THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

A Review of Near Field Authentication for Smart Devices

Ninad Khalate
BE Computer Engineering department
St. Francis Institute of Technology, Mumbai, Maharashtra, India
Raisa D'monte
BE Computer Engineering department
St. Francis Institute of Technology, Mumbai, Maharashtra, India
Craig Noronha
BE Computer Engineering department
St. Francis Institute of Technology, Mumbai, Maharashtra, India

Abstract:
NFC (Near Field Communication) chip has enabled smart devices available in the market to exchange information quickly between two devices, but in the process compromising on the security front, this lacking feature thereby inhibits the use of NFC. NFA (Near Field Authentication) poses as an alternative to NFC. NFA aims to fulfil the purpose of NFC for all smart devices without using NFC chips. Currently there seems to be no application available in the market that uses NFA. We as a team are motivated to build an Android application. We propose a system that uses human finger- movement to authenticate a connection between two devices in proximity of each other.

Keywords*: NFA, NFC, Near Field Authentication, BUMP, Bluetooth*

1. Introduction

Upondoinga thorough literature review we came to a conclusion that there in an inherentlack of applications that provide secure transmission of data. Also the number of smart devices embedded with NFC [7] chips in miniscule. Due to lack of security use of traditional Bluetooth method for data transmission is dwindling. The man in the middle attack is mainly responsible for low security of these methods. Near Field Authentication aims to overcome this security issues and generate a high entropy session key which establishes a connection between two devices which are in close proximity.

1.1. Key Exchange Protocols

The key exchange protocol used where derived from existing Diffie-Hellman KE protocol[3]. The two participants will generate their own one time use session keys using hash functions on the data set obtained from the pattern. Then this data set is encrypted using the public key encryption for which they use their own session key and the this encrypted data is exchanged. Both the participants then decrypt the received data make modification and send it back after encrypting it again. On receiving the data back they then decrypt it and realise the modification which has been pre approved. Thus they validate and authorise the connrction.

1.2. MITM

A Man-in-the-Middle (MITM) attack is a type of spoofing attack, where a person impersonates another person or program. Two users wanting to communicate with each other, decide upon an encryption algorithm and key to be used. After key exchange, the attacker present from the beginning can modify or decrypt the communication between the users.A MITM attack consists of a fully malicious adversary, who has access to the public communication channels. The attacker in an ideal situation, can eavesdrop any communication, tamper, delay, inject and block messages.The purpose of the adversary in this work is to obtain the session key generated by a NFA system without being captured, so that he can decrypt and obtain the succeeding communication messages.

2. Literature Review

2.1. Bluetooth

As bluetooth-capable devices come within range of one another, an electronic conversation takes place to determine whether they have data to share or whether one needs to control the other. The electronic conversation happens on its own, the user doesn't have to press a button or give a command.Once the conversation is established, Bluetooth systems create a personal-area network (PAN)[2], or **piconet**, that may fill a room or may encompass no more distance than that between the cell phone on a belt-clip and the headset on your head. Once a piconet is established, the members randomly hop frequencies in unison so they stay in touch

with one another and avoid other piconets that may be operating in the same room[2]. Bluetooth being convSSSenient is very vulnerable to MITM. Also once two devices are connected using Bluetooth they are paired that is remembered and not authorised the next time. This attracts the attacking adversary.

2.2. BUMP

The BUMP[4] application uses an accelerometer to establish a connection between two smart-phones enabling transmission of data. The BUMP system connects the two devices wanting to exchange data by comparing the data extracted during a bump between the two participating devices. The security and efficiency provided by the BUMP application depends entirely on its server, which is assumed as a trusted center. This however can prove to be a drawback, as the server itself may suffer from single-point- of-failure problem [5]. Internet accessibility is another con to this approach, as the app requires internet connection to match with another device and internet accessibility is not always available.

2.3. System Model

As one of the user draws a pattern using his index and middle finger he starts the authentication process. The first step involves feature extraction of the pattern on the individual screens of the users.The two devices interact with each other using the extracted feature sets and generate a similar session key. Finally, the two devices can establish a higher level communication by verifying that the session key acquired by both the devices is identical.

2.4. Feature Design

A zigzag movement formsaseriesofcurves,whichprovide many features to be extracted [1]. The time elapsed between the start point and every peak point is extracted. The starting point is the point where a finger touches the screen first and peak points are the points where the pattern direction changes. A time value collected by touch screen is accurate to 10^{-6}second [1];this high accuracy also leads to high sensitiveness and low robustness. After rounding the time value the decimal point values are dropped to get just the integer part.

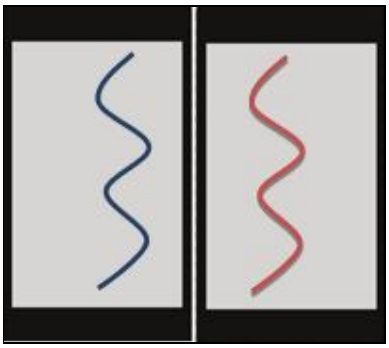

Figure 1: Finger drawn patterns example

2.5. Performance Analysis

Given a pair of peak points, it is considered to be a valid paper, if their value difference is less than 3. 70% of the considered pairs are found to be valid using NFA. The failure probability of the system is affected by the number of elements in the feature set, m. Given m and the proportion of valid pairs, the success probability of the reconciliation phase can easily be calculated. Consider, if the number of selected values is greater than 7 and the proportion is more than 70%, the success probability is more than 98% [2].

2.6. Security Analysis

Most of the attacks in a Near Field system come in the form of MITM attacks and dictionary attacks. When the two devices derive their respective one time use session keys they use the data set of the pattern drawn on them. Thus to intercept the on going interaction the attacking adversary must compulsorily have the exact data set as of both the devices. And that is very difficult to achieve by drawing the pattern explicitly. Here the fact that the patterns on both the devices been drawn by the fingers of the same hand is proved worth.That the explicitly drawn pattern can't possibly as coherent as drawn by the fingers of the same hand. Also a very low threshold has been set for the margin of error thus even the slightest difference between the pattern would lead to detection of an attacker. Also this authentication process takes place between the two devices every time a connection is to be established and every time a new set of pattern derived session keys are used making it more robust.

3. Gaps Identified from Literature Review

On reviewing various papers we understood that though the concept of establishing a connection between two devicesusing NFA is far more efficient and secure but it has never been implemented on the android platform. We propose that as android platform is vastly used to transfer data anapplication based on NFA will be of great value. We propose the following system:

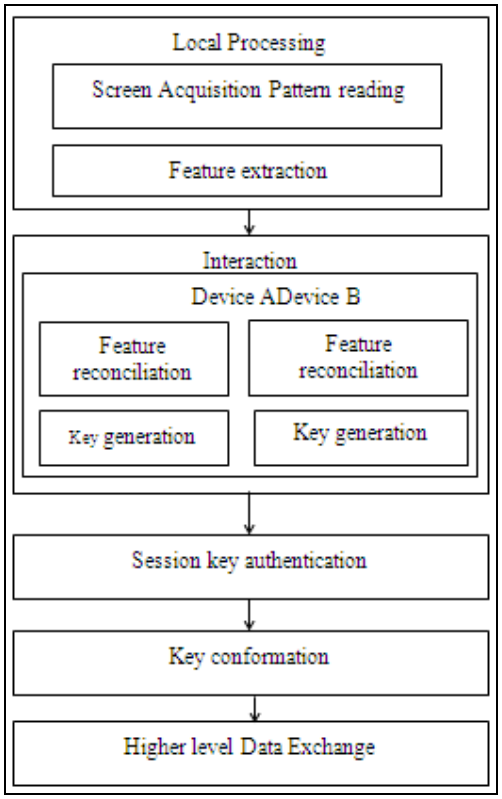

Figure 2: System Architecture

3.1. Velocity aspect

The existing NFA system uses the elapsed time sets on both the devices. Upon studying android programming, we found that the android platform allows us to use a velocity aspect which will help us in getting more precision. We aim to use this function to record the velocities of the patterns drawn on the individual screen and then comparing them. If verified we carry on with the further algorithm [6]. This velocity aspect allows us to add an extra layer of security.

3.2. Information exchange application:

We propose to develop an application using android programming that uses the NFA system for key exchange and generation and establishment of connection. We aim to develop an application that will enable the user to send data such as documents, images, audio and video in a secure environment.

4. References

1. Lingjun Li, Xinxin Zhao, Guoliang Xue, "Near Field Authentication for Smart Devices " , 2013 Proceedings IEEE INFOCOM,pp 375-379.
2. Bluetooth [Online]Available:http://electronics.howstuffworks.com/bluetooth2.html
3. M. Abdalla and D. Pointcheval, "Simple password-based encryptedkey exchange protocols," in CT-RSA, 2005, pp. 191–208.
4. BUMP TECHNOLOGIES. [Online]. Available: http://bump..
5. G. Lynch, Single Point of Failure: The Ten Essential Laws of Supply Chain Risk Management. Wiley, 2009.
6. S. Jarecki and X. Liu, "Fast secure computation of set inter- section," in SCN, 2010, pp. 418–435.
7. Near Field Technology [Online]Available: http://www.nearfieldcommunication.org/