Smartphone authentication solutions for E-banking

Sofie Bonander Priyanka Bhide
Email: {sofbo362, pribh243}@student.liu.se
Supervisor: Nahid Shahmehri, {nahid.shahmehri@liu.se}
Project Report for Information Security Course
Linköping University, Sweden

Abstract

This report will be focused on smartphone authentication solutions for E-banking, for the Swedish banks Swedbank and ICA-Banken, and the Indian bank ICICI Bank.

The main goal is to identify different authentication methods for bank apps and to identify common threats and how to mitigate those.

The research shows that the authentication methods, threats and mitigations are very similar to when authenticating from a computer. However, using an app is much more convenient and easy to use.

1. Introduction

Many banks today offer mobile solutions for E-banking [1]. As customer expectations change it is important for banks to remain relevant by offering new, convenient ways for handling bank errands [2]. At the same time it is important to protect personal data and the data is therefore often encrypted [3].

The banks have high priority on security and did not want to share any information with us about their work with authentication solutions for E-banking. Therefore this report will focus on theory about different authentication methods, followed by a section about transaction flows and security threats. The transaction flows are discovered by practical tests done by the authors.

Further the report covers an analysis about how to protect from the security threats. Finally the report covers conclusions based on the theory part of the report.

2. Background

2.1 Authentication factors

There are three typical authentication factors; something you know, something you have, and something you are. Something you know (i.e. passwords or passphrases) is the most common authentication factor. Something you have includes things such as hardware tokens or the mobile device itself. Something you are uses biometrics such as fingerprint readers or facial recognition software [19].

2.2 Authentication methods

There are many different methods and technologies available that banks can use to authenticate customers. An authentication method can, for example, include customer passwords, digital certificates, physical devices and one-time passwords [4]. Authentication methods can be divided into one-time data and reusable data [8].

2.2.1 One-time data

Examples on one-time data are unique passwords, called one- time passwords [4]. Another example on one-time data is challenge-response.

A challenge-response authentication is when an entity sends a challenge to another entity. If the second entity responds correctly it is authenticated [15]. When, for example, logging in to a system the server gives a challenge to the user and expects a password in return. The server authenticates the user´s identity after the user has provided the correct password. [9]

Systems which are challenge-response based usually use a security token where keys can be stored [10]. The response-generating algorithm that is used can be time dependent [9].

Token

A token is a hardware security device which generates one-time passwords. Such an electronic device can have functionalities where the token and the server share a large number of passwords. When a user wants to log in to a system the server can, for example, ask for the next available password. A more efficient method, are tokens that generate numbers built on a base secret and an algorithm that generates numbers after the request is sent [9].

Swedbank´s security device generates passwords that can be used one time only. The code that is generated is, for security reasons, only active for a limited time. The security device has an electronic chip with built in security functions which handles the unique control numbers and codes [5].

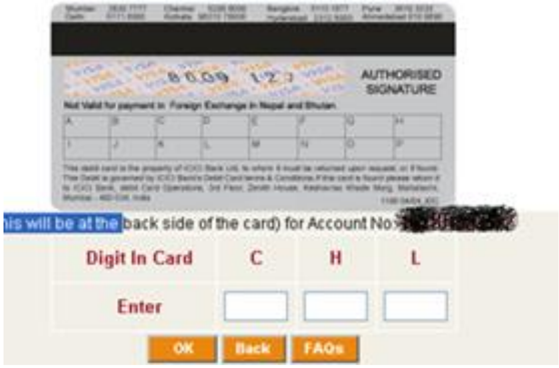
The security device is connected to the user´s social security number and is used for legitimation and when signing agreements. In order to be able to start using the features connected to the security device the user needs to enter a four digits long password [5].

An example of a two factor authentication is the combination of a static password and a one-time password [9]. This method is used when a customer of Swedbank wants to login to the app, using the token. The user is first given a challenge which is to enter a four digit pin-code into the token. This code is personal and has previously been chosen by the user. After providing the correct pin-code the token generates an 8 digit long password which is visible on the token for 60 seconds. The password is active for three minutes and must be entered into the app. If the user does not complete the challenge within three minutes the user needs to send a new request to the token which generates a new password.

ICA-Banken also uses a token that generates one-time passwords that are usable for a limited time. In order to use the token the user needs to insert the credit card in to the token.

Debit Card Grid values

ICICI Bank uses grid card authentication. On the back of the debit card there are 16 cells grid table, containing number and letter A to P. When using the grid card for authentication the user is asked to enter three values that have randomly been generated from the table [23]. See Figure 1 for an example of a debit card grid table.



AUTHORISED SIGNATURE

Not Valid for payment in Foreign Exchange in Nepal and Bhutan

A	B	C	D	E	F	G	H
I	J	K	L	M	N	O	P

his will be at the back side of the card) for Account No: [redacted]

Digit In Card	C	H	L
Enter			

Figure 1. Example of a debit card grid table [23]. For security reasons the numbers in the cells are not visible.

2.2.2 Reusable data

When users are allowed to choose their own passwords they often tend to use the same password in several systems [9].

When logging in to Swedbank´s or ICA-Banken´s app a static personal code can be used. Swedbank also offers the possibility to login using BankID.

BankID

BankID is based on a cooperation between ten Swedish banks. BankID is a service that makes it safe for the customer to access personal features and to sign agreements or other arrangements that is made over the Internet. The BankID contains information about name and personal number and is being protected by a private password. When using BankID the user is asked to enter this password when logging in to a system or when signing agreements [6]. When Swedbank´s customers login to the bank app using BankID they are allowed to transfer money using BankID when signing the agreement. This transaction flow is described in section 2.4.

Today, ICA-Banken is not connected to BankID. But they are aiming to be able to offer their customer this service during 2014 [7].

Personal code

Swedbank´s customers are also able to login to a limited version of the bank app using a personal code. The code is six signs long and must contain at least two numbers and two characters. [5].

ICA-Banken also offers the possibility to login to their bank app using a personal code. This code is four digits long and given to the user when he/she becomes a customer to ICA-Banken.

ICICI Bank offers a mobile banking application called iMobile. The user can check the balance of the account, make transactions and look at the last five transactions. The transactions made using iMobile follows the same security measures as when using Internet banking [20].

In difference to Swedbank´s and ICA-Banken´s app, which is downloaded as an app from App Store and Google Play, ICICI Bank´s customers can get access to iMobile by either send an SMS or download the service via ICICI Bank´s webpage [20]. During the activation process of the service the user is asked to set a four digit pin-code, which is later used for logging in. To be able to authenticate the user´s account and to login, first time users must complete a one-time grid card authentication. The grid card authentication is also used when transferring money [21].

Strong encryption protects the data that is being stored on the mobile phone and all data that is being exchanged between the server and the iMobile is encrypted using public key infrastructure, PKI. A 128 bit encryption fulfils the requirements for security [22].

2.3 Specific issues in regards to mobile devices

Although above-mentioned authentication methods are not unique to mobile devices there are some specific issues that need to be considered in regards to mobile devices for each of the three typical authentication factors.

Something you know; passphrases may be easier to enter and could provide better security than passwords. Something you have; in regards to mobile devices convenience is of high priority. Carrying an extra device or hardware accessory such as a token may therefore be perceived as less convenient. Something you are; this authentication factor still has some problems when using mobile devices that have not been addressed. Applications can not yet fully rely on the mobile device to gather biometric information due to the lack of a standard interface and usability issues exist [19].

2.4 Transactions flows

The authors of this report have done some practical experiments using Swedbanks´s app and ICA-Banken´s app. This section will cover information about how transactions flows can look like using BankID for Swedbank and token in combination with credit card for ICA-Banken. The transaction flow for ICICI Bank is based on theory about transactions, using iMobile.

The following described transaction flows assume that the user is not making any mistakes and that the transactions are being done from one bank to another. The procedures mentioned in the section 2.4.1, 2.4.2 and 2.4.3 are the same for transferring money between customers having the same bank. The only difference is that “Other bank” seen in the flows is not connected.

2.4.1 Money transfer using ICA-Banken´s app

When transferring money using a token and credit card, the user is first asked to log in to the system using a control-code, provided by the bank. The user needs to enter the control code in to the token and receives an answer-code which is entered in the app. The bank gives the user access to start a transfer. Sender, receiver, amount, date and an optional personal message is entered before pressing the accept button.

The user is asked once more to use the credit card and token in order to sign the agreement. This time the user needs to press the sign-button instead of the log-in button on the token. After the correct control-code and answer-code have been entered the transaction is submitted and the user is notified. An overview of the transaction flow is described in Figure 2.

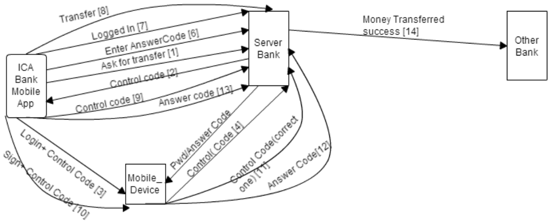


Figure 2. Overview of the transaction flow for ICA-Banken using token and credit card.

2.4.2 Money transfer using Swedbank´s app

Once the user is logged in to the bank app the user can transfer money between accounts. Information about sender, receiver, amount, date and an optional message is provided by the user before pressing an accept button. The BankID app is displayed, asking the user to enter the personal code. It is assumed that the correct code is provided and the transfer is being made. The BankID displays a message for the user, saying the transfer has been done. An overview of the transaction flow is described in Figure 3.

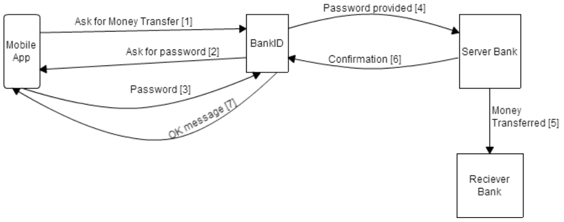


Figure 3. Overview of the transaction flow for Swedbank, using BankID.

2.4.3 Money transfer ICICI Bank´s iMobile

When transferring money using iMobile the user must use the grid card, found on the back of the debit card. The user is asked to enter numbers based on the three randomized letter. For example is the user asked to enter the numbers found in cell A, D, G which might correspond to the values 7, 96 and 47. When correct values are entered the transfer is being done. An overview of the transaction flow is described in Figure 4.

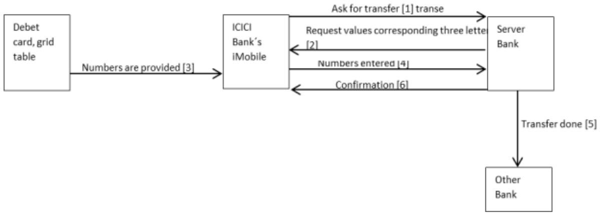


Figure 4. Overview of the transaction flow for ICICI Bank, using iMobile and grid card.

2.5 Security threats

Security is especially important when using mobile devices since outsiders easily can access personal data [3]. This section will cover information about some of the common threats related to the usage of E-banking services.

In general, the methods used for compromising sensitive information or taking control over a mobile phone are the same as for computers. Depending on which mobile platform that is used, the mobile phone is more likely to be infected by malicious code and other security issues. The number of users and the security of the operating systems are the two factors that will determine which mobile platform that is likely to be infected. [11]

iPhones are more secure than Android phones since they have better protection against traditional viruses. The protection is based on that all developers and the code itself must be approved before it releases on Apple’s App Store. It can therefore be said that Apple relies on that all malicious code is found during the inspection process. Google do not inspect all the content of an app before it releases. It is therefore more likely that malicious code spreads through Google Play than through App Store. Google however, have the possibility to remotely delete specific apps from Android phones that already had been infected [16].

Android represents 97 % of all malware on mobile platforms. But only 0, 1 % of the malware is spread via Google Play. The remaining part of malware is spread via third parties [17].

2.5.1 Trojans and other malicious codes

Malicious code such as Trojans can infect your mobile phone. The infected programs are usually customized for mobile phones. Trojans can be hidden in applications that the user think is not harmful. The most common way of infecting someone’s mobile phone is by spreading infected code via App Store and Google Play, which are the program stores for iPhones and Android phones. A Trojan can also be hidden in an infected hyperlink and when the user presses the link the intruder have access over the phone [11].

2.5.2 Eavesdropping

If the authentication is not encrypted and some attacker has access to the network somewhere between the user and the server, the attacker can be eavesdropping. Even though the traffic is encrypted it can still be exposed for eavesdropping, if the encryption keys used are compromised or if the encryption algorithm is not strong enough [9].

2.5.3 Man-in-the-middle

Man-in-the-middle appears when a user is connected to the hacker instead of to the bank´s legitimate server [9]. The easiest way for a hacker to become a man-in-the-middle is to be connected to the same open wireless network as the victim [13]. Figure 5 provides an overview of a man-in-the-middle attack.

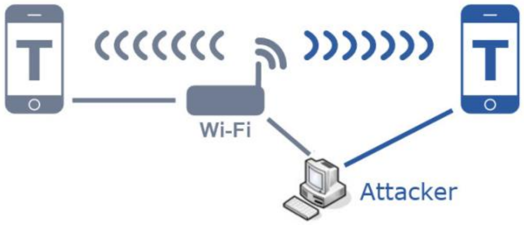


Figure 5. A man-in-the-middle attack, using an open wireless network [13].

The hacker can capture authentication data and use it to authenticate the bank. An attacker can for example, during a money transfer, change the account number to the hacker´s own account number and then the money is transferred to the hacker’s account [9].

2.5.4 Social Engineering

Social engineering is when an intruder impersonates to be someone the user knows or trust and take advantage of that position via email, telephone, chat, or something similar [12]. However, the most efficient social engineering technique seems to be human-to-human contact [9].

2.5.5 Phishing

Phishing is a type of fraud where the intruder fish for bank related information. There are different ways of phishing for information. One example is for the intruder to send the user a false email or tempt the user to visit an infected webpage. The email or webpage usually looks very similar to the one the bank uses, something which makes it easier for the user to fall into the trap. Other examples are theft of private codes. Someone can be watching you when you access the bank account, using private codes [12].

3. Analysis

Different devices have different security requirements and therefore it can be risky to reuse passwords. Systems with less protection can be hijacked and the password can then be compromised. Once someone has stolen the password the password can be used for attacking more sensitive systems. One-time passwords are more secure than reusable data. However, one-time passwords are still vulnerable to some attacks [9].

This section will present how to protect against some common security threats that is related to the usage of E-banking for smartphones.

3.1 Encryption

The strongest encryption technology available today is called SSL, Secure Socket Layer. SSL is a secure communication protocol that provides server authentication and encrypts the client´s information when transfer is done over the Internet [4].

SSL is used to prevent eavesdropping. The SSL is efficient as long as the user does not use accept any fake certificates. If a fake certificate is accepted the user can be threatened by a man in the middle attack.

In addition, the user needs to prevent others from gaining full access to the mobile device. If an intruder gets full access to it, the SSL-stack can be replaced with a modified version which allows eavesdropping on data that is not encrypted [9].

3.2 Update the software

In order to keep the mobile phone safe and prevent it from being infected it is important to download and install software updates. The updates usually include new features as well as security updates or fixes [11].

3.3 Trojans

The risk for Trojans can be mitigated by being extra careful when downloading apps from App Store or Google Play. Before downloading an app it is good to always look at reviews from other users and make sure that the developer of the app is trustworthy. It is also a good idea to read the detailed information about which information the app has access to on your phone. If the user make these security measures, the user do not need to download anti-virus software for the mobile phone. [11]

The protections available for mobile devices are very similar or identical to the ones available for computers. If a user wants to be extra safe, the user can install an anti-virus program for mobile phones. The anti-virus program scans apps and notifies the user with a verdict after the scanning is done. Depending on if the user thinks the verdict is acceptable or not the user can choose to continue the downloading of the app. [18]

3.4 Social Engineering, Phishing & other frauds

To be able to protect the mobile phone from unwanted intrusions the user can activate a pin code for logging in to the phone. This is especially useful if the mobile phone ends up in someone else's hands [11].

Furthermore, it is recommended to set up an anti-theft protection which allows the user to remotely delete data from the mobile phone. This is an especially important security measure, since the easiest way for someone to infect a mobile phone are by taking the physical device and manually install the malware [18].

In addition, iPhone owners can make sure to never use a mobile phone that has been jailbreaked. A jailbreaked mobile phone is more likely to contain malicious code since a jailbreaked phone makes it possible to download apps from other places than App Store. It is therefore recommended to only download apps from App Store if you have an iPhone since most viruses have been discovered during Apple's inspection process [16].

Furthermore, it is important to never share or document any economic information or personal information such as passwords, pin-codes and social security numbers which can be used for services provided by the bank app. If someone unauthorized get access to this kind of information it can be devastating [12].

Also, make sure to store the token and the credit card in a safe environment, since these items can be used for services related to the different bank apps.

3.5 Man in the middle attack

Make sure to have a safe Internet connection. Avoid using untrusted wireless networks such as those available at public spaces [13].

3.6 One-time password

The risks of being attacked using one time password can be mitigated by using one-time passwords that only are valid for a short period of time [9].

4. Conclusions and discussion

Based on the empirical data about Swedbank´s and ICA-banken´s authentication methods using a token it have been found that ICA-Banken uses more factors than Swedbank and ICICI Bank. According to [4], methods that only are dependent on one-factor are easier to compromise than those using multiple factors. It can therefore be argued that ICA-Banken´s transactions are more secure than Swedbank´s since ICA-Banken use both token and credit card, compared to Swedbank who only uses a token and ICICI Bank who uses a grid card.

From a perspective regarding convenience it can be argued that Swedbank offers a service that is more convenient than the ones ICA-Banken and ICICI Bank offer. When transferring money using Swedbank´s app the user do not need any other device than the mobile phone itself. ICA-Banken requires a token and a credit card in addition to a mobile phone, and ICICI Bank requires a grid card.

Some drawbacks regarding bank apps have been found. One drawback is that everybody does not own a smartphone. And even if you are a smartphone owner you might not feel comfortable with using the service. Some does not trust the security while others might not know how to use the app. The case can also be that the app does not offer all necessary features, and that might stop customers from using the app. It is therefore important that the bank offers an intuitive and easy used app, but it is also important that the app offers most of the services that you otherwise expect to solve using a computer or in person at the bank.

Depending on how the app and its graphical interface is developed it can be complicated to use the app. Some apps require that you have access to more than a personal code or have access to connected software which may complicate things.

However, there are still a lot of benefits with smartphone apps for E-banking. In general, bank apps offer a high level of service, provided in an easy and convenient way. An app is often more convenient than accessing the bank account by using a computer or going to a bank office.

Due to the convenience, the account holder is more likely to overview his/her account more frequently. By monitoring the account more often, the security increases and the risk of fraud decreases [14].

5. References

[1] Svenska Bankföreningen, Mobila Banktjänster [Online]. Available: http://www.banksakerhet.se/node/80 (Accessed: 24 April 2014).

[2] Bank systems & technology, The Path to SmartPhone Banking Apps [Online]. Available: http://www.banktech.com/core-systems/the-path-to-smartphone-banking-apps/232400051 (Accessed: 25 March 2014).

[3] Datainspektionen, Säkerhet för personuppgifter [Online]. Available: http://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf (Accessed: 13 May 2014).

[4] O.B. Lawal, A. Ibitola, O.B. Longe, "Internet Banking Authentication Methods in Nigeria Commercial Banks“, African Journal of Computing & ICT, 2013.

[5] Swedbank, Säkerhet- internet- och mobiltjänster [Online]. Available: http://www.swedbank.se/privat/sakerhet/saker-identifiering/internet-mobil-tjanster/index.htm#!/ (Accessed: 28 April 2014).

[6] Swedbank, BankID/e-legitimation - bevisa enkelt och säkert vem du är på nätet [Online]. Available: http://www.swedbank.se/privat/internet-och-telefontjanster/bankid-(e-legitimation)/index.htm (Accessed: 30 March 2014).

[7] ICA-banken, Frågor och svar [Online]. Available: http://www.icabanken.se/fragor-och-svar/teknik-och-sakerhet/ (Accessed: 14 May 2014).

[8] A.Vapen, N.Shahmehri, "Security Levels for Web Authentication using Mobile Phones", Linköping University, 2010.

[9] J. Hassmund, "Securing Credentials on Untrusted Clients", Linköping University, 2010.

[10] A. Vapen, N.Shahmehri, "2-clickAuth - Optical Challenge-Response Authentication using Mobile Handsets", Linköping University, 2011.

[11] Stiftelsen för Internetinfrastruktur, It-säkerhet för privatpersoner- en introduction [Online]. Available: https://www.iis.se/docs/IT-sakerhet_for-privatpersoner.pdf (Accessed: 14 May 2014).

[12] Swedbank, Bedrägerier [Online]. Available: http://www.swedbank.se/privat/sakerhet/sakerhet-vanliga-bedragerier/bedrageri/index.htm (Accessed: 28 April 2014).

[13] The Hacker News, T-Mobile Wi-Fi Calling App vulnerable to Man-in-the-Middle Attack [Online]. Available: http://thehackernews.com/2013/03/t-mobile-wi-fi-calling-app-vulnerable.html (Accessed: 14 May 2014).

[14] Bank systems & technology, The Path to SmartPhone Banking Apps [Online]. Available: http://www.banktech.com/core-systems/the-path-to-smartphone-banking-apps/232400051 (Accessed: 25 March 2014).

[15] Techopedia, Challenge-Response Authentication [Online]. Available: http://www.techopedia.com/definition/26138/challenge-response-authentication (Accessed: 16 May 2014).

[16] Mobil, Säkra din smartphone [Online]. Available: http://www.mobil.se/tips-tricks/s-kra-din-smartphone (Accessed: 16 May 2014).

[17] Feber, Android står för 97 % av allt malware på mobile [Online]. Available: http://feber.se/android/art/295094/android_str_fr_97_av_allt_malw/ (Accessed: 17 May 2014).

[18] F-Secure Corporation, Mobile threat report, July-September 2013 [Online]. Available: http://www.f-secure.com/static/doc/labs_global/Research/Mobile_Threat_Report_Q3_2013.pdf (Accessed: 17 May 2014).

[19] Cigital, Inc., User Authentication on Mobile Devices [Online]. Available: http://www.cigital.com/wp-content/uploads/downloads/2012/11/mobile-authentication.pdf (Accessed: 17 May 2014).

[20] ICICI Bank, iMobile- Your Bank on your mobile phone [Online]. Available: http://www.icicibank.com/mobile-banking/imobile.page? (Accessed: 18 May 2014).

[21] ICICI Bank, How to download [Online]. Available: http://www.icicibank.com/mobile-banking/download.page?#toptitle (Accessed: 18 May 2014).

[22] ICICI Bank, Security with iMobile [Online]. Available: http://www.icicibank.com/mobile-banking/security.page? (Accessed: 18 May 2014).

[23] ICICI Bank, ICICI extra layer of security for Online Transaction [Online]. Available: http://www.chromoz.com/icici-extra-layer-of-security-for-online-transaction.html (Accessed: 18 May 2014).