A Potpourri of authentication mechanisms The mobile device way

Rui A. Martins[1], Alexandre B. Augusto[2], Manuel E. Correia[1]
ruimartins@dcc.fc.up.pt, aaugusto@med.up.pt, mcc@dcc.fc.up.pt
[1]Center for Research in Advanced Computing Systems (CRACS-INESC-TEC),
Department of Computer Science, Faculty of Science, University of Porto; Portugal
[2]Center for Research in Health Technologies and Information Systems (CINTESIS),
Faculty of Medicine of University of Porto (FMUP); Portugal

Abstract—**Nowadays the use of mobile devices, such as smartphones and tablets, are rapidly increasing in network services, proliferating to almost every environment. This massive appearance of mobile devices creates significant opportunities to leverage these mobile devices to establish novel types of services. However there are also significant concerns about the privacy and security of sensitive data exchanged and stored on these devices. Since these devices are usually embodied with numerous characteristics like camera devices, 3G and NFC connection that can be used to create new alternative authentication schemes in order to guarantee users identity.**

This paper performs a survey on the current state of the art in alternative authentication mechanisms regarding access and authentication against the traditional login and password scheme by the usage of the mobile devices and their properties.

Keywords: mobile devices, smartphones, authentication, authorization, biometry, security, NFC communication, access control and usability

I. INTRODUCTION

Access control and user authentication is a very important subject in today's computerized world. The challenge these days is not encrypting data, but authenticating the user. Proof of a user's identity and authority must be obtained, before granting access to their data. [1] This authentication can come in the form of passwords, smartcards, biometric data, and much more.

Authentication mechanisms are designed to allow secure access to systems and services. These systems and services can be online websites which require user login, an ATM machine, which requires a PIN code to validate the card, various buildings which require authorized access to enter, or even our own phones. Many attacks can be made against authentication, allowing illegitimate access and impersonation of the legitimate user. In order to prevent this, more secure authentication schemes must be developed and deployed so that confidentiality, integrity and availability are guaranteed.

Mobile devices are nowadays very computationally able, have internet connection (3G and WIFI) and can store huge amounts of sensitive information and data. These mobile devices' capacities stared to be harvest in almost every sector (e.g. Healthcare sector [2] and Identity management sector [3]). Furthermore most of the time, mobile devices are personal devices, so personal and sensitive data is usually stored in them. This type of information may not be desirable to be accessible by anyone other than their owner. To keep this information from leaking out into the hands of others, mobile devices provide various security mechanisms. The most commonly used security and authentication mechanism is PIN codes or passwords. However, these mechanisms are not very secure, depending on various factors. For example, PIN numbers tend to be small and have a very small number of combinations, usually 4 digits, which is easily crackable by brute-force attacks; and passwords tend to be crackable, as most users do not bother with making them secure, and usually use very simple and guessable passwords.

This leads us to another problem. Users usually tend to neglect security in favor of convenience. Most users disable security mechanisms that are too complex and are too much of a burden for them. Many do not know the concept of secure passwords or authentication mechanisms or simply do not care. [4] Secure systems can be too annoying or burdensome, usable systems can be too insecure. So, in order to introduce proper security behavior, we must find a balance between usability and security.

These days, almost everyone has a smartphone. And these already come with various security mechanisms embedded in them, that can attest to the user's identity [5], usually provided by the phone's network provider, to strongly authenticate their users. They are also protected by authentication mechanisms,

to protect their data. Many other alternative mechanisms may be developed, to take advantage of their computing power, and usual components. Knowing this, smartphones can be used as secondary authentication devices that can authenticate the user in a more secure, reliable and certain way.

A. Authentication Factors

There are three types of authentication factors in which a user can be identified by the system. These can be used independently, or together, depending on the complexity and certainty that the system requires. The more factors the authentication uses, the more certain the identification is. [6, 4] The three factors are:

- Knowledge, or something the user knows (e.g. PIN, text based and pattern based passwords);
- Ownership, or something the user has (e.g. token, smart card, USB dongle);
- Inherence Inheritance or something the user is (e.g. biometric data like fingerprints, facial or voice recognition). This can also be divided into two types: Static (something the user is that cannot be modified) and dynamic (something the user does).

B. Identity Attacks

There are various types of attacks that can be done in order to obtain illegitimate access. They can be divided into [6]:

- Capturing (e.g. social engineering, shoulder surfing, spyware, eavesdropping);
- Cracking (e.g. guessing, dictionary, brute-force, and a mixture of dictionary and brute-force attacks);
- False identities (e.g. spoofing, man-in-the-middle);
- Physical attacks (e.g. theft, duplication)

The use of mobile devices usually involves situations in which there is no control of conditions such as lighting and levels of noise. This results in an unstable performance of biometric authentication methods and slows down their acceptance and deployment.

In this paper, we review various existing and proposed methods of authentication to access mobile devices and using mobile devices.

The paper is organized as follows: Section 2 explains the research methods and stages to obtain the material. Section 3 presents the results and surveys what has been obtained. Section 4 discusses and comments on the presented results. In Section 5, we derive our conclusions and what lessons can thus be inferred.

II. METHODS

This literature review was performed on January 28th, 2013 with searches in IEEE Xplore and ACM Digital Library. We applied the following queries:

- "*[ANY FIELD] ((authentication mobile devices) OR (authentication) AND (device))*" in IEEE Xplore
- "*[ANY FIELD] authentication mobile devices*" in ACM Digital Library

Due to the highly number of results obtained, we filtered the abstracts following severe exclusion criteria:

1. English as language;
2. Articles with less than 10 years;
3. Articles with high relevance on the search engines;
4. A cautiously review of the abstracts to exclude articles with the same or outdated authentication schemes.

After the article selection 12 articles were obtained. The full text articles were obtained by using the university of Porto network associated with the "*Biblioteca do Conhecimento Online"* (Online Knowledge Library) also known as *b-on*.

III. RESULTS

The obtained results can be divided into two separate authentication scenarios:

- *Authentication on the mobile device* where the user have to authentication himself in order to access his mobile device.
- *Authentication with the mobile device* where the user uses one or more mobile device credential to authenticate him in other systems.

A. Authentication on the Mobile Device

A.J. Nicholson et al. [1] propose a process of Transient Authentication: a small wearable token with short range wireless link and modest computational resources that constantly authenticates the user. When the device and the token part, the user is no longer authenticated and the device secures itself, and encrypts, flushes, and overwrites data depending on what type of data or storage it is securing. It relies on the following principles:

1. The device should only perform sensitive operations when the user is present. All encryption keys must reside on the token, which is worn by the user at all times.
2. No burdensome user interaction.

3. Securing and restoring the devices must not take too long, to prevent attacks, and to allow the system to be quickly ready for use from the user's perspective.
4. The device must not do anything regarding sensitive information without the user's consent and must guarantee the authenticity of the user's token and that it is not talking to other devices without the user's knowledge. They exchange public keys in order to do this.

Users must authenticate themselves on the token at least once a day, to secure the keys kept on the token as they would secure their office doors by opening them in the morning. Devices and tokens bind themselves to prevent attacks from others sitting nearby.

Jian Wang et al [7] propose a secure authentication and authorization protocol that employs a combination of MTM (mutually trusted modules) and biometric identification. Different users are able access different information and applications which are associated with different security levels. Users, devices and USIM (identifying SIM cards) can mutually authenticate and exchange encrypted messages.

Mobile devices are provided with some security elements by the network provider and manufacturers: For example, the IMEI, mobile network access authentication parameters, PIN and PUK on the USIM. The mutual trusted module is assumed to have private keys and public certificates.

Integrity checking is done by mutual authentication between the mobile device and the USIM using public key cryptography. The mobile device and USIM can both judge if they have the same owner.

This scheme uses variable authentication. If it requires stronger security, biometric data is used. Otherwise, a pass word is used.

Four security levels define which resources the device enables regarding the integrity checking performed by the mobile device and the USIM, and which authentication methods to use. Lower levels of security give access to fewer resources, and weaker authentication. Higher levels of security give access to more resources and require stronger authentication.

Xiaobu Yuan et al. [8] propose an authentication system capable of dynamically selecting combinations of normalization and fusion methods for optimal performance in working environments, using combined biometric data. This involves situations with no control of lighting and levels of noise. This results in an unstable performance of biometric authentication methods which slows down their acceptance and deployment.

Specific biometric techniques, such as normalization and fusion methods perform face and voice recognition. Combined approaches get fewer errors than standalone recognition in most scenarios. Dynamic selection of normalization and fusion techniques is needed as no method is better than the other on all cases. Dynamically selected combinations of authentication methods always outperform other methods. This approach needs limited processing power in the mobile device, since it only needs to capture the authentication data and send it to an authentication server.

Eiji Hayashi et al. [9] tackle the problem that mobile phones only support two access control states: locked or unlocked. They investigated user's reaction to different biometric authentication unlocking methods. They used five different types of authentication mechanisms: PIN, password, security questions, face recognition and combination of voice+face recognition (although, the biometric methods were simulated, and none of the participants knew about it).

Users were asked to divide their favorite applications into:

- Always available;
- Available on unlock;
- Mixed.

Most participants wanted the applications containing personal data to be only accessible after unlock. And applications that did not contain personal data were put in the always available situation. Voice+face combined recognition was preferred, despite believing that it might not be as secure as a password or PIN. PINs are preferred when the device is supposed to be a shared device, for their simplicity.

Using authentication levels, by performing biometric authentication as a weak authenticator and PIN or password for stronger authentication was a scenario that participants would like to see implemented.

Shari Trewin et al. [10] studied the usability of different biometric authentication methods: face, voice and gesture, regarding authentication time, error rates, the impact of the user actions required for authentication on performance in a memory recall task and their reaction to the authentication method itself, comparing them to traditional systems.

Voice recognition was the fastest authentication method, but photo recognition supported better performance in memory recall task. Voice verification was considered less usable than password, face and gesture recognitions. Combinations of authentication methods were very unpopular. Combining methods led to higher error rates.

Each biometric has the potential to improve on the traditional password approach. Face and Voice recognition are fast, but do not work for everybody, gesture recognition is reliable, but takes too long, face recognition win in the memory task context. Voice recognition is considered less usable than password, face and gesture recognitions.

Natural speaking voice did not meet the required quality; Face recognition poses a challenge even in good conditions. Combined biometric approaches were disliked, were more prone to failing to acquire and had a lower performance on the memory recall task.

Hamed Ketabdar et al. [11] propose a method of authentication using 3D magnetic signatures created in the air, using a small hand-held magnet. It uses the compass present in most current smartphones. This signature is created freely in the space around the device by a magnet held in hand. The movement of the magnet creates a temporal change in the magnetic field that is sensed by the compass. They adapt a template matching algorithm called multi-dimensional Dynamic Time Warping to analyze different 3D magnetic signatures and authenticate users. They compare the saved signature to the authentication signature by comparing the differences between the signal's speeds and timing. The magnetic detection does not suffer from illumination and occlusion problems.

Roland Schlöglhofer et al. [6] suggest an authentication system which tries to meet requirements of security and us-ability. This system offers traditional PIN and password, but also an ownership-based authentication method using NFC tags, and an image-based method.

The SecureLock Android application acts as a lock screen and implements various authentication methods. It allows all three factors of authentication discussed previously:

- The knowledge-based authentication (PIN, password, unlock pattern, gesture puzzle);
- The ownership-based authentication (NFC);
- The inherence-based authentication (Face-unlock);
- Combination of Knowledge/Ownership-based authentication (GesturePuzzle+NFC).

Using this application, and analyzing possible attacks done to the implemented authentication mechanisms, it was found that the combined Knowledge/Ownership-based authentication to be the most secure overall, as it combines various authentication mechanisms. In terms of usability, NFC and PIN are the most convenient usage cases. Although the combined Knowledge/Ownership-based authentication presents good results its complexity and duration of the mechanism are a burden to the application itself.

B. Authentication with the Mobile Device

Min-Hsao Chen et al. [12] propose an authentication method based on identifying the ownership and the location of the mobile devices, assuming that most users have with them a personal mobile phone device that can be used as a secondary authentication device. The devices use broadcast signals from wireless access points as location markers. The location information is used as a means of authentication by associating the user with the location of the device. This method uses the WLAN Access Point BSSIDs and SSIDs and the corresponding signal strength to triangulate the location of the user.

Stationary APs provide a relative location for the device. They do not need to be associated. The mobile device scans for broadcasting wireless APs and measures their strengths. The centralized server is the meeting point for the authentication system. It stores the username, password and AP information and compares it to the information given by the mobile device, the authentication device and the username/password provided by the user. The client authentication device also uses its wireless interface to determine the surrounding AP information.

Andrea Bianchi et al. [13] propose a system which allows users to enter a PIN for an ATM machine on a standard mobile phone and transmit it securely for authentication using modulated patterns of light shown on the phone screen and sensed by a cheap receiver unit.

ATM terminals require you to enter a PIN number in order to access your account. This is effective, but is prone to various attacks. The physical nature of the terminals means that they are in fixed positions, which makes your interactions observable. Their approach is supported in two existing concepts: a channel based on physical contact is resistant to Man-in-the-middle attacks; light can provide a secure out of band channel. It relies on existing technology on the phone, the screen, making it deployable on any device. This provides a secure and usable channel for authentication at public terminals. The results were positive and encouraging as a means of authentication on ATMs.

Shintaro Mizuno et al. [5] propose a system in which the user accesses a service provider through a PC over the inter net and also has a mobile phone (most users have their phone with them all the time) that has identifying capabilities.

This method uses the device's identifier to authenticate the users, without them having to use any personal information. The method binds trusted and non-trusted channels using the PCs session id and the phone's identifier. The authentication works as follows:

1. The user reads a session ID of a communication channel between a service provider and a PC using a barcode reader on a mobile;
2. The mobile device sends the session-id through a mutually authenticated secure channel over a mobile network to the authentication server;
3. The server matches the session-id, binds the user and the communication channel to provide the service to the PC.

Ming Ki Chong et al. [14] try to accommodate the wireless association of devices that have limited input capabilities to recognize a PIN number. This is based on

the use of accelerometers to detect user's movements as inputs for authenticating mobile devices. They are interested in device authentication rather than user authentication.

They rely on gestures made with the mobile devices that will translate to specific inputs (e.g. PIN numbers). This scheme has the same type of security of a traditional PIN number as they tackle input limitations, rather than security. Once a connection terminates, the passkey is discarded

IV. DISCUSSION

Several authors dedicate their research to the proposal and development of Authentication methods using mobile devices, and to access mobile devices. Our study allows the notion of what there is in the field of user authentication, and what alternatives to traditional password and PIN systems are being proposed and developed.

Encryption of personal and sensitive information is not the challenge tackled by most of these proposals. They aim to achieve security and privacy by the means of authentication methods that diminish attacker's ability to obtain someone else's personal information. Albeit some authors still use encryption schemes, to ensure security when using untrusted channels [1, 7, 12].

When proposing and developing authentication methods, there are two factors to take in to consideration [1]: security and usability. Secure systems can be too annoying to actually use, and usable systems can be too insecure to actually have security over sensitive information.

There is a separation in methods regarding the number of device states. Some authors propose systems based on a single authentication methods [1, 12, 13, 5, 11], like A.J. Nicholson [1], which proposes a token-based authentication system in which only one authentication system guards all type of data and applications. This means the device is either locked and nothing is accessible, or it is unlocked and everything is accessible. On the other hand, other authors [7, 8, 9] propose the use different security levels for different types of data, applications and resources. Higher security levels allow the use of more resources and require stronger authentication methods.

We see that methods that authenticate a user to a service or system using mobile devices usually is approached with the single authentication method, allowing all-or-nothing access to the system, which will only then take care of the access control. It would be interesting to see these methods try an approach with multiple levels of security, as seen on some proposals of authentication on the mobile devices.

The most approached authentication methods, as alternatives to traditional PIN or password methods, are biometric approaches. The specific type of approaches does not usually vary, as they tend to study mostly face and voice recognition.

Biometric approaches can be a very unstable type of authentication method, as there is no control in conditions such as lighting and levels of noise that can deteriorate the samples and perform poorly. This slows down their acceptance [8].

Another much approached scheme is the use of combined authentication methods that together, act as more accurate authenticators than standalone. This may be a solution for the poor performance of biometric methods in bad conditions. The most tried and used combination was face+voice recognition, which got the best overall results. However, despite the results, users seem to dislike them, as they are not as practical as passwords or PINs.

One of the big obstacles to alternative authentication methods can be the ignorance or negligence of the users. Many seem to believe that biometric approaches may not be as secure as password or PINs [9]. However, other studies [4] actually show that people know that these methods are insecure. The convenience of these alternative methods is also a challenge.

In terms of the authentication factors that are studied, the most explored is clearly the inherence (something I am) employed by biometric authentication. But there are also other schemes that use alternative Knowledge-based methods other than passwords of PINs.

V. CONCLUSIONS

This paper presents a review on current existing and authentication methods regarding access to mobile devices and authentication using mobile devices. We collected various papers on these subjects where authors described their proposals and used different methods of authentication, each one tackling a specific or a combined set of authentication factors.

Although we approached distinct use cases, and these distinct cases use different approaches, they can be used as a means to authenticate in all cases. For example, biometry can be used in the case of authentication with the mobile phone, not only to authenticate in the phone.

Another approach, which is the one we are interested in, is in combining both approaches. Meaning, that we want to be able to authenticate users on the mobile device (for ex ample, a smartphone), and with that, use the same device, to authenticate the user on another system. If we can prove to the device that we are the user we say we are, that device could act as an authentication token that strongly proves our identity. This way, we need not fear that the device could end up in the wrong hands, as it would be useless without our means of authorization.

Access to the device could be done with biometric methods of authentication, which provides the Inherence-based authentication (something that we are). With that, the smartphone acts as a token, providing an ownership-based

authentication (something that we have). These two factors of authentication provide and guarantee more security and better access control to our sensitive information.

Another thing this scheme could borrow from this research is to have different access levels, So that only when we need to access sensitive information do we need to perform such strong authentication. When only trying to access non-sensitive resources, we could only ask for a simple pass word, as it is less burdensome.

ACKNOWLEDGMENTS

This work is funded by the ERDF through the programme COMPETE and by the Portuguese Government through FCT - Foundation for Science and Technology and executed by the project Open Federated Environments Leveraging Identity and Authorization [PTDC/EIA- EIA/104328/2008]. and is being con ducted with the institutional support provided by FMUP and DCC/FCUP and the facilities and research environment gracefully provided by the CINTESIS and CRACS (Center for Research in Advanced Computing Systems) research unit, an INESC TEC associate of the Faculty of Science, University of Porto.

REFERENCES

[1] A.J. Nicholson, M.D. Corner, and B.D. Noble. Mobile device security using transient authentication. *Mobile Computing, IEEE Transactions on*, 5(11):1489 –1502, nov. 2006. 1, 2, 5

[2] Cátia Santos-Pereira, Alexandre B. Augusto, Manuel E. Correia, Ana Ferreira, and Ricardo Cruz-Correia. A mobile based authorization mechanism for patient managed role based access control. In Information Technology in Bio- and Medical Informatics, volume 7451 of Lecture Notes in Computer Science, pages 54–68. Springer Berlin Heidelberg, 2012. 1

[3] Alexandre B. Augusto and Manuel E. Correia. Ofelia - a secure mobile attribute aggregation infrastructure for user-centric identity management. In Proceedings of the IFIP SEC2012 (International Information Security and Privacy Conference), Crete, Greece, June 2012. Springer IFIP Advances in Information and Communication Technology. 1

[4] Noam Ben-Asher, Niklas Kirschnick, Hanul Sieger, Joachim Meyer, Asaf Ben-Oved, and Sebastian Moller. On the need for different security methods on mobile phones. In Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services, MobileHCI '11, pages 465–473,New York, NY, USA, 2011. ACM. 1, 2, 5

[5] Shintaro Mizuno, Kohji Yamada, and Kenji Takahashi.Authentication using multiple communication channels. In Proceedings of the 2005 workshop on Digital identity management, DIM '05, pages 54–62, New York, NY, USA, 2005. ACM. 1, 4, 5

[6] Roland Schloglhofer and Johannes Sametinger. Secure and usable authentication on mobile devices. In Proceedings of the 10th International Conference on Advances in Mobile Computing; Multimedia,MoMM '12, pages 257–262, New York, NY, USA, 2012. ACM. 2, 4

[7] Jian Wang and Nan Jiang. Secure authentication and authorization scheme for mobile devices. In Communications Technology and Applications, 2009. ICCTA '09. IEEE International Conference on, pages 207 – 211, oct. 2009. 3, 5

[8] Xiaobu Yuan and M.S. Rahim. User authentication on mobile devices with dynamical selection of biometric techniques for optimal performance. In Robotics and Biomimetics (ROBIO), 2010 IEEE International Conference on, pages 333 –338, dec. 2010. 3, 5

[9] Eiji Hayashi, Oriana Riva, Karin Strauss, A. J. Bernheim Brush, and Stuart Schechter. Goldilocks and the two mobile devices: going beyond all-or-nothing access to a device's applications. In Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, pages 2:1–2:11, New York, NY, USA, 2012. ACM. 3, 5

[10] Shari Trewin, Cal Swart, Larry Koved, Jacquelyn Martino, Kapil Singh, and Shay Ben-David. Biometric authentication on a mobile device: a study of user effort, error and task disruption. In Proceedings of the 28th Annual Computer Security Applications Conference, ACSAC '12, pages 159–168, New York, NY,USA, 2012. ACM. 3

[11] Hamed Ketabdar, Peyman Moghadam, Babak Naderi, and Mehran Roshandel. Magnetic signatures in air for mobile devices. In Proceedings of the 14th international conference on Human-computer interaction with mobile devices and services companion, MobileHCI '12, pages 185–188, New York, NY, USA, 2012. ACM.3, 5

[12] Min-Hsao Chen and Chung-Han Chen. Secondary user authentication based on mobile devices location. In Networking, Architecture and Storage (NAS), 2010 IEEE Fifth International Conference on, pages 277 – 281, july 2010. 4, 5

[13] Andrea Bianchi, Ian Oakley, and Dong Soo Kwon. Using mobile device screens for authentication. In Proceedings of the 23rd Australian Computer-Human Interaction Conference, OzCHI '11, pages 50–53, New York, NY, USA, 2011. ACM. 4, 5

[14] Ming Ki Chong, Gary Marsden, and Hans Gellersen. Gesturepin: using discrete gestures for associating mobile devices. In Proceedings of the 12th international conference on Human computer interaction with mobile devices and services, MobileHCI '10, pages 261– 264, New York, NY, USA, 2010. ACM. 4