Different Authentication Schemes Used in Smart Phones

P Lalitha Surya Kumari,
Assistant Professor,
Dept. of Computer Science and engineering,
Bharat Institute of Engineering and Technology, Hyderabad,
Andhra Pradesh, India

Prof. A. Damodaram,
Dept. of Computer Science and Engineering,
JNT University,
Hyderabad, Andhra Pradesh,
India

Abstract

With the growth of wireless technologies in sectors like the banking, aviation, military etc, the authenticity of a genuine user needs to be determined. The conventional authentication mechanisms such as password, biometrics and possession are prone to hardware failure, theft, expensive, etc. Hence, there is a need for a strong authentication solution. In this paper different existing authentication and authorization scheme for mobile transactions using smart phones are discussed. Smart phones are becoming increasingly more deployed and as such new possibilities for utilizing the smart phones many capabilities for public and private use are arising. This paper will explore the possibility of using smart phones as a platform for authentication and access control, using emerging technologies. The study performed and proposed multi-factor authentication such as combining NFC with other communication technologies such as Bluetooth has proven to be effective. This paper describes the distinguished features and the architecture of different emerging technologies used in Smart Phones.

Keywords-authentication; authorization; Smart Phone; GPS; NFC; RFID; Multi factor authentication;

1. Introduction

Wireless technologies have become increasingly popular in burgeoning military affairs and so is security, where the identity of an individual on the other side of the network has become challenging to determine. Thus, authenticity of an individual to access the private resources is the foremost concern and strong authentication between two parties (end-to-end) needs to be implemented.

With mobile devices constantly taking a bigger part in our everyday life, the ease of accessing a bank account, paying for any services or even checking medical journals independently of current time and place is getting more and more feasible. Having in mind that these kinds of services require access to the personal information or user, the logical major requirement is high security and strong user authentication methods.

Currently, one of the most common authentication mechanisms is based on the use of passwords [2]. This is due to its ease of implementation for the Service Providers (SPs), cost effectiveness and its familiarity to end–users. However, it has also been one of the least secure methods compared to other options. General tendency of people is to choose weak passwords for multiple services. As a result, accounts get hacked, people lose money, and their privacy is breached etc. In order to counter those problems, security critical services, such as online banking, started to use multi-factor authentication solutions. For example, permanent passwords are combined with other mechanisms, such as special tokens, that can generate one–time passwords. The use of more than one factor has been observed to be more secure than depending only on a single one.

Authentication and authorization are two of the most important security features for mobile transaction systems. Most commonly, these schemes depend on three factors: Something the user knows (secret), Something the user has (token), and Something the user is (biometrics). Even though these factors are sufficient for most cases, there is still additional room for improvements and

alternatives such as location of user (i.e. location based authentication, NFC [5] (i.e. RFID technology) etc.,

However, these solutions usually require a specially designed infrastructure and special devices. It is rather difficult for these solutions to get widely deployed since some special requirements have to be fulfilled. Meanwhile, smart phones are gaining popularity all over the world, especially in the US, Europe and Asia. Hence, we need to use different emerging technologies for stronger authentication using smart phones.

Through this paper we want to address following concepts:

- The most common and accepted authentication methods for mobile services
- The differences, opportunities and challenges concerning user authentication for mobile services
- Evaluation of security / usability / privacy trade-offs for different authentication mechanisms.

We recognize the potential of new mobile services that are emerging, but we would like to find out if security is on a sufficiently high enough level to provide adequate support for them or they can provide more threats and problems to users than benefits.

2. Prevalent mobile phone authentication methods

The first phase of this paper was to perform research on what is already developed and available in the area of user authentication for mobile service. For research we used Internet browsing, as well as search of research databases (e.g. IEEE, ACM, Elsevier). We saw that field of user authentication for mobile device is very wide and tried to organize our findings in four groups:

- Authentication based on something the user knows
- Authentication based on something the user has
- Authentication based on something the user is
- Authentication based on user's location

2.1 Something the user knows

Methods based on something the user knows are often associated with a password [2][10], multiple passwords, or a combination of a password and a username. The user has usually chosen a password before he/she starts using the service and provide same password by the user for every service in future. When we turn on our mobile phone, the first thing that happens is that it is prompted for the PIN code, before user can start using mobile phone. On that manner the user is authenticated to the mobile network, and also the user is protected from loss and theft of the mobile device.

Security level provided by this approach is not very high. This approach is very popular and widely accepted for mobile device. The biggest reason for this is high usability and easy implementation.

2.2 Something the user has

Authentication in this case is based on something that user has, a physical object. An object could be a mobile device or a token [10]. In this approach, a user is not required to remember some secret information (password) nor it is required to reveal any private information about him/her (like in biometrics).This approach for user authentication is especially suitable for authentication of a user for mobile applications and services. The biggest reason for this is that mobile device can be considered as physical object because it is a private device that belongs to just one person and because of that is ideal example of something the user has. Hence, the mobile device can be considered as the terminal providing the service as well as the user authentication token.

The possible approaches are:

- Private information is stored on hardware such as SIM card,
- Private information is stored on the specific file on the mobile device´s file system, and
- Private information is received through mobile service operation (SMS message).

Security level that is provided by using only this method is not so high. The attacker may gain full access to the user's private information and services if he or she steals the user's token or mobile device. Usability of this authentication approach can vary greatly depending on the type of token used

2.3 Something the user is

Ways to authenticate a user based on something he/she is are often based on scanning and analysis. These methods referred to as biometrics and authentication based on the person's unique traits such as fingerprints or behavior, such as walking patterns or typing patterns. That means traits are the physical structure of the user.

Biometric authentication methods [10] have been developed to counter the possibility that unauthorized persons may gain access when traditional security

methods like security pass cards or passwords are used. These methods include "fingerprint-based systems and iris, retina, face, palm print, voice, handwriting and DNA technologies" .However, there are known attacks on fingerprint readers as well (e.g. gummy bears) using different materials to simulate finger.Biometrics might be best suited for additional security, or as a second factor in a multifactor authentication process, rather than being used on its own. The use of biometrics can be quick and effective. It is virtually impossible to loose or forget like tokens or passwords because it is based on something the user is, a physical part of the user. The concern is if their information is somehow compromised, the users will not be able to change their fingerprint, like they would their password.

2.4 Location based authentication

Location based authentication [1][10][4] is not used much directly in present times. To find the users location some suggested methods involve using GPS [4] capable devices, for instance a newer cell phone, relying on the cell network or using Bluetooth or other range limited technology as a beacon. The different methods have advantages, disadvantages regarding granularity and range and different uses.

2.4.1 GPS (Authentication method based on user's location). A method that takes advantage of the recent advancement in location–sensing technologies, especially provided by smart phones, is needed. These advancements have led to the improvement and reliability of location information and thus rendering it more useful. With the current technology it is possible to make this technology transparent and convenient for users. It includes latitude, longitude and also altitude at which person who is trying to authenticate his identity. Location information is captured along with time at that particular moment. Location is most often associated with GPS [4] receivers. Adding location information into existing security mechanisms can be used to ameliorate the efficiency of authentication and access controls

3. Strong authentication used in smart phones

3.1 PassBan

PassBan [7][9] takes two factors for Authentication to the next level. A conventional two factor requires a user to enter a password and a code or PIN. In PassBan [7][9] the factors could be your face, voice, location, token, motion or an on-demand OTP (One Time Password). Though it may not be a foolproof system, it is sure takes the security level of two factor method a notch higher. The omnipresent smart phone is emerging as a promising replacement for passwords used in authentication.

Most of us have to remember countless passwords for different online services, and we are often asked to choose complicated strings of characters to make them harder to guess.Most experts agree that a password killer is necessary to bolster Web site security. The tendency of the people to use easy to guess simple passwords for different sites has drastically weakened their effectiveness. In addition to that encrypted passwords are easily acquirable by hackers due to sophisticated decryption technology. Because many people use smart phone, it's seen as the perfect place to store credentials. Many sensors can be used in the phone to identify a user, and hence the device can be used for stronger authentication.

People store and access a large amount of personal data using smart phones and tablets making them all the more valuable if they're lost or stolen
And yet, while there are number of companies focusing on securing desktop and laptop computers, the market for mobile security is still in its early stages.

PassBan is an pioneering developer of multifactor authentication using mobile and cloud-based technology. PassBan provides multifactor authentication technology using voice and facial recognition for in a smart phone. A mobile security startup called PassBan allow people to choose from a bevy of different authentication options—including one that we wear on our wrist.

PassBan released a free Android app called Passboard that allows you to secure individual apps on a smart phone with any of more than a dozen verification techniques, including identifying your voice, face, location, or a specific gesture.
PassBan unveiled its wearable verification device in the form of a smart wristband. By wearing the device, users will be able to unlock their mobile apps and gain access to the data they need.

PassBan's wearable verification devices work with any smart phone or tablet running the PassBan mobile user authentication client (currently on Android and iOS based devices). The service is free for sandbox (developer) use, and the encrypted and dynamic certificate exchange mechanism used by PassBan makes the wearable device highly secure.
If users have a smart wristband within the vicinity of their smart phones then PassBan pairs the smart phone with the wristband, users can then start mobile applications they've secured using wearable

verification, either by a gestures (movement) or by tapping on the smart-wristband.

Of course, this doesn't have to be the only layer of security, with PassBan allowing us to combine it with other methods like biometric verification (face, voice), location check, phone-factor (call), motion, token or Pass Color verification Sounds pretty secure. EMC-owned RSA acquired PassBan.

3.2 Smart Phone based Authentication

It is a Two Factor Authentication. Two Factor authentication (2FA) [3] is where a user's credentials are made up of two independent factors such as:

- Something the user knows (PIN, simple password, alpha-numeric password, alpha-numeric password with special characters, secret questions, passphrase);
- Something the user has (Keyfob [3] token, key, debit card, smartcard, mobile phone);
- Something the user is (Biometric such as fingerprint, retina, iris, face, veins, DNA, voiceprint, hand, typical usage patterns)

The first factor is The hardware token(something which we have) called Keyfob [3]. One type is the One Time Password (OTP) keyfob [3], which is typically carried on our key ring and displays a pseudo-random number that changes periodically. The keyfob itself contains an algorithm, a clock or a counter and a 'seed record' used to calculate the pseudo-random number.

The user enters this number to prove that they have the token. The server must also have a copy of each keyfob's seed record, the algorithm used and the correct time to authenticate the user.

The OTP keyfob software for smart phones is available as the hardware version, but instead of carrying around an extra piece of hardware it uses the smart phone to calculate the OTP from the 'seed record' along with the smart phone's clock and the algorithm contained in software installed on the smart phone, usually in the form of an App.

It does have some significant advantages over the hardware token for both organizations and end users. Unlike the hardware token, the smart phone version is not vulnerable to physical damage or loss. Also, for geographically disperse organizations the tokens can be sent electronically- no waiting for shipping or battling with reams of customs paperwork just to get that token to the other side of the world

The second factor is use of biometrics. One evolving area is the use of biometrics on smart phones to authenticate the user based on physical attributes or behavior. This moves the second factor to 'something you are' or 'something about your behavior'. Biometrics on smart phones is still in its infancy.

One biometric that has the potential to work across all types of smart phones is voice – using the device's microphone to capture biometric information.The voiceprint that the user has allows the user to be uniquely identified. The simplicity of using just the characteristics of your voice to authenticate is very appealing. But App vendors must allow them to incorporate this technology into applications. This combination of multiple factors is very powerful in assessing a user's identity and the smart phone is the perfect device to capture the information required. Most have a GPS receiver built in so they know where you are at all times. There are significant barriers to the adoption of both biometrics and risk based authentication technologies on smart phones. Both require that the Apps or the smart phones being secured have these technologies integrated with them. This can work when smart phone vendors produce integration kits for App developers and the App developers see the business case for a higher level of security; but this is going to seriously limit the Apps that you can allow your users to run.

There's no doubt that the use of two factor authentication is rising and that we rely on smart phones as business tools to get access to sensitive data. While the increased availability and decreased cost of using the smart phone as the replacement for the hardware token is valid, unless we move away from the traditional 'something the user has' factor, we're increasing the risk of the confidentially of our data being compromised.

3.3 NFC Enabled Smart Phones

Smart phones are becoming increasingly more deployed and as such new possibilities for utilizing the smart phones many capabilities for public and private use are arising. This paper will investigate the possibility of using smart phones as a platform for authentication and access control, using near field communication (NFC) [5][6]. To achieve the necessary security for authentication and access control purposes, cryptographic concepts such as public keys, challenge-response and digital signatures are used. The investigation performed and specifies that NFC supports the advanced communication required by this case.

NFC is an emerging technology based on Radio Frequency Identification (RFID) that allows devices to communicate over short distances (max 10 centimeters). This technology has already been

incorporated into some commercially available mobile phones, and services are already provided such as public transportation and ticketing systems.
Currently new smart phones are entering the market with technology such as NFC [5][6] (Near field communication). NFC will allow the smart phone to wirelessly interact with physical objects or terminals. The Interaction with physical objects will enable the phone to simplify the daily life for its users. NFC can seamlessly receive and transfer information which would otherwise be tedious work for the user to input.

3.3.1 Enhancing Authentication with NFC-Enabled Mobile Phones in eBanking

Our NFC-based authentication mechanism [5][6] relies on dual-interface smart cards, that is, cards with both contact and contactless interfaces. These cards might also be used as debit or credit cards. In fact, this is desirable to avoid burdening the customer with an additional card for e-Banking purposes.
The customer authentication mechanism works by using his card and its PIN, which is used to authenticate the customer to the card. More precisely, when the customer wishes to engage in e-Banking, he visits the Internet site of his bank, which requests his customer ID, eg his account or contract number. Once such an ID has been received by the bank, it replies with a challenge, which consists of an unpredictable number of between 6 and 8 digits

After the challenge, the customer starts the phone application by touching his bank card to the back of the phone. He then selects the log-in mode and types in the server-issued challenge. Prior to generating the corresponding response, the customer provides his PIN to authenticate himself to the card on phone's request. The phone sends the challenge to the card after the customer has been authentication by the card obtaining a cryptogram in return. Using this cryptogram – a bit-string cryptographically bound to the challenge and the internal card state – the phone generates a numeric code, ie the response, which is displayed to the customer. Subsequently, he sends the response to the bank server by typing it into the PC. When the response is received by the bank he latter checks whether it corresponds to the previously issued challenge. If this is the case, the bank presents the customer with his account(s) summary, as well as some appropriate transaction options.

The mechanism outlined above replaces the Personal Card Reader (PCR) required by some authentication schemes currently in use. This follows from the fact that the user needs only his phone and his card in order to authenticate himself to the bank.

The requirements of our authentication mechanism are quite low because on the one hand, phones are truly ubiquitous devices that can hardly be considered a burden; on the other, most people carry their bank cards with them in their purses or wallets, making.
Note that both the challenge and the response could be sent directly from the bank server to the phone and back via SMS, or some other suitable mechanism using the mobile phone network. This would not only simplify the mechanism, but also increase the level of security as a consequence of using the phone and a secondary channel, whose compromise is much less likely than the PC alone.

3.4 Smartphone Enabled Secure Access to Multiple Entities (SESAME)

SESAME [8] which consists of a user accessing web services on a Host Terminal via a smart device. Here the Host Terminal is used to view the web content while the smart device is used for authentication purposes. The flow of information from the Host Terminal to the web server is securely processed via Internet protocols. Similarly, the authentication mechanisms and schemes at the web server are unchanged. SESAME [8] mainly addresses the interaction between a user and the Host Terminal for accessing services. Specifically, we address the problem of inputting credentials via a Host Terminal to access a service. Incidentally, addressing this specific problem also addresses the limitation of memorizing textual passwords. SESAME provides an avenue that is complimentary to textual passwords and their usage, mainly providing a way to better support its use while removing their limitations. A user during the registering process for a web service chooses a strong password. User then stores his/her credentials for the service (username and strong password) on a smart device by manually entering this information. Whenever user has to access the web service, he/she will securely transfer the credentials from his/her smart device to a Host Terminal or a cloud service which will then forward user credentials to the appropriate Service Providers. The Service Provider authenticates the user and delivers the service to the Host Terminal.

Future Internet Services of SESAME can be integrated to leverage the services of the Cloud and Service Providers can integrate SESAME to register and authenticate users based on their biometrics. Further extension to the future architecture can be made by replacing the password based authentication

with the use of only username and Biometric Hash (BH). This architecture would require the Service Provider to support the use of BH as the authentication scheme.

4. Conclusion

This paper has been discussed about different existing and emerging technologies used for authentication in smart or mobile phones. This paper says that multi factor provides stronger authentication than prevalent single factor authentication.

The four authentication factors, that is, "something the user knows", "something the user has", "something the user is" and "user's location " are irrefutably fine features in authenticating the identity of an individual but they still do not suffice for very strong authentication. One cannot completely depend upon these aspects when authenticating an individual.

From research that we conducted and summarized in previous part of the paper, we can see that there are many approaches for performing user authentication, for mobile devices. We saw that there is no unique solution that is appropriate to every situation. There are numerous factors that must be taken in consideration when selecting authentication method, as for instance: usability, security, specific functionality of the application/service, privacy, user requirements. The biggest challenge is finding the right balance between these factors, and selecting the authentication method that is suitable for the specific service and accepted by the users.

This paper identifies security as main issue that can greatly affect their development and deployment. Because of that in our paper we decided to research more in depth different authentication methods and their suitability for Smart Phones. During our research we identified main authentication methods that are used today for mobile devices and their main characteristics. Our main conclusion based on previous work is that there are many approaches for user authentication for mobile devices or Smart Phones now, but only couple of them are really accepted and in everyday usage. Also we see some potential to other types of authentication (e.g. biometrics), but still the main obstacles are limited capabilities of mobile devices and users perception of the methods.

References

[1] Seema Sharma, University of New Orleans "Location Based Authentication" http://www.signify.net /resources/articles/the-rise-of-two-factor-authentication-tokens-vs-smartphones

[2] Feng Zhang, Aron Kondoro, Sead Muftic "Location-based Authentication and Authorization Using Smart Phones"http://www.diva-portal.org/smash/get/ diva2:576463/FULLTEXT01.pdf

[3] Grant Le Brun, Head of Engineering and Research Labs at Signify "The rise of two-factor authentication: tokens vs smartphones"http://www.signify.net/ resources/articles/the-rise-of-two-factor-authentication-tokens-vs-smartphones

[4] Torben Kuseler & Ihsan Alshahib Lami "Using Geographical Location as an Authentication Factor to Enhance e-Commerce Applications on Smartphones" http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/volume6/Issue4/IJCSS-735.pdf

[5] Diego A. Ortiz-Yepes, January 2009 Special theme: The Sensor Web "Enhancing Authentication in e-Banking with NFC-Enabled Mobile Phones"

[6] Electrical and Computer Engineering Technical Report ECE-TR-14 "Mobile Authentication With NFC Enabled Smart Phones" http://eng.au.dk/ fileadmin/ DJF/ENG/PDF-filer/Tekniske_rapporter/samlet-ECE-TC-14.pdf

[7] Smartphones could evolve into password killers http://www.citeworld.com/security/22225/smartphones-could-evolve-pa ssword-killers

[8] Ameya Sanzgiri Anandatirtha Nandugudi Shambhu Upadhyaya Chunming Qiao "SESAME: Smartphone Enabled Secure Access to Multiple Entities" http:// www.acsu.buffalo.edu/~ams76/SESAME.pdf

[9] Darshik Jariwala in Business, Security "RSA acquires PassBan, to provide Multifactor Authentication" http:// www.techstagram.com/2013/07/27/rsa-passban/

[10] Final Report-INFS5261 Hans –Joachim,Jelana Mirkovie, Ivika Milanovic, Oyvind Bakkeli "Authentication Methods "http://www.uio.no/ studier/emner/matnat/ifi/INF5261/v10/studentprojects/ authentication- methods/ FinalReport Authentication Methods.pdf