A Secure Pattern Based Near Field Authentication for P2P Systems

*1G.Dhanalakshmi, *2M.Akshaya, *3 V.Chetana, *4 P.Jayanthi

*1Associate Professor, Panimalar Institute of Technology, lakshmi3481@gmail.com
*2UG Student, Panimalar Institute of Technology, akshayamohan30@gmail.com
*3UG Student, Panimalar Institute of Technology, chethnavj@gmail.com
*4UG Student, Panimalar Institute of Technology, jaykrishnan95@gmail.com

Abstract— Authentication between two smartphone in close proximity is important. For example, when we transfer a file or image between two handheld devices via Bluetooth it must be transferred in a secured manner. This approach uses a pattern based authentication in which, when you pair a device with another device it will ask for a pattern and each time the pattern which we draw differs so that it cannot be predicted easily. The pattern is drawn simultaneously in two smartphone. Direct image matching is not efficient here because each smartphone size may get vary. So we use image processing technique. Here pattern is stored as an image in the phone storage and three process will take place namely crop, crisp and key generation. Each device will transfer the key to another device. QR-code is used to hide the key and another device can scan the QR-code from that device. This is to prevent the handheld devices from Man-In-The-Middle attack and to establish a secure connection between two devices in a shorter range of communication. And also to provide a close proximity authentication system which does not depend on NFC Chips.

Keywords –Smart device, QR Code Scanning, Device authentication, authenticated key exchange.

I. INTRODUCTION

This work is motivated by a common scenario of using smart devices. The idea of near field proximity authentication system is inspired by the observation that touch screens are now widely equipped by smart phone. The goal is to design a system that works on off-the-shelf smartphones and is able to authenticate whether two devices are in the near field. This is called near field proximity authentication (NFPA). We propose to use people on-screen finger movements to construct a near field proximity authentication system. Near field proximity authentication is to compel two smart phones to appear close together when the authentication is carried out. For Instance, Assume that Alice and Bob, carry their smart devices and meet each other in a public place. Alice is going to transfer some of their photos to Bob via the free public Wi-Fi provided by the public place. However, they want to do the transmission confidentially because the photos are private to them. Over the insecure public Wi-Fi, Alice and Bob need to set up a one-time cryptographic session key to protect their communications. In order to agree on a one-time session key, they should first invoke some key exchange (KE) protocol, such as Diffie-Hellman KE protocol. Since Alice and Bob are meeting in person, they can carry out a proximity authentication before executing the KE protocol to defend against Man-In-The-Middle (MITM) attacks. A mobile payment system may require that the proximity authentication can be implemented only if the smartphone and the cashier's POS terminal stay in the near field. The communication range of Bluetooth is between 1 meter and 100 meters cannot provide sufficient granularity. Recall that function of an NFPA system is to ensure that the two smartphones are in the near field when the authentication succeeds.

With the widespread usage of smart devices, we will see an increasing number of demands for NFPA. As mentioned above, mobile payment is one example. Another example is to establish a one-time usage secure channel for two smartphones. Secure file transmission between two devices is an example. The physical close proximity ensured by NFPA provides another layer of the security assurance to these application scenarios. It is because the physical proximity implies that the application progress is under smart phone owner's supervision. We believe that more applications will benefit from NFPA. Constructing NFPA system on top of NFC is a natural choice. However, as mentioned previously, NFC system is not available on many smartphones. Therefore, it is necessary to construct an NFPA system compatible for smart devices without NFC chips.

II. EXISTING SYSTEM

The Man-In-The-Middle attack is the major threat for handheld devices to agree a session key in which they do not share any prior secret in advance, even if these devices are physically located in the same place. Insecurely typing passwords into handheld devices or comparing long hexadecimal keys displayed on the devices screen, many other human-verifiable protocols have been proposed in the literature to solve the problem. Most of these schemes are non-scalable to more users.

Taking password based protocols used in Bluetooth For example, two users input the same password of four to eight digits in both handheld devices. Passwords are usually poorly chosen by human it is easily predictable and an adversary may oversee the devices screen and key pad using a hidden camera or a telescope while the user keying the password.

It is also impractical to require every handheld device to register a public key from a certificate authority. Moreover, to avoid the MITM attack in directly sending public key to another device, the device owners need to assert the integrity of the public key. Comparing two long strings is also a difficult task for human beings. Therefore, public key based solutions are also not applicable to this environment. An MITM attacker is difficult to attack the communication carried out by an NFC system. However, Current NFC systems depend on NFC Chips, which are not available on many smart devices.

III. RELATED WORK

Proximity authentication authenticates whether two devices are in geographic proximity. However, the range of a proximity authentication can be as large as tens of meters. NFPA constricts this range to several centimetres, i.e. near field. In other words, when an NFPA is passed, the two devices should be less than a few centimetres apart. Motivated by this work, Balfanz et al. [1] proposed the concept of location-limited channel, over which users carry out the authentication process. The transmission range of the channel in their work could be from centimetres to meters. In addition, the authors of [1] used infrared as their location-limited channel, which is not available on many smart devices. the trusted centre scheme is not a suitable choice either, because Internet access is not always available when two people want to perform authentication on their smart devices. In the meantime, it is difficult to derive the same session key from one bump hit due to high oscillation in the measured data of accelerometer. Some works [2], [3], [5], [6] proposed to use the accelerometer data captured during the period of time when a person is shaking two smartphones. Mayrhofer and Gellersen [2] used a signal processing approach to remove the differences between sensed data sets in order to generate a shared session key. The protocols in [2] do not need a trusted center. The problem of shake based approaches is that it is difficult to hold and shake a big device. Kumar et al. presented another survey paper [4] focusing on secure device pairing.They implemented the surveyed pairing approaches on the same platform to conduct a comprehensive and comparative field study. Studer et al. [3] proposed an MITM attack against those motion based approaches. They assumed that there is a powerful adversary who can observe the user's motion, such as shake or bump, so that he can

emulate a similar motion pattern to carry out an MITM attack. While the success rate of their attack was sensitive to the delay induced by the attacker, their work suggests that a slighter movement is preferred than shake and bump when a third person is standing nearby. Finger movement is such a slight movement that is easily hidden from observations of strangers. In order to defend against MITM attacks, some prior studies suggested to use human comparison after the secret exchange, because an attacker cannot change the output on the device screen.

IV. PROPOSED SYSTEM

We propose a close proximity authentication near field proximity authentication (NFPA) that is able to authenticate whether two devices are in the near field and to establish secure transaction using a temporary confidential channel using a secret key. The idea behind our approach is inspired by the observation that touch screens are now widely equipped by smart devices. Therefore, we propose to use people on-screen finger movements to construct a near field proximity authentication system. In order to force two smart devices to stay close to each other, we let a person move two fingers of one hand, usually the index finger and the middle finger simultaneously on the two smart device screens.

The reason we use this motion is that it is easy and natural to perform and it produces sufficient variations in terms of the sensed data. The more variations the data has, the more difficult it is for an attacker to carry out a dictionary attack. Since the two finger movements are done by one hand, they are highly coherent to each other. We leverage this coherence to generate the session key for the two smart devices. A near field proximity authentication (NFPA) system is a mutual proximity authentication system between two parties.

For Authenticating two mobile devices we use QR code Technology for key transfer from one Mobile to another. Based on the Key generated from the Pattern drawn in one mobile device, the other will authenticate while receiving the key through QR Recognition. Then the device will check for the Percentage of Correctness in patterns drawn in two mobile devices .If the matching accuracy is more than 70% means pairing will be done between devices and data transfer can be done by encrypting the data using session key generated.

V. PRATICAL IMPLEMENTATION

A) Human Verifiable Pairing

Here we give a same signature to both devices, with the help of that we store the signature in SD card as an image in a way that a both devices ensures a new confidential pairing methodology. Two mobile devices whichever needs to share a confidential information is placed side by side in close proximity and a pattern is drawn using two fingers of one human. The generated patterns are saved as a jpeg image on the SD Card of the mobile in which it is drawn. After that we use the java image processing, to crop the image where the signature is drawn based on that image pixel scanning.

B) Image Processing and Key Generation

Here Image processing techniques is used, because Direct Image Matching Strategies will not work out. The Direct Image Matching Techniques will not be employed Owing to the following constrains. As the Screen size differs for both the mobile devices, As the screen Resolution might also be different leading to pixel deviation and As the Pattern drawn in both the handheld devices might occupy different position. This Constrains restrict the process to be compared for Direct Image Comparison. So we proposed a new strategy to compare the Images using Image Processing techniques in java. A key will be generated based on the patterns drawn on either of the mobiles. Our Novel approach to extract a key from the pattern that follows pixel manipulations which will be done after crisping the particular portion of the Image manipulating threshold. Shake points or Trim points is calculated based on the curves in the image and the key points were calculated and manipulated forming a unique key.

C) QR-code generation and communication device

The Extracted Key is then exchanged to other device without the possibility of Man-In-The-Middle Attack by embedding it into a QR Image and a data can be transferred in a Human verifiable manner. Only if both the keys are matched for optimal accuracy a secret channel is created by a common agreed parameter and the successful pairing involves file sharing that is encrypted and send as chunk by chunk and can be decrypted by the other.

In Our approach , on average the sender spends less than one second on encoding key into QR-code, less than one second on sending packet through wireless network, and one second on AES encryption. On the other side, the receiver spends about three seconds on decoding key and less than one second on decrypting and verifying message.

VI. SECURITY ANALYSIS

A) Shoulder Surfing Attack

Shoulder surfing attack refers to issuing direct observation techniques, such as looking over someone's shoulder, to receive information. It is commonly used to obtain passwords, PINs, security codes, and similar data (e.g. Entering PIN in ATM machine).In the proposed system, a new PIN-entry method is used. The basic layout of our method comprises a vertical array of digits from 0 to 9, with another array at adjacent of ten familiar objects such as + and / etc. For simplicity, we assume the number of digits in a PIN is four, and the proposed method may be applied to any case with $N \geq 2$ digits. There are a total of four rounds. The first round is the session key decision round and the remaining rounds are PIN-entry rounds. In session key decision round, ten randomly arranged symbols are displayed to the users. The user recognizes the symbol immediately below the first digit of his/her PIN as temporary session key and presses “OK.” In the example shown where the PIN is 3712, the user recognizes symbol as the session key because it is collocated with the first digit of the PIN, 3. The remaining rounds are PIN-entry rounds, in which the ith digit of the PIN is entered in i th round for i = 2, 3, 4. In each rounds, the user is again given a random array of ten symbols, and he/she enters a PIN digit by rotating object array and aligning the session key with the current PIN digit. For this task, the user can use two additional Buttons (“Left” and “Right”) to align the symbol with current PIN digit.

B) Man-In-The-Middle Attack

A Man-In-The-Middle attack is a type of cyber-attack where a malicious actor or the intruder inserts him/herself into a conversation between two parties, impersonates both the parties and gains access to information that the two parties were trying to send to each other.We have avoided the man in the middle attack by which server generates the 6 digit binary value.The user enters a PIN digit by rotating the object array and aligning the session key with the current PIN digit.Hence the intruders will receive only the six series of ten symbols ,but not the original password.

VII. CONCLUSION

Thus we design and developed a Pattern based mutual Near Field Proximity Authentication (NFPA) for safe and secure data dissemination eliminating MITM and Shoulder Surfing Attacks in insecure public networks between peer devices using QR Code Technology. We justify our system to be stable secure time efficient and reliable under pairing of any Android devices.

VIII. REFERENCES

[1]. D. Balfanz, D. K. Smetters, P. Stewart, and H. C. Wong, "Talking to strangers: Authentication in ad-hoc wireless networks," in NDSS, 2002.

[2]. R. Mayrhofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," IEEE Trans. Mob. Comput., vol. 8, no. 6, pp. 792–806, 2009.

[3]. A. Studer, T. Passaro, and L. Bauer, "Don't bump, shake on it: the exploitation of a popular accelerometer-based smart phone exchange and its secure replacement," in Proceedings of the 27th Annual Computer Security Applications Conference. ACM, 2011, pp. 333–342.

[4]. A. Kumar, N. Saxena, G. Tsudik, and E. Uzun, "A comparative study of secure device pairing methods," Pervasive and Mobile Computing, vol. 5, no. 6, pp. 734–749, 2009.

[5].C.Castelluccia and P. Mutaf, "Shake them up!: a movement based pairing protocol for cpu-constrained devices," in ACM MobiSys, 2005, pp. 51–64.

[6]. L. E. Holmquist, F. Mattern, B. Schiele, P. Alahuhta, M. Beigl, and H.-W. Gellersen, "Smart-its friends: A technique for users to easily establish connections between smart artefacts," in Ubicomp, 2001, pp. 116–122.