CHAPTER – 4

SECURED AUTHENTICATION PROTOCOL SYSTEM FOR MOBILE PHONES

4.1 Objectives

The evolution of mobile networks and terminals has changed the way of communication with people, increasingly able to stay in touch with greater mobility and flexibility than ever before. Mobile security is not simply a type of software or solution: it is a combination of solutions that together best meet the security policies and practices of the enterprise. Users and service bringers are slowly and steadily switching to PDAs and Mobile-phones for electronic commerce transactions. The key factor is the password security that is used for authentication. A simple graceful method called Secured
Authentication Protocol System for Mobile Phones (SAP-MOB) to solve the authentication problem in an omnipresent manner is presented. This work SAP-MOB survives all known attacks significant to this mode of authentication.

4.2 Introduction

Mobile and Wireless networks make people free from the tethers which had bound them to the fixed place in the past, and they also enable users to work more flexibly and conveniently.[JUNG08]. New mobile solutions must also integrate as easily as possible with existing enterprise IT infrastructures. If the enterprise requires higher security, add-on applications can be installed and deployed on mobile devices.[MOBI].

Today’s technically advanced cell phones are capable of not only receiving and placing phone calls, but storing data, buy and sell stock, surf the internet, money transfer and can even be used to manages the bank accounts. The state-of-art PDA (Personal Digital Assistance) and cell-phones are now as authoritative as Personal Computers. Current studies concuss report that very large number of cell-phones and PDAs are getting lost everyday.[HARR01, SUZA01].

The problem faced by the user is not only the loss of physical device, also but the valuable data and personal information that is stored in the device. The one and only way to prevent hackers by accessing the valuable information from the stolen device is to place a user authentication system. The widely used user authentication system for a mobile device is PIN (Personal Identification Number). In this PIN system, whenever the user wants to access the device, the user has to enter a 4 digit number. But this kind of authentication system is prone to
various kinds of attacks like guessing based on personal information, shoulder surfing and guessing based on keypad marks and man-in-the-middle attacks.

Vast majority of the cell-phones have ITU E 1.161 International Standard Keypad layout, which is shown in Figure 4.1. Entering password with this kind of keypad is difficult. Apart from the difficulty, password system is as vulnerable as PIN for all the mentioned attacks. One alternative to PIN and password is biometrics based user authentication. But generally validating a user’s identity in case of a biometrics based authentication system requires huge amount of computation power and extra hardware, which many not be available in most of the cell phones.[RAKE08].

![International Standard Keypad](image)

**Figure 4.1**: The ITU E 1.161 International Standard Keypad most widely used cell-phones keypad layout.

Now a days the most popular mobile devices like Black Berry, HTC, PDA and Smartphones support QWERTY keypad systems and Windows OS due to the technology innovations.

### 4.3 Various user Authentication mechanisms in Mobile Devices
Confidentiality, authentication, integrity, non-repudiation and access control are considered as the main services of a security system. Among these services authentication has been identified as the bottleneck. The compromise of the authentication service breaks down the whole security system, and we cannot proceed to provide the other services without the valid identities of communicating parts being successfully established.[ZHOU99]. Moreover, the protocols should be communication efficient with balanced load over the network.

Here considered three methods as Personal Identification Number method (PIN), Password method and Biometrics method as authentication mechanisms in mobile devices.

**4.3.1 Personal Identification Number Method (PIN)**

The most popular and widely accepted user authentication method for mobile device is PIN. The idea of PIN is almost similar to the traditional password system. Whenever the user wants to access his/her mobile, he/she has to enter a secret 4 digit number.

In HP Protect Tools Windows Mobile user have to choose their passwords on selection basis that makes hackers to guess the passwords on repetitive process.[HPPR05].

In eCommerce identification Mobile PIN an alternative to TAN lists, each user’s password will be assigned in a manner of PIN methods.[JURG02]. Decimalization table attacks for PIN cracking are performed using decimal encryption for the chosen user’s password. Users have to enter the same 4 digit password from his/her mobile as password.[MIKE03]. This make the hackers for easy guessable of keypad marks.
4.3.2 Password Method

Password is one possible alternative to authenticate user. The most popular and widely used keypad layout for cell-phones is ITU E 1.161 International Standard Key Pad. The main problem with the password schema in the mobile environment is the difficulty to enter the password by using the ITU E 1.161 International Standard Keypad.

For instance let us consider the user’s password as MOBILE. To enter this word using ITU E 1.161 International Standard Keypad, the user has to type 14 keys (1 time for M, 3 times for O, 2 times for B, 3 times for I, 3 times for L, 2 times for E). By typing 14 keys every time, to unlock the security system in mobile device is really difficult. To avoid these kind of overheads, the users will tend to pick passwords, which are having characters A, D, G, J, M, P, T, W (all the first characters in the keypad buttons), which makes it almost all similar to PIN methods.

4.3.3 Biometrics Method

Biometrics based user authentication provides more security for mobile devices than conventional PINs and passwords.[CLAR07]. Example of Cell-phones is represented in Figure 4.2.
Figure 4.2: Examples of Cell-phones, which are having inbuilt fingerprint reader.

Fig. 4.2a is the cell-phone, which is developed by applied biometrics and Fig. 4.2b is a PDA, demonstrated by Ericsson [W19] at CeBIT 2001.

But very powerful PDAs from HP [W17] and Ericsson [W18] have inbuilt fingerprint readers to authenticate the users before accessing the device. While retinal scan provides the highest crossover accuracy, its user acceptance is low, which makes it hard to introduce this authentication mechanism for daily life systems. [COLO02].

In [ALBA05], this system can identify the captured images send by the user to the remote server. Using this kind of process the malicious users can send duplicate images to the remote server which affects the total system. But security with biometrics for mobile devices will come really at a high price.

4.3.4 Drawbacks in Existing Methods and the Proposed Solution

➢ The system upon comparing the 4 digit secret word with the word that is stored in its database will either allow or deny the user to access the device in PIN method. Some of the problems that are associated with this mechanism are Brute-force attack, Shoulder surfing and guessing based on the keypad marks.

➢ In [KAZU08] user has to choose their password from the scrolling authentication panel. A hacker can view characters from the pre-indication part along with the arrow key moves. This is one of the reasons for password based authentication system not being used widely in the mobile environments.
It is rare to see Biometrics based user authentication system for mobile devices like PDAs and cell-phones. It is because Biometrics based authentication requires high computation power and extra hardware, which may not be available in most of the modern day cell-phones and PDAs.

In this work, a novel authentication system called Secured Authentication Protocol System for Mobile Phones (SAP-MOB) is presented, which is specially designed for mobile devices. It can be used in any mobile, which is having standard telephone keypad as in QWERTY keypad systems. The key features of this method are,

- The user can use it in a simple manner.
- It is impervious to all the known attacks.
- It doesn’t require high computation power.
- It doesn’t require extra hardware.
- It supports all Windows OS mobile devices.
- Due to images, the password can be easily remembered by the users.

This strategy is implemented to protect information from unauthorized confession and to provide mechanisms to authenticate mobile users.

### 4.4 Image Based Authentication System

The fundamental idea of SAP-MOB is based on premise that ‘humans are good at identifying, remembering and recollecting graphical patterns than text patterns’.[SHEP67]. The core devise of SAP-MOB is that, ‘Instead of remembering a sequence of characters as password, users have to remember a sequence of images as their password’.

124
Whenever the user wants to access the mobile, the SAP-MOB displays an N x N matrix of cells, which is known as Graphical image patterns. In each cell of the image pattern an index number is displayed, that is used to enter the passwords. The typical 3 x 3 graphical image pattern is represented in Figure 4.3a. For providing password the user has to enter the index number provided at the images. While entering index numbers in the password area, the numbers will be replaced by bullet marks. For example, if the user chooses images G O A then the index numbers 7, 4 and 8 should be entered in a selected order.

Figure 4.3a: A typical 3 x 3 Graphical Image Pattern is viewed when the user wants to access the mobile device. Fig. 4.3b. Confirmation of password in a shuffled manner.

While confirming password, images and index numbers were shuffled, so user has to re-enter the password by giving different index numbers according to the images chosen. According to the user’s choice now the user has to enter 8, 5 and 9 as index numbers while confirming password. It is represented in Figure 4.3b. Here both image patterns and index numbers are represented as dynamic arrangements in every login attempt. Due to this setup no
one would be able to read or guess the mechanism involved. The user can select the images on some sequences familiar to him/her. Due to shuffling mechanism, this method reduces the guess ability of the persons who are related to the users. During entry of password, only bullets appear in the password area which avoids the shoulder surfing attacks. When sending index numbers in the network plane, it will be converted into a computed Ascii value, so that Man-In-The-Middle attack is prohibited.

Each image will be mapped with a corresponding number which is stored in the Image-Map table. Instead of comparing the images, the mapped numbers are compared. It serves as user friendly for the end-user and machine friendly for the system by reducing the comparison time by using numbers rather than images. A mapping mechanism which validates the index numbers with hidden numbers is represented in Table 4.1.

<table>
<thead>
<tr>
<th>Image Numbers</th>
<th>Const Hidden Characters</th>
<th>Index Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Iteration 1</td>
</tr>
<tr>
<td>MI1</td>
<td>11</td>
<td>2</td>
</tr>
<tr>
<td>MI2</td>
<td>22</td>
<td>6</td>
</tr>
<tr>
<td>MI3</td>
<td>33</td>
<td>1</td>
</tr>
<tr>
<td>MI4</td>
<td>44</td>
<td>5</td>
</tr>
<tr>
<td>MI5</td>
<td>55</td>
<td>9</td>
</tr>
<tr>
<td>MI6</td>
<td>66</td>
<td>4</td>
</tr>
<tr>
<td>MI7</td>
<td>77</td>
<td>8</td>
</tr>
<tr>
<td>MI8</td>
<td>88</td>
<td>3</td>
</tr>
<tr>
<td>MI9</td>
<td>99</td>
<td>7</td>
</tr>
</tbody>
</table>

Table 4.1. A Sample Image-Map Mechanism for SAP-MOB

Using this mapping mechanism the shuffling process of images and index numbers are generated. The images are validated only by using the hidden characters and index numbers
which reduce the time complexity of comparing the images. The image positions are generated using permutation sequences. Let \( A = \{\text{MI}_1, \text{MI}_2, \text{MI}_3\} \), this set can be arranged in \( 3! \) ways as, 
\[
[\text{MI}_1] [\text{MI}_2] [\text{MI}_3], \quad [\text{MI}_1] [\text{MI}_3] [\text{MI}_2], \quad [\text{MI}_2] [\text{MI}_1] [\text{MI}_3], \quad [\text{MI}_2] [\text{MI}_3] [\text{MI}_1], \quad [\text{MI}_3] [\text{MI}_1] [\text{MI}_2], \quad [\text{MI}_3] [\text{MI}_2] [\text{MI}_1].
\]

For \( n \) images \( n! \) sequences were generated and it will be used randomly for every attempt of registration or login.

### 4.5 Security Potency of SAP-MOB

In general, several attacks are possible on an authentication system. For mobile devices, hackers can be classified into two groups; they are internal hackers and external hackers. Internal hackers are the people, whom the user knows. Whereas external hackers are the people, whom the user doesn’t know. Robbers are the best example for external hackers. These external hackers can do two different kinds of attacks on the mobile devices like PDAs and cell-phones, they are Brute force attack and guessing based on the keypad marking. Apart from these two attacks, the internal hacker can perform two more kinds of attacks. They are guessing based on personal information and Shoulder surfing attacks. In this section for security analysis, we compare the strengths of a 4 digit Personal Identification Number (PIN) with a 3 image password in SAP-MOB for 3 x 3 Graphical image pattern designs. [RAKE08].

1) **Brute force attack**

The hacker can try two kinds of Brute force attacks on the cell-phones / PDAs. The first way of attacking the system is to ignore the Graphical Image Patterns and try with some random numbers. Considering the case where the length of the password in Graphical Image Pattern is
3; for each log-in session there will be a unique 3 digit index number which will represent the correct password for that session. This password entry will be changed for every session according to the index number. In literature there is no known algorithm that can search a randomly changing string in polynomial time.

For better understanding of the system we will consider a simple case, where the password is a three digit index number. The probability of guessing the correct index number for the first time will be \(1/999\) i.e., 0.001. That means the probability of the failure will be 1-0.001, i.e., 0.999. If the guess was wrong, then the probability of the next guess being right will be \(1/998\). If we keep guessing the probability of failure will converge to zero at 999th attempt. Thus the correct password can be always guessed in a finite number of attempts.

In the case of SAP-MOB, this is not applicable because the cell-phone / PDA randomly change its Images and index numbers. If we consider the same example of 3 images as password, the probability of guessing the correct password in the first attempt will be \(1/x^3\) (where \(x\) is the number of possible numbers). But unlike in password system, the probability of guessing the correct password will remain \(1/x^3\). It is because for the cell-phone / PDA, password images will change for every attempt, which makes two guessing events independent of each other. Due to the independent nature of these events a Bruteforce attack will never converge.

The other way of performing a Bruteforce attack is to try all the combinations of images. For example, if we take a 5 x 5 Graphical Image Pattern there will be 253 different patterns of length 3. Hence the total possible number of Graphical Image Patterns is 16,525. If we consider the 4 digit PIN the total number of possible combinations is 10,000(104). Hence we can say that 3 image patterns is more secure than PIN, with respect to image based Bruteforce attack.
2) **Guessing based on the keypad marking:**

If a cell-phone has a PIN, every time the user must enter the same set of digits to access the resource. For a deeply used mobile, it is common that the color on the keypad will fadeout. If the hacker gets the mobile, then based on the keypad marks, he/she can easily find out the PIN digits that are become paler in the keypad. If the hacker gets the 4 digits that are in the user’s PIN, then the hacker has to try for 4! (i.e., 16 combinations to break the PIN). But in the case of SAP-MOB, the users have to enter their passwords in a dynamic manner. This makes SAP-MOB prohibited to Guessing based on the keypad markings.

3) **Guessing**

If the hacker knows all the personal information about the user, he can easily break the PIN by trying the number like the year of birth, house number, car number, etc. But in the case of SAP-MOB, it is very difficult to guess because the user selected the password which is a sequence of images based on some stories or family details.

4) **Shoulder surfing**

Shoulder surfing is looking over someone’s shoulder when they enter a password or a PIN code. It is an effective way to get information in crowded places because it is relatively easy to stand next to someone and watch as they fill out a form, enter a PIN number at an ATM machine, or use a calling card at a public pay phone. Shoulder surfing can also be done at a distance with the aid of binoculars or other vision-enhancing devices to know the password.
Shoulder surfing can be done easily on the password system, just by seeing the keys that the user is typing. But in the case of SAP-MOB, the hacker observes the key pressed by the user. Then hacker use to apply the same observed index numbers when they get the cell-phone / PDA in their hands. Due to shuffling mechanism incorporated in SAP-MOB the images and index numbers are shuffled and when the hacker enters the password digits as what he/she observed, it will give a wrong authentication request to the server. Comparison of attacks made with existing and proposed system is represented in Graph 4.1.

SAP-MOB, being a dynamic password system, is not vulnerable to Keylogger attack, Guessing based on Personal Information attack, Bruteforce attack, Shoulder Surfing attack, Guessing based on Keypad Mark attack and Database Server Compromise attack.
Even if the hacker gets the index number digits at first attempt he/she cannot reuse the digits to login to the system, because of the dynamic nature of the Graphical Image Pattern system.

4.6 System Design
The SAP-MOB totally encompass of four parts. They are SAP-MOB Core, Index number generator, Image Map Table and Authentication Database Server. The Block diagram is represented in Figure 4.4.

Figure 4.4: The Block diagram of the SAP-MOB encompass of four main parts. They are SAP-MOB Core, Index Number Generator, Image Map Table and Authentication Database Server.

SAP-MOB Core controls and monitors all the activities in the SAP-MOB. Index Number Generator generates the index numbers according to the number of digits considered for image patterns. Considering 3 x 3 image pattern there will be 9 images, for each image d digits (d = 1,2,3,…) is used. In Image Map Table, for n images n! sequences will be generated and it will be chosen at random. Authentication Database Server maintains the user’s information.

1) User Registration Phase

In user registration first the user wants to create a new Image password by making a request to SAP-MOB Core for authentication. Then the SAP-MOB Core acquires the 1st image set and 1st index number set from their appropriate places. After getting N² image patterns and index numbers (where N is the size of the Graphical Image Pattern matrix) the user has to enter
the 1\textsuperscript{st} set of Image password. The time-sequence diagram of the user registration phase is represented in the Figure 4.5.

If the user chooses three images as the Image password from 3 x 3 Graphical Image Pattern matrixes, he/she has to confirm the password from the 2\textsuperscript{nd} set of Image patterns and index numbers. This makes the user to get proficient with the Image patterns.

![Diagram of the user registration phase]

Generation of Image Password for the user
Validation and Verification Phase

Validation is performed in both user registration and user login phases. In user registration, by confirming password from the user both the 1\textsuperscript{st} and 2\textsuperscript{nd} set image passwords are verified. If any conflict occurred in verification process then user has to re-enter the confirmation password. Validation phase consists of two process; they are Tackle Phase and Respond Verification Phase. The step performed in tackle phase is from Image Map Table a set of $N^2$ images and from Index Number Generator a set of $N^2$ index numbers will be enfold and sent to user to tackle the user authentication status. It is represented in Figure 4.6.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{tackle_validation.png}
\caption{The Tackle Phase in the Validation process of User authentication system in SAP-MOB for User Registration.}
\end{figure}
In Respond Verification Phase the fetched password from the user through SAP-MOB core will be verified with the password stored at Authentication Database Server. It is represented in Figure 4.7.

**Figure 4.7: The Respond Verification Phase in the Validation process of User authentication system in SAP-MOB for User login.**

The steps involved in this phase is,

- User password at the time of registration will be encrypted and stored at the Authentication Database Server.
- User password at the time of login will be encrypted and it will be verified with the stored password at the Authentication Database Server.

Based on the result the SAP-MOB core will either allow or deny the user to access the device.

### 4.7 Implementation Results

In this new system all drawbacks of existing methods are overcome with new Secured Authentication Protocol System using Images for Mobile. This system is implemented in
Windows OS model PDAs/Cell-phones. Using Graphical Image Pattern method the user gets authenticated in User authentication system, which does not provide any repetitive methods for the user to not to get irritated. No leakage of information is possible in this new method which avoids guessing based on keypad marks and guessing based on personal information.

**Figure 4.8a**

**Figure 4.8b**

**Figure 4.8c**

**Figure 4.8d**

**Figure 4.8e**

*Figure 4.8: Different views of Graphical Image Patterns* **Fig. 4.8a.** Virtual keypad access in Pocket PC 2003 SE Emulator. **Fig. 4.8b.** User successfully added into the database. **Fig. 4.8c.**
In [RAKE08] the pattern followed makes the user more confused. Because the user have to choose the positions as secret code, but some of the positions have marked as same numbers (E.g. Number 2 is placed in 2 or 3 positions). This makes the user to get confused by choosing the same position twice makes the entry as twice the same number, which is marked as different positions as secret code. This drawback is overcome in proposed method by giving unique values as password entries even if the user chooses the same image twice. The proposed method is implemented and it is represented in Figure 4.8. For every authentication the images were shuffled and index numbers were varied and shuffled.

4.8 Conclusion

For an authentication mechanism to be considered effective, it must be unique and tamper-proof. In the present set up the user is not required to be physically attached to the authentication information. Possession of something that is not physically attached to the user can result in that the authentication information getting lost, stolen, or otherwise compromised. A novel method is presented for User authentication system in the mobile world. SAP-MOB is systematizing both in user and service provider planes. Our system is simple and easy to use and remembered by the user, even when the user has to remember several passwords. We have shown that SAP-MOB endure all known attacks in the mobile concord. Thus our system overcomes the problem encountered in existing systems and ensures the confidentiality and authentication in User Authentication System.