Secure Authentication for ATM transactions using NFC technology

Divyans Mahansaria
Dept. of Information Technology
Jadavpur University
Kolkata, India
divyansmahansaria@gmail.com

Uttam Kumar Roy
Dept. of Information Technology
Jadavpur University
Kolkata, India
royuttam@gmail.com

Abstract— **Automated Teller Machine (ATM) is a convenient way to meet the banking needs of the users. However, the use of debit card or other types of cards during ATM transactions has some problems like prone to ATM skimming, magnetic strips of card getting damaged, manufacturing and transportation cost of cards, longer time to authenticate users etc.**

The objective of this research is to consider smart phone in Near-Field Communication (NFC) Card Emulation mode as an alternative to ATM cards. In NFC the distance between the respective devices needs to be very small (typically less than 4 cm) which makes NFC ideal for making payments and for other transactions involving sensitive/private data. In the proposed system, in order to authenticate at the ATM kiosk, the user needs to swipe his/her smart phone in front of the NFC reader. An ATM card is not required for authentication and the system will still have a stronger security compared to the system in which ATM card was used. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

Keywords— Secure Authentication, ATM, One Time Password, Near Field Communication, Security Attacks.

I. INTRODUCTION

Automated Teller Machines (ATMs) play a vital role in providing the people easy access to cash and carry out other banking activities. Thus, it is of paramount importance to safeguard users and provide them convenience while transacting using ATM. Physical ATM cards along with Personal Identification Number (PIN) are in widespread use all around the globe to authenticate at ATM kiosks. However, there are some issues on the use of physical cards during ATM transactions. First, ATM skimming resulting to theft of card information and subsequently card cloning (even for chip based cards) has become a burning issue nowadays. Second the magnetic strip/chip used in the cards get damaged and become non-functional due to repeated usage. Third, manufacturing large number of cards and transporting them to the end users involve considerable cost. Fourth, physical cards require relatively longer time to authenticate users leading to long queue at the ATM kiosks.

Near-Field Communication (NFC) is a method that enables two electronic devices (or a device and a NFC Tag) to establish communication, by bringing them close to each other. NFC has advantages over Bluetooth, Radio Frequency Identification (RFID) and other communication technologies to carry out secure transactions. One of the advantages is that NFC tag doesn't need a power source – it is passive and is simply read or written to by the powered terminal. A Bluetooth tag requires power to broadcast its signal. Radio Frequency (RF) from another Bluetooth device is by far not enough to power a Bluetooth radio chip. Another advantage of using NFC is that for NFC technology to work, the distance between the respective devices needs to be very small (less than 4 cm). In case of Bluetooth, the data theft may occur because of the long distance (even up to 100 meters) provision for the data transfer. This makes NFC ideal for making payments and for other transactions involving sensitive/private data. NFC is faster and easier to set up than Bluetooth connection. Unlike RFID which enables a one way wireless communication typically between an unpowered RFID tag and a powered RFID reader, NFC is capable of two way communication and can therefore be used for more complex interactions such as card emulation and peer-to-peer (P2P) sharing.

Some of the research work proposes different types of financial applications based on NFC. One of the applications of NFC technology is in contactless payment operation. An NFC purchase transaction between an NFC smartphone (or an NFC bank card) and an NFC point of sale terminal is performed instantaneously and within a short range of communication (around 10 centimeters) without any physical contact [6]. A. Meschtscherjakov etal. [2] proposed an application called MyPocketATM which includes services such as Balance Reader, Currency Check, ATM Info and others. Balance Reader visualizes the balance of a bank account; Currency Check displays the actual value of foreign banknotes in the home currency and ATM Info could check fees of NFC-tagged ATMs.

The objective of our proposed work is to replace physical ATM cards by smart phones in NFC Card Emulation mode during an ATM transaction to counter the issues prevalent with the use of ATM cards. The combination of NFC with smart devices has led to widening the utilization range of NFC. In card-emulation mode, a NFC device behaves like a contactless smart card. In this mode, the mobile phone does not generate its own RF field; the NFC reader creates this field instead. At the ATM kiosk, in order to authenticate, the user needs to swipe his/her mobile phone in front of the NFC reader. During an ATM transaction, an ATM card is not required and the system will still have a stronger security compared to the system in which ATM card was used. Through data encryption

This work is partially supported by the project entitled "QR code-based Multi-Factor Authentication Using Mobile OTP and Multi-dimensional Infinite Hash Chains" under RUSA 2.0 (Ref. No. R-11/668/19)

978-1-7281-1576-4/19/$31.00 ©2019 IEEE

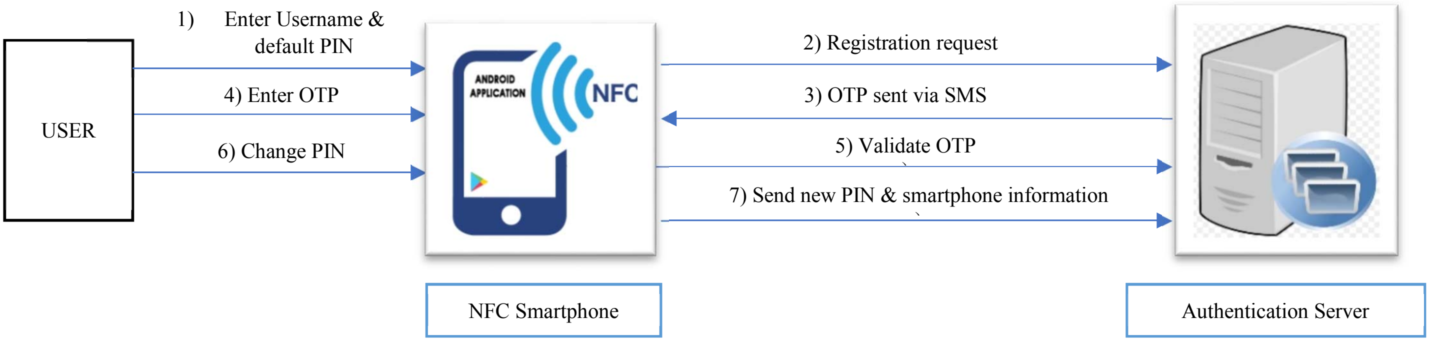

Fig. 1. Registration Phase

and secure channels, NFC technology keeps the customer information safe. Security analysis and threat modelling shown in this paper highlights the security strength of the system during authentication.

II. RELATED WORKS

To carry out secure ATM transactions a NFC enabled solution was proposed by Mandalapu etal. [1]. Here, the first level of authentication involves ATM card swiping or manual ATM card number entry. The successive process features the use of an NFC enabled cell phone having access to Internet. The user is required to tap the cell phone on the NFC tag fixed on the ATM. The tapping opens up a webpage on the mobile phone's browser and requests for a pre-registered phone number as a user input. Following this step, the user is required to enter a Pattern Password that was previously registered online during the registration process to use NFC. The pattern password appears as a random set of numbers. The OTP is then generated on a subsequent page. This OTP needs to be entered on the ATM's screen before a preset timeout. Some of the drawbacks of the solution are the requirement of ATM card to carry out ATM transactions, a need to remember the pattern password and an increase in authentication duration at ATM kiosks.

H Lee etal. [3] has proposed an authentication solution using digital signature and NFC card emulation on android. In this solution the mobile device of the user saves the server information together with the private key and the server stores the mobile device UUID and the corresponding public key. During authentication the server returns a nonce, which includes the server info, a time-stamp, and a fixed length of random bits, to the client. The NFC reader will then start to scan for NFC cards as soon as the client receives the nonce. The user has to swipe his/her mobile device at the NFC reader in 30 seconds once the reader starts scanning. Before the mobile device can communicate with the NFC reader, the user should execute the card emulation application and enter the PIN code. The mobile device signs the nonce with the corresponding private key and sends its UUID together with the signed nonce to the reader. The client then passes the message received from the mobile device to the server for verification. The usefulness of this solution compared to traditional password based authentication has been highlighted in the research. However, the solution has certain drawbacks. The need to store a private key securely and computation of digital signature in the mobile device during each authentication is an additional overhead. The private key would be server specific and hence for each new website/application different private keys needs to be stored by the mobile device.

R.M. Ranasinghe etal. [4] has proposed the design of a devise that functions as a RFID or NFC tag with fingerprint authentication to overcome some of the security risks with the use of RFID and NFC technologies. To input data into the device, the user must select the data input option (new set of data or to update existing data). To output data from the device, the output data option is selected. After the input or output selection, the fingerprint authentication process is carried out. Data is exchanged between the device and NFC/RFID reader or writer via RF signal only after the validation of the fingerprint. The major drawback of this proposal is the need to carry an extra device by the user. The device is sophisticated comprising power input source, display screen, navigation buttons, fingerprint scanner, battery, antenna, storage etc.

S. Sridharan etal. [5] has proposed connection of ATM network to public domain to facilitate transactions with third party applications using the ATM terminals. NFC is proposed to be used where in the user, after inserting ATM Card, would communicate via only their NFC enabled mobile phones. However, there are issues with the proposed work. The use of NFC as a communication medium with ATM terminal is not significantly justified. The third party applications need to store confidential information of ATM card details and user's mobile number. Moreover, reserving NFC spectrum band to the government and establishment of jammer signal around all the ATM terminals are an additional overhead.

Our proposed solution detailed in section III of this paper uses NFC technology to secure ATM transactions without the need of a physical ATM card. It does not have the issues prevalent in the above related works.

III. PROPOSED SOLUTION

In this section, the working principle of the solution is described in details. For a better understanding, we divide the solution into two phases: *registration and authentication*.

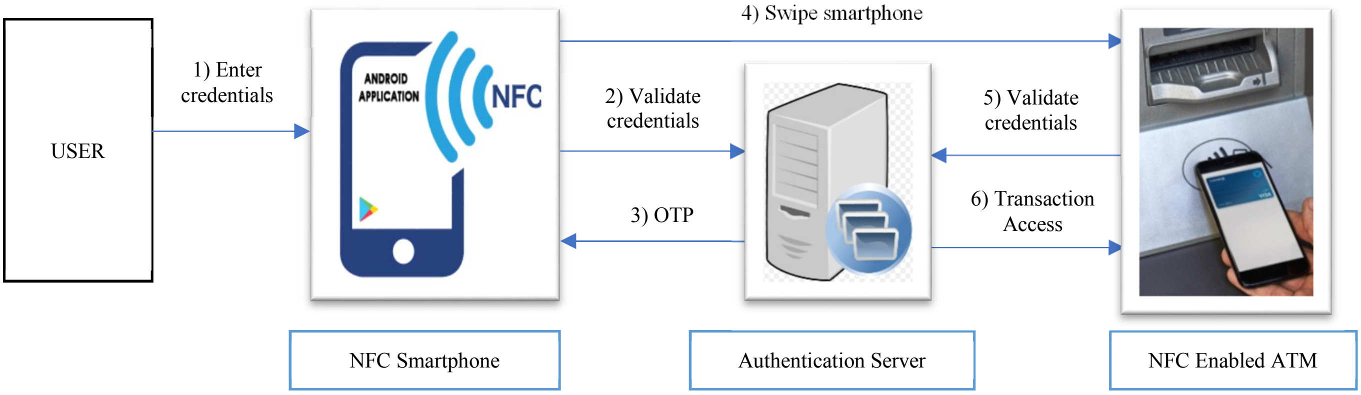

Fig. 2. Authentication Phase

A. Registration Phase

The registration phase is shown in figure 1. In order to register a user, a unique username and default PIN corresponding to the user is setup and securely communicated (either physically or using electronic means) to the user. This communication of initial secret information is in congruence with the current banking process, deployed by some of the banks for ATM card registration. In order to use the proposed authentication system, user needs to install the custom authentication application (from Google Play Store, Apple App Store or any other source) in his/her usual smartphone. Now using the installed app along with the received unique username and default PIN, user needs to register with the authentication server. At the time of registration a One-Time Password (OTP) is sent to the mobile phone of the user via Short Message Service (SMS) which needs to be entered during registration. The user needs to select a new PIN i.e. change the default PIN during registration. If registration is accepted by the authentication server, the user's smartphone specific unique information such as device id, make (like Samsung, Apple etc.), model number (Galaxy Grand, iPhone X etc.), OS type (Android, iOS etc.) and others are sent to the server and the server stores this information and tags it to the username. This completes the registration process.

B. Authentication Phase

During authentication, information exchange takes place between the authentication server and the user in order to verify the identity of the user. In order to gain access to various systems and confidential data, a user needs to be authenticated. Thus it is of paramount importance to safeguard the authentication process from the vulnerable security attacks.

The authentication phase is shown in figure 2. In the proposed system, user needs to enter the username and PIN in the custom authentication app registered on his/her mobile phone. The credentials along with the device specific unique information are transmitted to the authentication server via internet on the mobile phone. On receiving the information the authentication server validates it for correctness. After successfully validating the information the authentication server responds back with an OTP and that OTP gets stored in the authentication app. The validity of the OTP is for preset time duration (say 30 minutes) from the generation time. The stored OTP will not be visible to the user.

This generated OTP can be used anytime during its validity duration to carry out a transaction. Thus a user can perform a transaction at an ATM kiosk during the OTP validity duration.

Before reaching an ATM Kiosk the custom authentication app can be opened and card emulation mode started. At the ATM kiosk, in order to authenticate, the user needs to swipe his\her mobile phone in front of ATM machine NFC reader. When the mobile phone comes in contact with the NFC reader the authentication data (i.e. the username and generated OTP) from the custom authentication app gets transferred to the NFC reader through a secure channel. The NFC reader sends this authentication information to the authentication server for verification. If the authentication information is correct then transaction access is granted to the user.

IV. Discussion

In the proposed scheme, at the time of authentication a NFC supported smartphone is required. Smartphones are already in use worldwide by a very large number of mobile phone users and the usage of smartphones show an increasing trend in near future. Many of the modern smartphones have NFC reader built-in and support NFC card emulation. Thus a dedicated physical card/device for authentication is not required for the users already possessing a NFC supported smartphone.

The custom authentication app is required on user's smartphone. The installation of this custom app can be done from sources such as Google Play Store, Apple App Store or others and is a one-time activity in an ideal scenario. At the time of registration of the app in a smartphone a default PIN corresponding to a unique username of the user is required. The default PIN is securely communicated (either physically or using electronic means) to the user. When user registers the app on a smartphone the smartphone specific unique information such as device id, make (like Samsung, Apple etc.), model number (Galaxy Grand, iPhone X etc.), OS type (Android, iOS etc.) and others are sent to the server and the server stores this information and tags it to the username. This device specific unique information is used by the authentication server to determine whether the source requesting for authentication is genuine. A need might arise for the user to format his/her smartphone or replace it with a new one. In such cases, a new default PIN can be generated from the custom app itself and after a new default PIN is generated the custom app automatically de-registers from the current device where is it installed. The user needs to install a fresh copy of the custom app from sources such as Google Play Store, Apple App Store or others (as mentioned earlier) in the new device. Using the new default PIN the app is registered in the new device.

Some of the advantages of using smart phone in NFC card emulation mode over ATM card

- If a user loses his/her ATM card and a criminal accesses it then the criminal can read the card and find out some of the secret information. If that same person loses his/her smartphone and has it protected using pattern, password or biometrics the criminal cannot easily break into the smartphone. Also, the stolen smartphone data could be wiped off remotely.
- Through data encryption and secure channels, NFC technology can help consumers make transactions quickly while keeping their information safe at the same time.
- There is manufacturing and transportation cost involved to deliver ATM card to the end user. In NFC card emulation mode a mobile phone supporting NFC feature is required.
- In case of ATM Card, there is a lag time to setup authentication for a user because physical card needs to be tagged and send to a user. In case of smart phone, lag time will be much less as the authentication setup will be software based.
- A user might not notice a stolen ATM card for many days if it is infrequently used. Mobile phones have become an indispensable part of the daily life so a stolen mobile phone will be easily noticed.
- Smart phone in NFC card emulation mode is a paperless green solution by use of software instead of printing physical ATM cards.

Security Analysis and Threat Modelling

Threat modelling has become an important part to assess the security of a system. In this section we determine the threat model, including the security objectives, the trust boundaries as well as possible threats.

Security Objectives

The most important goal of an authentication system is to protect users' privacy, i.e. the attackers cannot pretend to be the real user. To achieve this goal, in the existing method of authentication in ATM, the attackers should not be able to get the PIN and the corresponding ATM card at the same time. Also, the authorized actions after a successful authentication should be secure as well.

Trust Boundary

There are four components in this scheme, and four possible channels for transferring data, as shown in Fig. 3.

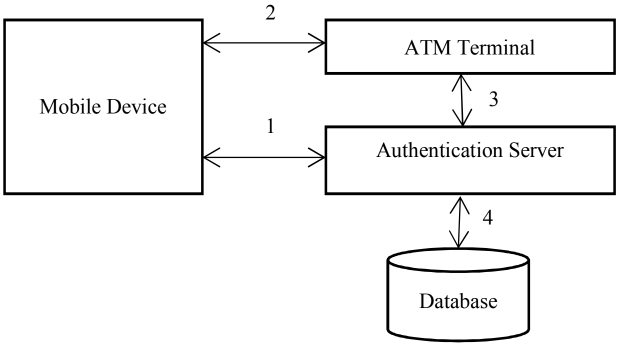

Fig. 3. Trust boundary and the communication channels

We assume that the mobile device component is uncompromised as long as it is in the possession of the user. It is assumed that ATM terminal, authentication server and database are secure components as securing these components is taken care by the existing ATM system and it is not in the scope of this paper.

The communication between mobile device and the authentication server takes place via internet and it is secured using Transport Layer Security (TLS) or Secure Sockets Layer (SSL). The security of communication channel between ATM terminal and authentication server as well as the channel between authentication server and database is assumed to be taken care by the existing ATM system and it is not in the scope of this paper. The mobile device communicates with ATM terminal via NFC technology.

Threats

The threats could be on the components, communication channels and the authentication protocol of the system.

Attacks on the components: In an adverse scenario a smartphone can be stolen. Mobile phones have become an indispensable part of the daily life so a stolen mobile phone will be easily noticed in short time duration. The user can have the option to de-register the app on his/her stolen mobile phone using various means such as online banking account, visiting the bank branch and others. On de-registering, the app will not be usable on the stolen device. A new default PIN needs to be obtained to register a fresh app on the new device. In this case, the process of obtaining a new default PIN is the same as described earlier for obtaining the default PIN for the very first time during registration. If the smartphone is protected using pattern, password or biometrics the criminal cannot easily break into the stolen smartphone and also the smartphone data could be wiped off remotely.

Attacks on the communication channels: The security of the internet connection is based on TLS or SSL. Therefore, if the certificate is valid, the packets cannot be modified or snooped during transmission. The mobile device communicates with the ATM terminal via NFC channel. As stated earlier the communication distance and the lifetime of a NFC channel are short and thus making it difficult to be compromised by an attacker.

Attacks on the authentication protocol: In the existing ATM system an ATM card and corresponding PIN is used to validate the user. ATM skimming resulting to theft of card information and subsequently card cloning (even for chip based cards) has become a burning issue nowadays. Also, the attackers are exploiting methods such as shoulder surfing by direct observation, hidden cameras or other vision-enhancing devices to steal the PIN corresponding to the ATM card of the users. In the proposed scheme, NFC card emulation mode is considered as an alternative to ATM card. An OTP is generated by the mobile app which is used for authenticating the user. The authenticity of the device requesting the OTP is validated before generating the OTP. Since the OTP is valid only for one login session it is resistant to replay attack.

V. Conclusion And Future Work

ATM is a convenient way to meet the banking needs of the users. ATM machines are deployed worldwide and used by a very large population of the world. So it is essential that the ATM transactions are safe and quick. The use of debit card or other types of cards during ATM transactions has some problems like prone to ATM skimming, magnetic strips of card getting damaged, manufacturing and transportation cost of cards, longer time to authenticate users etc. In this paper, we have proposed a novel solution of smart phone in NFC Card Emulation mode as an alternative to ATM cards during transactions at ATM kiosk. Here a smartphone supporting NFC feature (which is present in many of the modern smartphones) is required. The discussion on the advantages of using smart phone in NFC card emulation mode over ATM card shows that it is a useful alternative. Security analysis and threat modelling highlights the security strength of the proposed system against the vulnerable attacks during authentication.

In our future work, the plan is to focus on the security aspects of the custom authentication app to be installed on the smartphone. Also, an exhaustive analysis will be carried out on the possible security attacks during ATM transactions which have not been addressed in the scope of this paper.

References

[1] A. Mandalapu, D. Deepa, L. Raj and A Dev, “An NFC featured three level authentication system for tenable transaction and abridgment of ATM card blocking intricacies”, 2015 International Conference and Workshop on Computing and Communication (IEMCON), Vancouver, Canada, October 15–17, 2015, IEEE Xplore.

[2] A. Meschtscherjakov, M. Tscheligi, C. Gschwendtner and P. Sundström, “Co-Designing for NFC and ATMs: An Inspirational Bits Approach”, 15th International Conference on Human-Computer Interaction with Mobile Devices and Services”, Munich, Germany, August 27 - 30, 2013, ACM.

[3] H. Lee, W.C. Hong, C.H. Kao and C.M. Cheng, “A User-Friendly Authentication Solution Using NFC Card Emulation on Android”, 7th International Conference on Service-Oriented Computing and Applications, Matsue, Japan, November 17–19, 2014, IEEE Xplore.

[4] R.M. Ranasinghe and G.Z. Yu, “RFID/NFC device with embedded fingerprint authentication system”, 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), Beijing, China, November 24-26, 2017, IEEE Xplore.

[5] S. Sridharan and K. Malladi, “New Generation ATM Terminal Services”, International Conference on Computer Communication and Informatics (ICCCI -2016), Coimbatore, India, January 7-9, 2016, IEEE Xplore.

[6] V. Coskun, B. Ozdenizci and K. Ok, “A Survey on Near Field Communication (NFC) Technology”, International Journal of Wireless Personal Communications, Springer, vol 71(3), pp. 2259-2294, August, 2013.