ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 7, Issue, 02, pp.12805-12807, February, 2015

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

REVIEW ARTICLE

TWO WAY MOBILE AUTHENTICATION SYSTEM

Bableen Osan, Ekta Lakhwani and *Divya Mulchandani

Department of Computer Science and Engineering, Jhulelal Institute of Technology, Nagpur, India

ARTICLE INFO

Article History:
Received 04th December, 2014
Received in revised form
29th December, 2014
Accepted 05th January, 2015
Published online 28th February, 2015

Key words:

Two Way Mobile Authentication,
PIN (Personal Identification Number),
Facial Scan, Security and Smart Phone.

ABSTRACT

When it comes to security, most mobile devices are a target waiting to be attacked. This arises the need for security. There are certain domains wherein the confidentiality of information is of utmost importance and needs to be protected from unauthorized users. Hence, authentication is used for protection of this information. The usage of authentication techniques has been persistent in the domain of security. However, older techniques are now more vulnerable and fail to provide the same level of protection as they once did. Hence, there is an arising need for the advent of new techniques that make use of authentication at increased complexity so that level of security is enhanced. Two Way Mobile Authentication Systems (2WMAS) describes the methods for implementing stronger authentication in smart phones. The two approaches being used in two way mobile authentication system are- Something you know: Personal Identification Number (PIN) something you are: Facial Scan

INTRODUCTION

In the ever-changing world of global data communications, inexpensive Internet connections, and fast-paced software development, security is becoming more and more of an issue. Hence, security is now a basic requirement for every smart phone. Traditional cryptography solutions use symmetric and asymmetric keys to perform encoding and decoding of given messages or data. Applying these existing solutions on mobile devices to support mobile accesses encountered several issues in a wireless network environment. They are

A. Weak and unreliable connectivity.
B. Limited processing power and memory.
C. Limited battery operation time.
D. Very limited inputs.

To deal with these issues in a wireless network environment, there are several approaches to using key-based security techniques

a) Offloading complex computations to a server.
b) Reducing network traffic with better protocols.
c) Allowing cryptography algorithms to run in offline (disconnected) modes.
d) Improving cryptography algorithms.
e) Adding specialized chips to perform cryptography.

Corresponding author: Divya Mulchandani,
Department of Computer Science and Engineering, Jhulelal Institute of Technology, Nagpur, India.

A brute-force approach uses symmetric or/nd asymmetric key cryptographic techniques without considering the limitations of mobile devices and networks. In current wireless networks, such as GSM and GPRS, only private keys (or symmetric keys) are used to implement cryptographic solutions. They are useful to authenticate the mobile users and mobile devices to a provider system. Another brute-force approach (**Grecas, 2003**) uses a public key-based cryptographic solution. The major problem using public keys in encryption/decryption is its complex algorithm and higher processing time.

Recently, some published research papers proposed mobile key-based security solutions by modifying existing public-key algorithms. As known, most people still prefer to use asymmetric-key cryptographic techniques on mobile devices over symmetric-key cryptographic techniques. However, they be must be customized and improved for the use on mobile devices. There are innovative approaches using a combination of new cryptographic algorithms based on data distribution, time distribution, and workload distribution.

The main purpose of two way mobile authentication is to provide stronger authentication in smart phones that will decrease the probability that the requestor is not who he/she claims to be.(i.e., providing false evidence of his/her identity.

Literature survey

Modern cryptography intersects the disciplines of mathematics, computer science, electrical engineering and many others. Cryptography is the practice and study of techniques for secure

communication. More generally, it is about related to various aspects in information security, data integrity, authentication and non-repudiation. Applications of cryptography include ATM cards, computer passwords, and electronic commerce. It is heavily based on mathematical theory and computer science practice (Fig 1). Cryptographic algorithms are designed around computational hardness assumptions, making such algorithms hard to break in practice by any adversary.

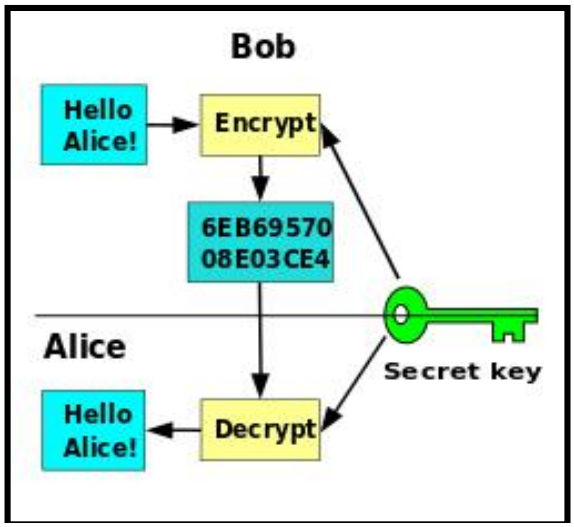

Fig. Cryptography

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted). Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality. Many have been thoroughly broken, such as FEAL. Two Factor Authentication (2FA) is where a user's credentials are made up of two independent factors such as

A. Something you know

Methods based on something the user knows are often associated with a password, 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. This same password has to be provided by the user for every future use of the service.

B. Something you are-

According to Wikipedia, 'Bio' means 'life' and "metrics" means 'measurement'. Biometrics is the measurement of characteristics of human being. Biometric security is a security mechanism or technology, provided in a given application environment (or systems), identifies the individuals and their accesses of the systems by measuring their physical or behavioural attributes. Because of the uniqueness exhibited by these attributes of mobile users, it is possible to uniquely identify them and their accesses on the mobile devices. Some of the biometric examples are explained below

1. Fingerprint Technology- The fingerprint technology is the oldest one among all biometric identification. It is based on the series of three dimensional lines, called ridges, and the space between then, called valleys. The ridges and valleys are unique to a person and therefore help to verify the identity. The location on the fingerprint where the ridges begin, stop, fork or intersect is called Minutiae. By extracting minutiae, it is possible to retrieve key features of a fingerprint. Matching the minutiae and the number of ridgelines between neighbouring minutiae is used as methods for personal identification.
2. Voice identification- Voice-based biometric security technology identifies authentic mobile users based on their voice inputs. A voice biometric solution provides a stronger security as compared to other non-biometric security solutions.
3. Facial scan- Face recognition biometric systems are considered as the most effective security solutions for mobile users. They require a camera to capture the mobile user's facial image. Since most mobile phones today are equipped with a camera, the major technology concern is how to provide efficient face recognition algorithms to process captured images with the limited memory storage on mobile devices.

Existing security tools

1. Google Authenticator is an application that implements TOTP security tokens from RFC6238 in mobile apps made by Google, sometimes branded "two-step authentication". Authenticator provides a six to eight digit one-time password users must provide in addition to their username and password to log into Google services or other sites. The Authenticator can also generate codes for third party applications, such as password managers or file hosting services. Previous versions of the software were open source.
2. App Lock can lock SMS, Contacts, Gmail, Facebook, Gallery, Market, Settings, Calls and any app you choose, with abundant options, protecting the user's privacy. App Lock can hide pictures and videos, App Lock empowers user to control photo and video access.

Proposed system

The Interface Builder tool has been utilized as well to get access directly from Android Eclipse, which has a user interface for the application. With this tool, the user interface can be designed in a graphic way, making easy great part of the task. Another tool used is the Android Eclipse Emulator, to test the progress during the development of the application. In the first stage of development, Two way mobile authentication application is strongly dependent to create the password and the security question. In the second stage of development, all the features of the face will be scanned and we can see the list of applications that can be locked or unlocked depending upon the choice of the user.

Two Way Mobile Authentication Systems provides two main functionalities

A. Pin- It will allow users to set the pin and the security question, when they open the application for the first time
B. Facial Scan- It will allow the user to scan his face after successful pin authentication.

Applications

Two way mobile authentication systems can be used in institutes for attendance. It can also be used in sensitive areas like military and banks and further we can implement it for tablets.

Conclusion

This hybrid authentication provides a higher level of security and reliability provided by the asymmetric technique in smart phones. During our research we identified the main authentication methods that are used today both for mobile and stationary devices and studied their main characteristics. Beside their general theoretical characteristics that we found in documentation we additionally tried to see what people think about them, how they accept them and do they think they are suitable for current and future services. Based on previous work, our main conclusion is that there are many approaches for user authentication for mobile devices 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

Aloul, F., Zahidi, S. and El-Hajj W. Two Factor Authentication Using Mobile Phones, IEEE/ACS International Conference on Computer Systems and Applications

Beumer G., A. Bazen, and R. Veldhuis, "On the accuracy of EERs in face recognition and the importance of reliable registration," in Proc. SPSIEEE Benelux DSP Valley, 2005, pp. 85–88.

BioID, BioID Face Database. (Online). Available: http://www.humanscan.de/

FERET, FERET Face Database. (Online). Available: http://www.itl.nist.gov/iad/humanid/feret/

Furnell, N. L. C. a. S. M. Authentication on users on mobile telephones – A survey of attitudes and practices. Computers and Security, 2005 24(7): p. 519-527.

Harris, J. A. A One Time Password Scheme .International conference on Parallel Processing Workshops, 2002 Proceedings.

Hielmas and B. Low, "Face detection: A survey," Comput. Vis. Image Underst., vol. 83, no. 3, pp. 235–274, Sep. 2001.

http://www.ijcaonline.org/archives/volume75/number2/13085-0341

http://www.ijirs.com/vol2_issue-5/12.pdf

http://www.medieteknik.bth.se/fou/cuppsats.nsf/all/df07117852a2263bc125775f00359561/$file/Thesis_MEE10_36_1.pdf

IAshchenko 2002. "*Cryptography: an introduction*". AMS Bookstore. P.6. ISBN 0-8218-2986-6.

Ronald Cramer, Victor Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure Against Adaptive Chosen Cipher text Attack", Aarhus University, New York University, Aug., 2003.

Whitfield Diffie and Martin Hellman, 1976. "New Directions in Cryptography", IEEE Transactionson Information Theory, vol. IT-22, Nov. 1976, pp: 644–654.

****