Mobile PassPattern System (MPPS)

Advanced User Authentication system for mobile devices

T. Rakesh Kumar
MS Scholar, Department of CSE
Indian Institute of Technology Madras
Chennai, India
rakeshk@cs.iitm.ernet.in

S. V. Raghavan
Professor, Department of CSE
Indian Institute of Technology Madras
Chennai, India
svr@cs.iitm.ernet.in

***Abstract*— Mobile handheld devices such as PDAs and Cell-phones are here to stay. Users and service providers are slowly and steadily switching to PDAs and Cell-phones for electronic commerce transactions. The key factor is security of the information such as password that is used for authentication. Besides, all identification related information follow the first authentication step. We propose a simple, yet elegant method called Mobile PassPattern System (MPPS) to solve the authentication problem in a ubiquitous manner. We have shown that MPPS withstands all known attacks relevant to this mode of authentication.**

Security; User Authentication; Mobile devices security;

I. INTRODUCTION

Reached 3.3 billion or half of the human population, makes the mobile phone the most widely spread technology and the most common gadget in the world. The ability to keep in touch with family, business associates, and access to email are a few of the reasons for the increasing importance of cell phones. 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 PDAs (Personal digital assistance) and cell-phones are now as powerful as a Personal computer. Recent studies concuss report that very large number of cell-phones and PDA are getting lost every day [2, 3]. The most disturbing thing to the user is not the loss of the physical device, but the data and personal information that is stored in the device.

The only way that one can prevent the others from accessing the data from a stolen device is to place a user authentication system. The widely used User Authentication for a mobile device is PIN (Personal Identification Number), the idea of PIN is fairly simple, when ever the user wants to access the device, the user have to enter a 4 digits 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. Apart from PIN, passwords can also be used as a user authentication method. Vast majority of the cell-phones have ITU E 1.161 International Standard Keypad layout, which is as shown in Fig 1. Entering password with this kind of keypad is really 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 the 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.

In this paper, we present a novel authentication system called Mobile PassPattern System (MPPS), which is specially designed for mobile devices. The key features of this method are,

- It can be used in any mobile, which is having standard 12-key telephone keypad.
- Very simple for the user to use.
- Immune to all known attacks.
- Doesn't require high computation power.
- Doesn't require extra Hardware.

II. STATE OF THE ART IN USER AUTHENTICATION FOR MOBILE DEVICES

In this section we are explaining various user authentication mechanisms that are used for mobile devices (cell-phones and PDAs).

A. PIN (Personal Identification Number)

The most popular and widely accepted user authentication method for mobile device is PIN (Personal identification number). The idea of PIN is almost similar to the traditional password system. When ever the user wants to access his/her mobile, he/she has to enter a secret 4 digit number. 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 access the device. The main advantage with this authentication method is, it is simple and it can be used with all mobile phones, which are having the standard 12-key telephone keypad. Some of the problems that are associated with this mechanism are bruteforce attack, shoulder surfing, guessing based on the keypad marks. In-depth security analyses of all the popular authentication systems are explained in section VI.

978-1-4244-2829-8/08/$25.00 ©2008 IEEE

B. *Password*

Password is one possible alternative to authenticate user. The most popular and widely used keypad layout for cell-phones is ITU [4] E 1.161 International Standard Key Pad.

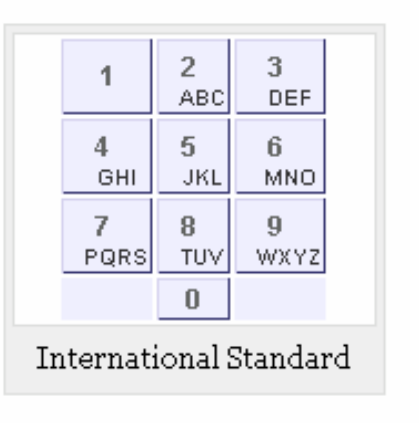

Figure 1. The ITU E 1.161 International Standard Keypad layout is most widely used cell-phones key pad layout.

The main problem with the password schema in the mobile environment is, it is difficult to enter the password by using the ITU E 1.161 International Standard keypad. For instance let us consider the user password as LINUX, to enter this word using ITU E 1.161 International Standard keypad, the user have to type 12 keys (3 times for L, 3 times for I, 2 times for N, 2 times for U and 2 times for X). But typing 12 keys every time to unlock (access) the mobile device is really difficult. This is the one of the reason why, password based authentication system is not widely used in the mobile environment. To avoid these kinds of over heads, the users will tend to pick passwords, which are having characters A, D, G, J, M, P, T and W (all the first characters in the keypad buttons), which makes it almost all similar to PIN (Personal Identification Number).

C. *Biometrics*

Biometrics based user authentication provides more security for mobile devices than conventional PINs and passwords [1].

But, 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. But very powerful PDAs from HP [9] and Ericsson [8] have inbuilt fingerprint readers to authentication the users before accessing the device. But security with biometrics for mobile devices will come at a really high price.

Figure 2. Examples of Cell-phones, which are having inbuilt fingerprint reader. Fig. 1.a is the cell-phone, which is developed by appliedbiometrics[7] and Fig. 1.b is a PDA, demonstrated by Ericsson[8] at CeBIT 2001.

D. *Motivation for Mobile PassPattern System (MPPS)*

The discussions hither to underline the need for an user authentication system, that is simple, easy-to-use, inexpensive, robust against attacks such as bruteforce, shoulder surfing, and all above doesn't demand any special hardware/software.

III. MOBILE PASSPATTERN SYSTEM (MPPS)

Mobile PassPattern System (MPPS) is a challenge-response system for mobile devices, which is based on PassPattern System (PPS)[6]. As PPS, MPPS is a user authentication system, which is primarily focuses on mobile devices like cell -phone and PDA's. The fundamental idea of MPPS is based on premise that 'humans are good at identifying, remembering and recollecting graphical patterns than text patterns' [5]. The core idea of Mobile PassPattern system is that, '*Instead of remembering a sequence of characters as the secret, users have to remember a shape (which is stored internally as a sequence of positions) as the secret*'.

Whenever the user wants to access the mobile, the MPPS displays an NxN matrix of cells, which is known as PatternSquare. Each cell in the PatternSquare is a number, as shown in Fig. 3. The PatternSquare is the challenge that is displayed by the device to the user.

1	2	0	8	5
7	1	7	3	6
4	8	3	4	1
5	2	0	9	5
7	9	6	5	3

Figure 3. A typical 5x5 PatternSquare that a user see when he want to access the device.

The PatternSquare will be generated dynamically upon each user request. Hence the number in each cell of the PatternSquare may change or their position may change or both, for every authentication request.

At the time of registration the user is asked to choose a sequence of positions as shown in Fig. 4, by typing the number in those positions. The sequence of positions then becomes the user's Mobile PassPattern (MPP). The cell sequence of the PassPattern so chosen will remain the secret between the user and the system

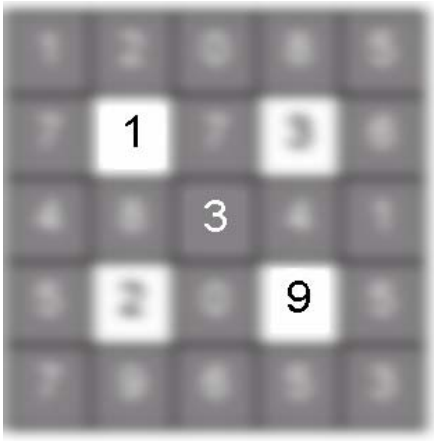

Figure 4. A example of a user selected Mobile PassPattern of length 3 position from a 5x5 PatternSquare.

The user has to remember only the shape (cell sequence in the PatternSquare) as that is the only secret. For the user to get authenticated, he/she has to type the numbers that are present in the chosen shape (Mobile PassPattern) in the PatternSquare. The cells in the PatternSquare are colored in such a way that, the user can easily remember his/her Mobile PassPattern (MPP). Whenever the user wants to access the device, the user has to type the sequence of numbers which appear in the user's PassPattern presented by the system as a challenge (This sequence of numbers that is entered by the user is referred to as Secretcode). During every presentation of the PatternSquare, the contents change and hence the user has to type a different SecretWord as shown in Fig. 5, during every authentication process such as login.

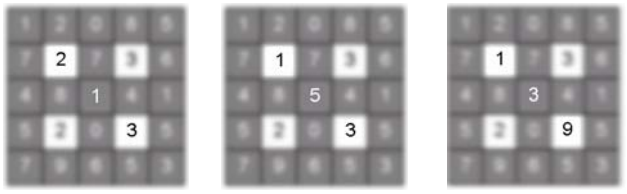

Figure 5. The above figure shows PatternSquares that are displayed to the users at different login attempts. Secretcodes corresponding to the Mobile PassPattern in Fig. 2 will be "213", "153" and "139".

The users can choose any set of position as their Mobile PassPattern (MPP). The user can select the Mobile PassPattern based on some sequences familiar to him/her, for example knight's moves on a chess board or some symmetric positions. Because of the coloring of the cells, remembering the Mobile PassPattern will be easy for the user. Some sample Mobile PassPatterns are given in Fig 6.

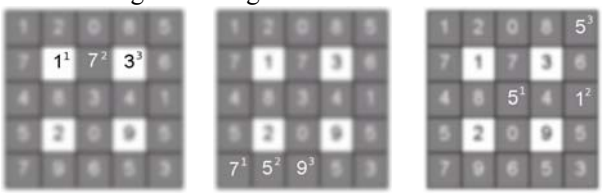

Figure 6. Some sample selections of Mobile PassPatterns. The corresponding SecretCodes to the user selected Mobile PassPatterns are 173, 759, 515.

IV. System Design

The Mobile PassPattern System totally comprises of three parts, they are, MPPS Core, Random number generator and Authentication database.

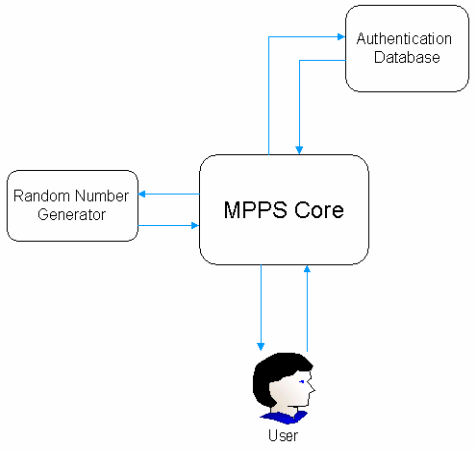

Figure 7. The Block diagram of the MPPS comprises of three main parts, they are MPPS Core, Random number generator and Authentication server.

MPPS Core controls and monitors all the activities in the MPPS. Random number generator generates the N^2 random numbers (N is the size of the PatternSquare) and sends all them to MPPS core. For the PatternSquare of size 5x5, the will be totally 25 cells. To fill this 25 cell, random number generator will randomly pick 5 numbers 2 times and other 5 numbers 3 times (5x2 + 5x3=25). Authentication Database contains the Mobile PassPattern of the user.

A. Registration Process

When ever the user wants to create the new Mobile PassPattern, the MPPS Core sends the current clock value of the mobile device to the random number generator. Based on the clock value, the random number generator will generate 25 2 digit numbers (for a 5x5 PatternSquare) and sends them to MPPS Core. Only at the time of registration process, the Random number generator generates 2 digit numbers. This is because the MPPS Core have to identify the locations that are selected by the user. The MPPS Core converts these 25 numbers into a PatternSquare and posts this as a challenge to

the user. The user has to select any three positions, by the typing the numbers that are there in his selected Mobile PassPattern (MPP). The same step is repeated for one more time, but with a different PatternSquare. The main idea of this is to avoid the typing errors (This is same as retyping the password or PIN). The time sequence diagram of the registration phases is as fallows,

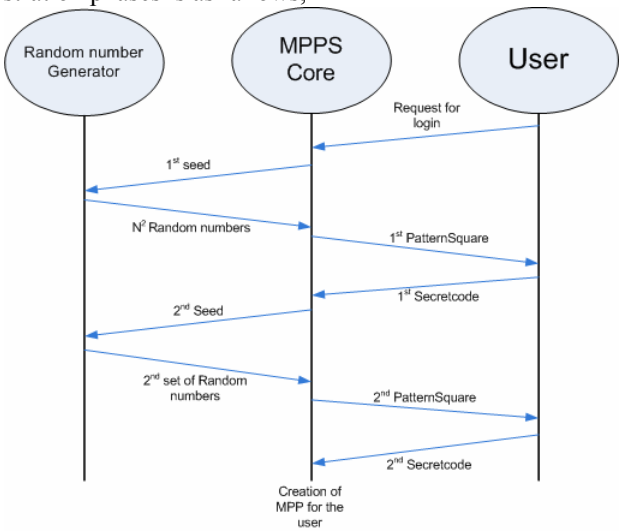

Figure 8. The Time-sequence diagram of the Registration process in Mobile PassPattern System (MPPS).

B. *Validation Process*

Validation Process consists of two phases; they are *Challenge Creation phase* and *Response Verification phase*. The first step in the Challenge Creation phase is, the MPPS Core sends the clock value as the seed to the Random number generator. Based on the seed value, Random number generator generates the 25 digits and sends them to the MPPS Core. Once MPPS Core gets the 25 digits, it will convert them to the PatternSquare and send it as a challenge to the user.

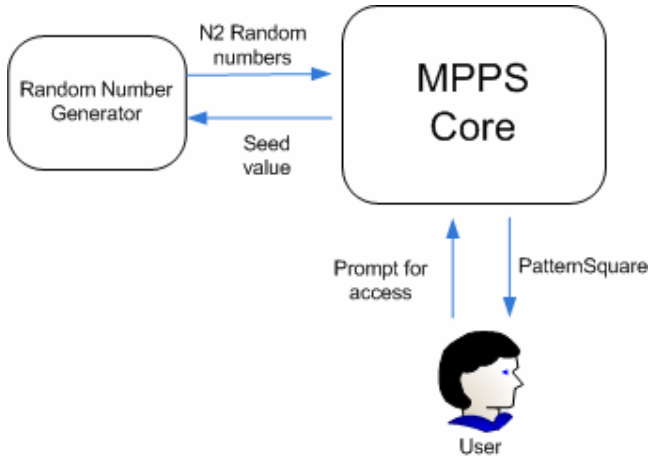

Figure 9. The Challenge Creation phase in the Validation process of user authentication in Mobile PassPattern System (MPPS).

Based on the PatternSquare and Mobile PassPattern (MPP) of the user, the user enters the Secretcode. MPPS core maps the Secretcode with the positions and compares them with the positions that are stored in the Authentication Database. Based on the result, the MPPS core will either allow or deny the user to access the device.

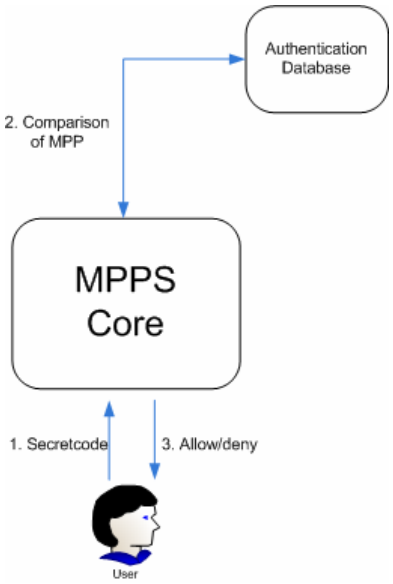

Figure 10. The Response Verification phase in the Validation process of user authentication in Mobile PassPattern System (MPPS).

V. SECURITY ANALYSIS

For mobile devises, hackers can be classified into two groups; they are internal hackers and external hackers. Internal hackers are the people, whom the user knows. Where as the external hackers are 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, they are Bruteforce 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.

In this section for security analysis, we compare the strengths of a 4 digit *Personal Identification Number (PIN)* with a 3 position *Mobile PassPattern (MPP)* in a 5x5 Pattern Square.

A. *Bruteforce attack*

The hacker can try two kinds of bruteforce attacks on the cell phones/PDAs. The first way of attacking the system is to ignore the Patternsquare and try with some random string. If we take the case where the length of the PassPattern is 3; for each log-in session there will be a unique 3 digit number which will represent the correct Secretcode for that session. This Secretcode will change every session. 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 number. The probability of guessing the correct 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.

Where as in the case of MPPS this is not applicable, because the cell phone will randomly change the Secretcode. If we consider the same example of 3-position PassPattern, the probability of guessing the correct word in the first attempt will be $1/x^3$ (where x is the number of possible numbers, 10). But unlike in password system, the probability of guessing the correct word will remain $1/x^3$. It is because; for the cell phone, Secretcode will change for every attempt, which makes two guessing events independent of each other. Due to the independent nature of these events a bruteforce search will never converge.

The other way of performing a bruteforce search is to try all the combinations of positions. For example, if we take a 5x5 Patternsquare there will be 25^3 different patterns of length 3. Hence the total possible number of PassPatterns is 16,525. If we consider the 4 digit PIN (Personal Identification Number), the total number of possible combinations are 10,000(10^4). Hence we can say that 3 position MobilePassPattern is more secure then PIN, with respect to position based bruteforce attack.

B. Guessing based on the keypad marking

If a cell-phone have a PIN (Personal Identification Number), every time the user must to enter the same set of digits to access the resource. For a heavily 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 can easily find the digits that are there in the user PIN. If the hacker gets the 4 digits that are their in the user PIN, then the hacker have to try 4! i.e., 16 combinations to break the PIN. But, in the case of Mobile PassPattern System, the users have to enter completely different numbers. This makes Mobile PassPattern system immune to Guessing based on the keypad marking.

C. 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, car number, etc. But in the case of Mobile PassPattern System, it is very unlikely that the user selected Mobile PassPattern is a shape, based on users family details.

D. 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 MPPS, even though the hacker observes the key pressed by the user, the hacker must find the location of that digit. As explained in the section V, each digit in PatternSquare will at least repeat twice and some digits may repeat even 3 times. Even tough the hacker gets the keystrokes and the PatternSquare; it is very difficult to guess the exact MPP of the user.

VI. CONCLUSION

In this paper, we presented MPPS – a novel method for authenticating a user in the mobile world. MPPS is configurable – both by the user and the service provider. MPPS Passpattern - equivalent of password - is simple and easy to remember, even when the user has to remember several Mobile PassPatterns. We have shown that MPPS withstand all known attacks in the mobile context. We are in the process of extending our work to understand user choices of Mobile PassPatterns and its impact on MPPS security, opening new vistas remaining unexplored.

REFERENCES

[1] N.L. Clarke, S.M. Furnell, "Advanced user authentication for mobile devices", Computers & Security, Volume 26, Issue 2, Pages 109-119, March 2007.

[2] V. Harrington, P. Mayhew, "Mobile phone theft", Home Office Research, Development and Statistics Directorate, December 2001.

[3] Suzanne Briscoe, "The Problem of Mobile Phone Theft", Contemporary Issues in Crime and Justice, Number 56, March 2001.

[4] International Telecommunication Union http://www.itu.int

[5] Shepard, R.N., "Recognition memory for words, sentences and pictures", Journal of verbal Learning and verbal Behavior 6, Pages 153-163, 1967.

[6] T. Rakesh Kumar, S. V. Raghavan, "PassPattern System (PPS): A Pattern-Based User Authentication Scheme", IFIP Networking 2008, Lecture Notes in Computer Science 4982, pp: 162-169, Springer Berlin / Heidelberg, May 2008, Singapore.

[7] Applied Biometrics Limited, http://www.appliedbiometrics.com.uk

[8] iPAQ Pocket PC, Smartphone, and Handheld Computer PDA, http://welcome.hp.com/country/us/en/prodserv/handheld.html

[9] Ericsson mobiles, http://www.ericsson.com