i.e. instant code sent by any authentic body to confirm the authenticity of the person. . OTP algorithms are critical to the security of systems employing them since unauthorized users should not be able to guess the next password in the sequence [3].

Most password-based user authentication systems place total trust on the authentication server where passwords or easily derived password verification data are stored in a central database. Conciliation of the authentication server by either outsiders or insiders subjects all user passwords to exposure and may have serious problems. Hence for the solving of these issues single server system many of the systems has been proposed such as multi server systems, public key cryptography and password systems

The process of password authentication is used for many services. Especially financial transactions needed it very much and various attacks are imposed on such systems. To maintain the high level of security many researchers work on it. The rest of paper is organized as follows. In Section II describes about background information of password authentication. Section III describes related work in fields of authentication systems followed by a conclusion in Section IV.

2 BACKGROUND

The ever increasing use of internet around the world has without doubt increased the usage of internet based services,

This has necessitated the need of more secure ways of communications. The issues of Confidentiality and Integrity of systems are of prime importance and more research towards these issues has been called for around the world.

In the present day environment, there is a need to make sure that only the authorized clients can be able to access the secured data or sensible information. Hence one-factor authentication is not adequate in terms of security with the high risks involved in e-business.

3 Related Work

In 2013, Sundari B. S. et al [1] presented a new method password authentication system for mobiles. They call it Password Authentication System Using New Intense Secure Algorithm in mobile and server in Two Way Communications (PAST). It is a two way password authentication system. A person can login with their existing password and after than a system generated verification code is sent to user's register GSM mobile. This verification code provides actual access of service. The same concept is used by various banking and other financial transaction based organizations. This concept is similar to one time password key (OTP). The use of mobile id offers extra verification mechanism. A user must have both login passwords along with registered mobile number for getting code in form of short message service (SMS) [1].

Anamika et al [7] proposed Password Authenticated Key Exchange (PAKE) protocols have been played an essential role in providing secure Communications. PAKE protocols permit a client and a server to authenticate each other and generate a strong common session key through a pre-shared human memorable password over an insecure channel. Two-party password-based authenticated key exchange (two-PAKE) protocol is quite useful for client-server architectures. However, in large-scale client-client communication environments where a user wants to communicate with many other users, Two-PAKE protocol is very inconvenient in key management that the number of passwords that the user would need to remember.

Password-based authenticated key exchange (PAKE) protocols enable two users to generate a common, cryptographically-strong key based on an initial, low entropy,
shared secret (i.e., a password). The difficulty in this setting is to prevent off-line dictionary attacks where an adversary exhaustively enumerates potential passwords on its own, attempting to match the correct password to observed protocol executions. Roughly, a PAKE protocol is secure if off-line attacks are of no use and the best attack is an on-line dictionary attack where an adversary must actively try to impersonate an honest party using each possible password. On-line attacks of this sort are inherent in the model of password-based authentication; more importantly, they can be detected by the server as failed login attempts and defended against.

Two-way SMS applications are more intricate than one-way. In two-way SMS applications, a user can initiate a conversation by sending messages. The life cycle of two-way SMS can be divided into 4 main steps 1. User sends request to SMS gateway 2. SMS gateway forwards request to application server 3. Application server processes request and responds to SMS gateway 4. SMS gateway forwards request back to user mobile (fig. 1). In contemporary, using one way communication for authentications a few drawbacks are obtained when assess than two way communications. In theft or hack in database, if the conformation codes are sent through the user mobile its saves all substantiation codes in databases. For hijacker it is easy to hack the databases and enter the code in pc so it's here security and protection altitude is low. On the other hand in two way communications it's also stored the user details in databases. But here, the hijacker will hack or theft the codes but not access because it's all access in user mobile [1].

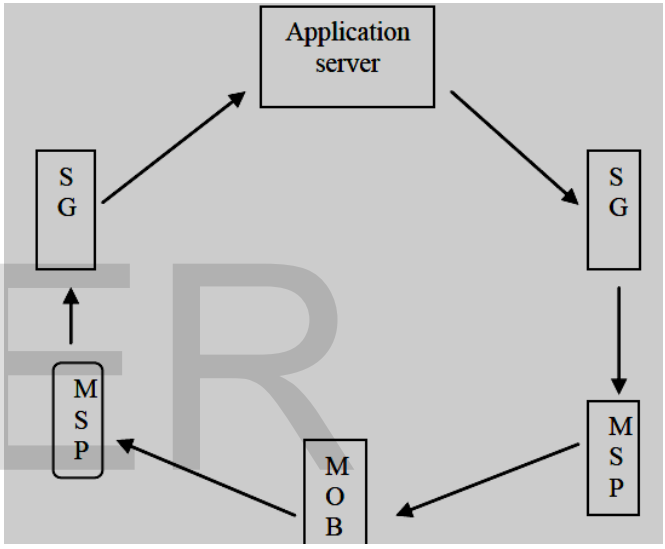

Figure 1: Two way communication basic operations [1].

A novel two-factor authentication scheme was proposed in [2]. In this scheme Bluetooth-enabled handheld device is used to enforce password-based authentication due to that improving convenience and usability.

They [3] suggested a mobile-based software token system that is supposed to replace existing hardware and computer-based software tokens. The technique implemented is secure and may contain three parts: software installed on the client's mobile phone.

In year 2012, Rosa Thomas presented The Decline and Dawn of Two-Factor Authentication on Smart Phones. When it comes to an authentication of a subject (e.g. a bank client) or even a message originated at this subject (e.g. payment order issued), there are three well-known factors that the verifier (e.g. the bank) can use to assure itself about the subject identity. By carefully combining several authentication factors together they can get two- or even three-factor schemes. In banking area, two-factor authentication schemes became de facto standard. Such schemes usually combine first and

second factor. In practice, the first factor is usually of a form of PIN or password that the client types, for instance, into a web-based internet banking application. The second factor is usually of a form of mobile phone that is known to be able to receive short messages directed to a particular mobile phone number. During authentication procedure, the bank generates a one-time password (OTP) and sends it via Short Messages Service (SMS) to that particular cell phone number. If the client is able to retype this OTP into the web application, the second authentication factor is regarded as successfully verified (i.e. the client has the mobile phone) [6].

This basic study was focused on a relatively small part of the whole information system (e.g. mobile banking) that is running on the client smart phone. There are several other parts of the system that already do actively contribute to its security. These can, sometimes, even compensate certain weaknesses of the mobile platform. Their discussion is, however, beyond the scope of this elaboration. Their aim was to investigate on how far we can effectively go right on the mobile device under very decent assumptions on its security. The conclusion is that the two-factor authentication with an adequate level of security is still achievable. On the other hand, it is definitely challenging task to design such mechanism securely. First of all, we have to fully understand the relevant threat model. Such a simple model was presented here with certain accent on so called after-theft attack [6].

Vinod Moreshwar Vaze [9] has proposed a new technique of authentication using one time private key. Here in this paper the generation of key is one time and as soon as the sender and the receiver uses this key it will automatically gets destroyed so that the storage cost is reduced as well as the chances of eaves dropping as well as different attacks as been reduced. It works similar to the digital signatures which can be used for the authentication of the sender and then receiver. The main advantages of key generation using OTPK is that the time complexity is reduced, storage cost gets reduced as well as prevention from various attacks sin the network also gets reduced.

4 PROPOSED METHODOLOGY

For strong authentication only Text based password is not enough sufficient for sensitive data transmission. Therefore as an alternative here we are using image base authentication along with one time password to secure two way communications. In our work we are using two way authentications for two way communication.

The proposed methodology works in the following phases:

1. This is registration phase, in this user registered himself by providing necessary information.
2. The server responds by generating otp and sends it to the user.
3. Sender enters otp and responds to server.
4. In this, client generates a master key and sends it to the server. Server generates the same master key and verifies the key (client).
5. Now, client will generate second master key using image and send it to server. Server will verify it.
6. Server check second factor by matching image keys.
7. Both the level of authentication has been passed by the user then client generate session key for communication.
8. Server establish the session between communicating parties.
9. After communication will be over the key generated get destroyed.

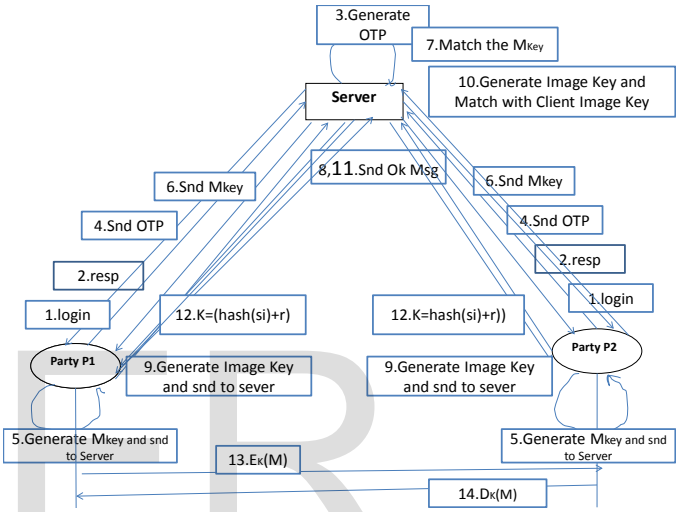

Figure 2. Working of proposed methodology

5 RESULT ANALYSIS

The security of the proposed methodology can be analyzed on the basis of certain security parameters.

Security Parameters	Prevention
Replay Attack	Yes
Man-in-the-middle Attack	Yes
DOS Attack	Yes
Confident ability	Yes
Password Impersonation	Yes
Dictionary Attack	Yes

Table 1. Analysis of the Security Prevention

Parameters	Existing Technique	Proposed Technique
Computational Overhead	high	Low
Computational Time	high	Low
Additional Security	NO	Yes
Attack Prevention	intermediate	high

Table 2. Comparative Analysis of Security issues

6 CONCLUSION & FUTURE WORK

Due to the growth of mobile users; many essential financial services are mobile based. So it is must to ensure the security of mobile applications. Many techniques are discovered in the field of mobile authentication. The proposed methodology implemented here provides more security as compared to other existing protocols implemented for mobile communication. The proposed work also provides less storage cost.

Although the technique implemented here for the authentication provides efficient results, but further enhancements can be done since during the key generation from images takes more computational time and also a three factor based authentication is implemented.

REFERENCES

[1] B. Shanmuga Sundari, G. Anusooya Devi and S. Shahina "Password Authentication System using New Intense Secure Algorithm in Mobile and Server in Two way Communications", International Journal of Computer Applications, ISSN: 0975 – 8887, Volume 75– No.2, August 2013.

[2] Roberto Di Pietro, Gianluigi Me, Maurizio A.Strangio "A Two – Factor Mobile Authentication Scheme for Secure Financial Transactions", International Conference on Mobile Business 2005.

[3] Aloul, Fadi, Syed Zahidi, and Wasim El-Hajj. "Multi Factor Authentication Using Mobile Phones", International Journal of Mathematics and Computer Science, vol. 4, pp. 65-80, 2009.

[4] Shi, Elaine, Yuan Niu, Markus Jakobsson, and Richard Chow. "Implicit authentication through learning user behavior." In Information Security, pp. 99-113. Springer Berlin Heidelberg, 2011.

[5] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin "Diversity in smartphone usage", In MobiSys, 2010.

[6] Rosa, Tomáš. "The Decline and Dawn of Two-Factor Authentication on Smart Phones." INFORMATION SECURITY SUMMIT, 2012.

[7] Anamika Chouksey, Yogadhar Pandey" An efficient password based two server authentication and pre-shared key exchange system using smart cards.",International journal of computer science and information technologies,Vol.4(1),2013,117-120.

[8] Vinod Moreshwar Vaze," Digital Signature on-line, One Time Private Key [OTPK]", International Journal of Scientific & Engineering Research, ISSN2229-5518, Volume 3, Issue 3, March -2012.

[9] Ram Ratan Ahirwal, Swarn Sanjay Sonwanshi"An efficient secure id based remote user authentication scheme using smart card" International journal of applied information system,foundation ofcomputer science vol1-No. 6,2012.