BIOMETRIC SYSTEM PENETRATION IN RESOURCE CONSTRAINED MOBILE DEVICE

M.SUJITHRA[1] AND DR G. PADMAVATHI[2]

[1]Assistant Professor, Department of Computer Technology & Applications,
Coimbatore Institute of Technology,
Email: sujisrinithi@gmail.com

[2]Professor& Head, Department of Computer Science,
Avinashilingam Institute for Home Science and Higher Education for Women,
Coimbatore, Tamil Nadu, India.

ABSTRACT

Over the past few years, the usage of mobile devices to access data has becoming more frequent, and the usage of mobile devices in the applications such as web-browsing, email, multimedia, entertainment applications (games, videos, and audios), navigation, trading stocks, electronic purchase, banking and health care are increased, therefore data security is essential and also it becomes a challenge in securing the data in the mobile device. User authentication schemes such as Password or Personal Identification Number (PIN) based authentication in mobile device is a difficult process for providing safe access to precious, private information or personalized services. To address these problems in the mobile devices, biometric system can be developed which are more secure, affordable and memorable authentication scheme based on graphical assistance, images and audio. We believe that biometric authentication is the most secure approach among other authentication mechanism. This paper discusses the various features of biometrics and mobile device security threats.

KEYWORDS

Biometrics, Mobile Device, Authentication, Threats, Security.

1. INTRODUCTION

As mobile devices continue to evolve in terms of the capabilities and services offered, so they introduce additional demands in terms of security. The need for more security on mobile devices is increasing with new functionalities and features made available. To improve the device security we propose biometric authentication as a protection mechanism. The main reason to use biometrics on the mobile device is to protect the data on the device and to provide secure yet convenient access to the device and to the network it may be connected to. Unfortunately, mobile device theft is on the rise and insurance plans are becoming more expensive. It is very common to lose your mobile phone or have it stolen. The use of biometrics protects the data on the device and serves as a theft deterrent since the device is useless to others when it is protected with biometric security. A good biometric solution makes security convenient. New handsets deploying biometric approaches are being announced regularly, with many based upon fingerprint and voice solutions. Other biometrics however is also being introduced some of which are: facial recognition, signature recognition and newer approaches of iris recognition and gait recognition can be used for mobile device authentication. [1]

The remainder of this paper is organized as follows: Section II briefly describes the Mobile Device threats, attacks and their vulnerabilities. Section III presents detailed analysis of Biometric characteristics, its system, including performance evaluation and benefits. Section IV discusses the implementation challenges of biometrics security in mobile devices and Finally Section V concludes this paper.

DOI : 10.5121/ijbb.2013.3104

2. MOBILE DEVICE THREATS, ATTACKS &VULNERABILITIES

The usage of the mobile phone over the last few years has made fundamental changes in our daily life. Mobile devices, namely Personal Digital Assistants (PDAs) and smart phones are containing ever more personal information, including address books, schedules as well as payment information. Smart phones or mobile phones with advanced capabilities like those of personal computers (PCs) are appearing in more people's pockets, purses, and briefcases. Smart phones' popularity and relatively lack security have made them attractive targets for attackers. According to a report published earlier this year (2012), smart phones recently outsold PCs for the first time and attackers have been exploiting this expanding market by using old techniques along with new ones. One example is this year's Valentine's Day attack, in which attackers distributed a mobile picture-sharing application that secretly sent premium rate text messages from the user's mobile phone. [2]

2.1 SECURITY THREATS FOR MOBILE PLATFORMS

Mobile phones are becoming more and more valuable as targets for attack. People are using smart phones for an increasing number of activities and often store sensitive data, such as email, calendars, contact information and password on the devices. Mobile applications for social networking keep a wealth of personal information.

2.1.1 VULNERABLITY

A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.

2.1.2 THREATS

People eager, willing, and qualified to take advantage of each security weakness and they continually search for new exploits and weaknesses.

2.1.3 ATTACKS

Threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically the network devices under attack are the endpoints such as servers and desktops.Table 1 shows the various attacks on mobile devices. [3]

Table 1: Various Attacks on Mobile Devices

Attacks Causes (Features)	Attack Type	Mobile Security Affects
Mobility	Lost or theft device	Authentication, Confidentiality
Limited resources	DoS(Denial of Service)	Data Integrity, Confidentiality, Availability
Strong Connectivity Requirement	Viruses or worms (malware)	Data Integrity, Confidentiality, and Charging

Several major security issues loom over the use of such devices, including

- Mobile devices are often stolen or missing, due to their small size.
- The contents in the mobile devices are unencrypted or encrypted under a flawed protocol.
- Mobile devices are pron to middle-man attack or viruses attack from wireless connection

- User authentication is weak or disabled or in a common default mode, the authentication mechanism is single static password authentication can be circumvented easily. Figure 1 illustrates the various threats in mobile environment.

To overcome the security problems mentioned above, mobile locks or laptop locks are general solution for better guardian of such devices physically. In order to enhance the security in data, biometrics authentication can be used with complicated algorithms are practiced.[4]

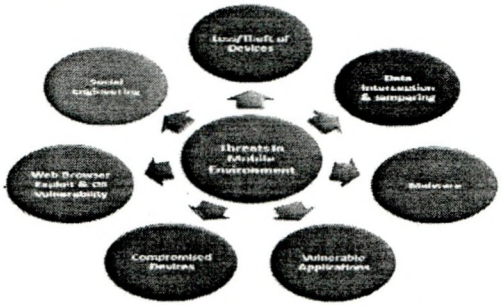

Figure 1. Various threats in mobile environment

2.2 VARIOUS MOBILE DEVICE PLATFORMS

To protect data on mobile devices, it is important to know about mobile device operating systems that power most of today's smart phone and tablets.

Apple's iOS: Incredibly popular operating system from Apple, running devices such as the iPhone, iPad, iPod Touch, and Apple TV.

Google's Android: Google's mobile device operating system, powering devices from several device manufacturers.

Microsoft's Windows Phone: A newer operating system from Microsoft that ships on devices from a variety of vendors. Windows Phone 7 represents a complete redesign of Microsoft's previous operating system, Windows Mobile 6.5.

Blackberry: A long-standing favorite in the enterprise due to security and manageability features. The i-OS and Android platforms have increased in popularity in recent years and have become alternatives to Blackberry in many enterprises.

Nokia's Symbian: Open-source operating system managed by Nokia. In 2011, Nokia announced that it would begin building devices based on the Microsoft Windows Phone operating system, rendering the future of Symbian questionable. [5]

3. BIOMETRIC SYSTEM OVERVIEW

Biometrics is a method of recognizing a person based on his/her unique identification. Biometric identification is often used in large-scale systems such as computer systems security,

secure E-banking, Mobile devices, smart cards, credit cards, secure access to buildings, health and social services. Biometric system refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. It is generally a pattern recognition system that makes a personal identification by establishing the authenticity of an individual. Authentication using biometric characteristics is more convenient because they cannot be forgotten, lost, or stolen which ensures the physical presence of the user while offering a significantly higher security. One individual has three possibilities to prove its identity:

a) Something an individual DATA (e.g., a password, Personal ID Number (PIN), the combination to a lock, a set of facts from a person's background).

b) Something an individual POSSESSES (e.g., a token or card, a physical key to a lock).

c) Something an individual IS (Intermediate System) (e.g., personal characteristics or "biometrics" such as a fingerprint, Iris, voice pattern).

Generically biometrics is categorized in two types: physiological and behavioral. Physiological approaches perform authentication based on a physical attribute of a person, such as their fingerprint, face, Iris, Retina, Hand Geometry and Ear. By contrast, behavioral biometrics utilizes distinct features in the behavior of the user to perform the relevant classification, such as their voice, signature, and key stroke. Physiological biometrics tend to be more trustworthy approaches, as the physical features are likely to stay more constant over time and under different conditions, and tend to be more distinct within a large population . For this reason physiological approaches are often used in identification-based systems, whereas behavioral characteristics (which tend not to have such unique characteristics and vary more with time) are therefore mainly used for verification purposes.[6] Figure 2 describes user authentication types.

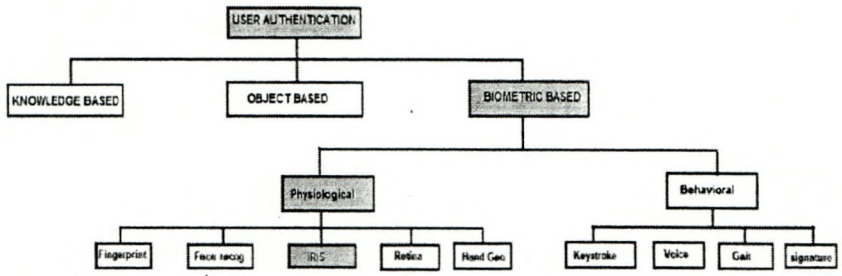

Figure2. User Authentication Mechanism

3.1 CHARACTERISTICS OF A BIOMETRIC SYSTEM

As defined by the International Biometric Group (IBG) biometrics is "the automated use of physiological or behavioral characteristics to determine or verify identity". As can be seen in the definition, biometrics can be used in two distinct modes: identification to determine identity and verification to verify a claimed identity.

Identification: In this mode the biometric system reads a sample from the user and tries to find a match by looking at the entire database of registered users. A 1: N comparison is performed and thus is often more demanding in terms of distinctiveness of the biometric characteristics.

Authentication/Verification: In this mode the system tries to verify a claimed identity. The user provides a sample and an identity (e.g. a username). The system retrieves the template that it keeps relative to the claimed identity and checks whether the newly acquired sample matches that template. This is a 1:1 comparison and is in general a much easier procedure to implement as it can be less demanding in both processing and distinctiveness of the features.

3.2 BIOMETRIC SYSTEM METHODOLOGY

Regardless of the biometric technique or the comparison mode utilized, the way in which the biometric process takes place is identical. Figure 3 illustrates the generic biometric system where the two key functions of the biometric authentication process are shown enrolment and authentication.

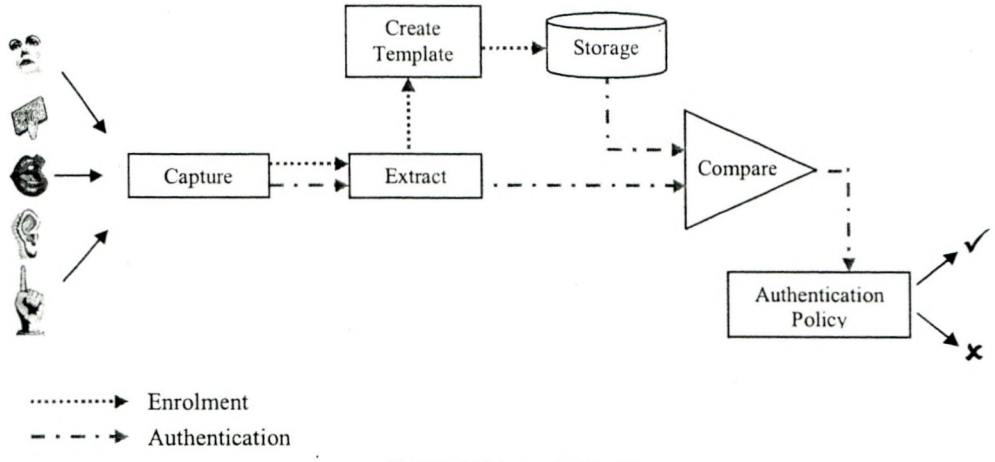

Figure 3. Biometric System

Enrolment represents the procedure where the user provides the biometric information to the system for it to store and generate a reference profile for subsequent authentication. The biometric sample is captured by an appropriate sensor and the reference template is generated through the extraction of features that the system requires to use for authentication. The reference template is then stored to the template database for it to be used in future.

Authentication represents the process that takes place when a user requests access to the system. At that time, an identification or verification of his identity must take place in order to be established as a legitimate user. A new sample is acquired from the sensor, which is subsequently compared to the reference template. The result of this comparison goes through the authentication policy of the system which determines whether the sample and template are matched closely enough to recognize the user as legitimate. [7]

3.3 BIOMETRICS PERFORMANCE EVALUATION

Biometrics does not operate like passwords, where the correct input of the secret knowledge can assure access to the system with 100% accuracy. With biometrics a legitimate user might

provide a sample, but several factors may still cause them to be rejected by the system. These factors might be environmental (e.g. a bad acquisition from a fingerprint sensor due to a cut finger or inadequate lighting for face recognition or too much background noise for voice verification) or related to the underlying uniqueness of the characteristics involved. This might not only lead to rejecting an authorized user but also in accepting an impostor. The quality metrics used to evaluate the performance of the biometric system are as follows:

False Acceptance Rate (FAR), which represents the probability of an impostor getting accepted by the system (sometimes referred to as the Impostor Pass Rate).

False Rejection Rate (FRR), which represents the probability of falsely rejecting an authorized user (sometimes referred to as the False Alarm Rate).

Failure to Enroll Rate (FTE), which refers to situation where the sample is not able to provide enough information to create a template. That can be due to noise from the capture or a lack of features from the user, for example burned fingers.

Failure to Acquire Rate (FTA), which refers to the situation where the system is unable to acquire a sample from the user. [8]

3.4 BIOMETRIC SYSTEM BENEFITS

A biometrics security system offers the following benefits:

- **Guarantees physical location of the user &High-throughput.**
  It can be determined with certainty that the user was that the point when and where the biometric template collected. When there is a need to identify a person from a large population, automatic biometric identification may be the only efficient solution.
- **Biometric trait is unforgettable, cannot be lost and shared.**
  Unlike the classic passwords that need to be remembered, biometric traits cannot be forgotten because they represent something that the user is: physically or behaviorally. Unlike authentication tokens, ID cards or passwords written on a piece of paper, biometric traits cannot be lost. Due to their nature biometric traits cannot be shared between users. This ensures that the user that logs in the system is the actual user and not a colleague that is trying to help.
- **It is appealing & cost efficient.**
  Most people find biometric systems appealing because of the ease of use and because it is impressive how a door can be opened by just a swipe of a finger. Sure there will be an upfront cost with the installation of the system and with user's education but in the long run it proves cost efficient due to the benefits listed above. It cannot be shared and it guarantees physical location this way no employee can help-out a colleague that is late by punching-in in the time system on his behalf. And it cannot be lost or forgotten this way costs of reissuing new identification tokens are reduced, the desktop support time is reduced because the need of resetting passwords will be less, if any, and the down-time of the employees because they've got locked out from the systems is also reduced.
- **It can provide emergency identification &prevents identity theft.**
  In those cases when a person cannot identify itself, using a biometric system may be the only way to find his identity. In the most cases of identity theft, the impostor used victim's name and personal identification number to create credit card accounts and use those in his behalf. Using biometric security systems makes it practically impossible for impostors to pretend they are somebody else.

4. IMPLEMENTATION CHALLENGES IN MOBILE DEVICE SECURITY

In recent years, new mobile device technology has inspired many business mobility initiatives. By providing better information whenever and wherever it's needed, mobility streamlines and

accelerates business process, enables businesses to deliver better service, and provides significant competitive advantages. User authentication is the primary line of defense for mobile and handheld devices such as Personal Digital Assistants (PDA). Authentication determines and verifies the identity of the user in the Mobile Device. Because of the limits of mobile devices, implementing mobile security solutions must address the following needs and challenges in building mobile security. [9]

- **Energy saving security solutions**
  The limited battery life and operation time requires mobile security solutions to be implemented in an energy saving approach.
- **Limited applications of existing security solutions**
  The limited computing capability and processing power of mobile devices restrict the applications of many existing complex security solutions, which require heavy processors.

- **Restricted size of screen and keyboard**
  It restricts the input and output capabilities of mobile phones, which in turn cause some security related applications, for example, password protection may not be easy for mobile users. Table 2 lists few biometric traits currently available on mobile handsets.

Table 2: Biometric Applications on Mobile Handsets

Technique	Product/vendor
Fingerprint	NTT DoCoMo
Face	Omron (Omron), Oki Electric (Biometrics.co.uk)
Signature	PDALock (PDALock)
Iris	xVista (Cellular-News)
Gait	VTT (Young)

- **Higher portability and inter-operation issues**
  Since mobile devices may be equipped with different mobile platforms and operation environments, mobile security technologies and solutions must be implemented with a higher portability to address interoperation issues.

- **Mobility & Strong personalization**
  Each device comes with us anywhere we go and therefore, it can be easily stolen or physically tampered, unique owner.

- **Strong connectivity**
  Smart phone enables a user to send e-mails, to check her online banking account, to access lot of Internet services; in this way, malware can infect the device, either through SMS or MMS or by exploiting the Internet connection.

- **Technology convergence**
  Single device combines different technologies which may enable an attacker to exploit different routes to perform her attacks.

- **Reduced capabilities**
  Even if smart phones are like pocket PCs, there are some characteristic features that lack on smart phones, e.g. a fully keyboard. [10]

Some examples of future risks associated with smart phones include

- Data leakage resulting from device loss or theft.
- Unintentional disclosure of data, Attacks on decommissioned devices.
- Network spoofing & Surveillance attacks.
- Financial malware attacks.
- Network congestion.

Although biometric technologies provide effective security solutions for mobile accesses, they have some limitations. For example, when thieves cannot get access to secure properties, there is a chance that they will stalk and assault the property owner to gain access [11]. In 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car (see http://en.wikipedia.org/wiki/Biometric).However, we must also consider the above discussed factors when choosing a proper biometric trait for mobile device authentication.[12]

5. CONCLUSION

The growth in the creation and maintenance of secure identities for mobile devices has created challenges for individuals, society and businesses particularly in mobile added value services (mobile banking, mobile check-in, mobile ticket, et. al) and government security services. Although many obstacles remain, the growth in wireless technology, and the improvement of mobile devices will stimulate growth in the mobile biometrics market. Security has been one of the important elements in Mobile environment. The conventional Pin and Password authentication on mobile devices provides lower level security while biometric authentication offers higher level security. Biometric systems are offering a more convenient way to secure private information stored on mobile device. Biometrics systems are also adding security to remote transactions initiated using a mobile device. Due to the strict requirement for security, biometric systems can be used for authentication purpose. It is because biometric systems are the least vulnerable to intrusions. In fact, researches in the field are growing. Therefore, in the future the industry would expect even wider use of biometric systems in the mobile device authentication.

6. REFERENCES

[1] Anil K. Jain, Arun Ross and Salil Prabhakar, (2004) "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technologies, vol. 14, no. 1.

[2] C.R. Mulliner,(2006) "Security of smart phones", Master's thesis submitted to University of California, Santa Barbara.

[3] M.Sujithra, Dr. G.Padmavathi, (2012)"Mobile Device Security-A survey on Mobile Device Threats, Vulnerabilities and their Defensive Mechanism", International Journal of Computer Applications (IJCA) Volume 56 - Number 14.

[4] Anurag Kumar Jain,DevendraShanbhag(2012) "Addressing Security and Risks in Mobile Applications".

[5] Roberta Cozza, (2011) "Forecast: Mobile Communications Devices by Open Operating System, Worldwide, 2008-2015," Gartner.

[6] Mathew Kabatoff John Dougman, BioSocieties, (2008) "Pattern Recognition: Biometrics, Identity and State – An Interview with John Dougman", 3, 81, 86, © London School of Economics and Political Science, London UK

[7] KresimirDelac, MislavGregic, (2004) "A Survey of Biometric Recognition Methods", 46th International Symposium Electronic in Marine, Zadar, Croatia.

[8] M.Sujithra, Dr. G.Padmavathi, (2012) "Biometrics for Low Power Mobile Devices", International Conference on Mathematical Modelling and Applied Soft Computing (MMASC 2012) (Towards high performance and knowledge optimization) Volume 2, pp1016-1023.

[9] Paul Ruggiero and Jon Foote, (2011) "Cyber Threats to Mobile", Produced for US-CERT, a government organization, Carnegie Mellon University-US.

[10] Tseng,D; Mudanyali, O;,Oztoprak.C;Isikman,S; Sencan,I;Yaglidere,O&Ozcan , A(2010), Lensfree Microscopy on a cell phone.Lab on a chip, vol .10, No.14,pp.1782-1792,ISSN 1473-0197.

[11] Racic, R., Ma, D, Chen, H. Exploiting MMS Vulnerabilities to Stealthily.(2011)*http://www.cs.ucdavis.edu/~hchen/paper/securecomm06.pdf*

[12] Mobile Device Security: Securing the Handheld, Securing the Enterprise. (2011)*http://www.good.com/media/pdf/enterprise/mobile_device_security_wp.pdf*

Authors

M.Sujithra is the Assistant Professor in the Department of Computer Technology and Applications of Coimbatore Institute of Technology, Coimbatore. She is having teaching experience of 9 years. She is pursing PhD in Avinashilingam University for women, Coimbatore. Her areas of interest include Mobile Device Security, Biometrics, Information and communication Security.

Dr.G.Padmavathi is the Professor and Head of computer science of Avinashilingam University for women, Coimbatore. She has 25 years of teaching experience and one year of industrial experience. Her areas of interest include Real Time Communication, Network Security and Cryptography. She has 140 publications in her research area. Presently she is guiding PhD's Scholars and M.Phil Researchers. She has been profiled in various Organizations her academic contributions. She has completed four projects funded by UGC and DRDO. She is life member of many preferred organizations of CSI, ISTE, WSEAS, AACE, and ACRS.