

Emerging Security Technologies for Mobile User Accesses

Nirav Jobanputra, Vijayendra Kulkarni, Dinkar Rao, and Jerry Gao, Ph.D.
San Jose State University, email: jerrygao@email.sjsu.edu

Abstract

Ubiquitous use of mobile phones has caused an emergence of applications targeted to mobile platforms. Since mobile devices become the major mobile platforms for users to transfer and exchange diverse mobile data over the wireless networks or wireless internet, mobile security for mobile accesses becomes very important and critical to assure secured mobile transactions, mobile data integrity and confidentiality. Mobile security also is critical to protect mobile users and mobile-based application systems from unauthorized accesses and diverse attacks. As an emerging technology survey paper, this paper discusses the security concepts, issues, and challenges in mobile accesses, summarizes and analyzes the state-of-the-art of security technologies for mobile accesses. Moreover, the paper discusses and compares the existing mobile security solutions and technologies.

Keywords: mobile, security, decryption, encryption, biometric.

1 Introduction

Mobile phones have become the breath and soul of technologies in today's fast emerging world. According to GSM Association Press Release in 2006, the mobile networks will cover 90% of the world's population by 2010. In 2006, Smartphone sales have risen from 7.40 million in 2003 to 69.2 million and are expected to reach 190 millions in 311 millions. Clearly, there has been a rapid growth in the cellular market, especially in recent years, and it is still projected to grow at the same rate or even better based on mobile market analysts. The major contributing factor for the brisk growth of the mobile phone market is the integration of a number of functionalities in the mobile devices. Today, mobile phones are used for much more than just for communications. They are provided with a rich service plan, to offers a wide spectrum of mobile functions and services, including personal data management, entertainment capabilities (such as digital games and music), mobile messaging, and location-based peer-to-peer applications, secure mobile payment and advertising services.

The strong demand of mobile applications and services raised increasing concerns on the security for mobile accesses, user privacy, and mobile applications. This leads an increasing demand on emerging mobile security technologies and solutions for mobile accesses. Hence, security becomes very important for mobile users and mobile accesses, and it is becoming a hot research topic in m-commerce applications and services. Although many mobile security solutions and technologies are proposed and developed in the recent years, there is lack of a comprehensive study and review about the existing mobile security issues and solutions.

This paper focuses on the mobile security topics and solutions relating to mobile accesses. It discusses mobile security concepts, problems, challenges and needs, and reviews the state-of-the-art mobile security emerging technologies and solutions. The paper focuses on its discussions on two emerging areas of mobile security: a) key-based

security solutions for mobile devices, and b) bio-information based security solutions. Moreover, the paper compares the existing solutions and technologies and discusses the future directions and future needs in mobile security.

As a tutorial review paper, this paper is structured as follows. The next section contains the categorization of the threats to a mobile phone. It discusses mobile security concepts, relating issues and challenges in mobile user accesses. Section 3 summarizes and compares the current emerging bio-information based security solutions for mobile devices. In addition, this section also discusses the related major players and their products. Section 4 reviews and compares the new key-based cryptographic security solutions for mobile accesses. Finally, Section 5 presents the conclusion remarks, future directions and needs for mobile security.

2 Understanding Basic Mobile Security Concepts, Threats, and Needs

What are the mobile security threats in mobile access?

Whenever discussing mobile security, we must understand mobile security threats to mobile phones and mobile accesses. Mobile phones have certain specific features (such as mobility) which make these devices more vulnerable to security attacks. Collin Richard Mulliner in [Mulliner 2006] listed the following features.

- **Mobility:** This is the most important characteristic of the mobile phones. Since mobile users can take them to anywhere, the chances of getting stolen, lost, or physically tempered increases as compared to stationary devices.
- **Strong Personalization:** As a personal device, mobile devices usually are not shared among multiple users.
- **Strong Connectivity:** Mobile phones are commonly used to connect to other devices over the wireless networks (or wireless Internet) for data exchanges.
- **Technology Convergence:** Today numerous functional features are integrated in the mobile phones, for example gaming, video and data sharing, and internet browsing.
- **Limited Resources and Reduced Capabilities:** Comparing with stationary devices, mobile devices have four major limitations: a) limited battery life, b) limited computing power, c) very small display screen size, and d) very small sized keys for inputs. These limits bring the challenges in building mobile security technology.

These features render mobile devices vulnerable to certain types of attacks. Table 2.1 summarizes these attacks, relating causes, and potential affects.

TABLE 2.1: Categorization of Attacks

Causes (Features)	Type of Attack	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
O.S. Weaknesses, Code Exploitation	Break-In Attacks	Prepare ground for other attacks

What are Mobile Security Requirements and Needs?

Although the fundamental concepts of security remain the same while considering mobile security relating mobile accesses, some new needs and requirements must be considered to cope with the above threats in mobile accesses. They are summarized as followings.

- **Mobile access confidentiality:** This makes sure that only the authorized persons are allowed to access to mobile data through mobile devices.
- **Mobile data integrity:** This makes sure that mobile data are consistent, correct and accessible.
- **Mobile service availability:** This requires the mobile resources on mobile devices only be accessed and used by the legitimate owners.
- **Disputed mobile service charging:** This refers to the case in which a mobile subscriber may be charged for mobile services and connection times because someone else caused the mobile device to access such mobile services without the user's knowledge.

These mobile security threats bring new requirements and needs for more effective mobile security solutions and technologies to ensure mobile access security on mobile devices so that the end-to-end protection between mobile devices can be assured.

What are the Implementation Challenges in Mobile Security?

Because of the limits of mobile devices, implementing mobile security solutions must address the following needs and challenges in building mobile security.

- ***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.
- ***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.

3 Bio-information Based Security for Mobile Devices

This section reviews bio-information based security solutions for mobile user accesses. It discusses the basic concepts and needs of biometric security, and presents the existing biometric technologies and solutions. Moreover, it compares different biometric solutions, discusses the major players, their products and applications. Furthermore, some future needs for biometric identification solutions are discussed.

3.1. Basics of Biometrics Security

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 behavioral 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. Physiological attributes of mobile users are related to the shape of their body.

These include their finger prints, face recognition and iris recognition. Their behavioral attributes include voice, key stroke patterns, and signatures. As shown in Figure 3.1, these attributes are the major targets for studying, analysis and measurement in Biometrics. The general process in Biometric identification is given in the Figure 3.2.

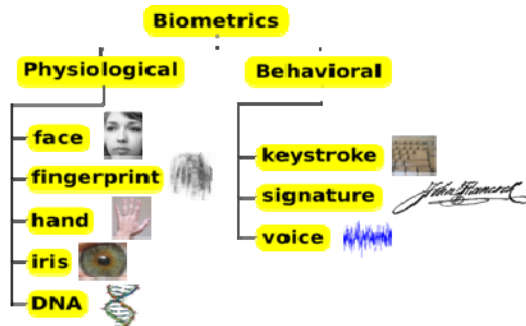


Figure 3.1 Classification of Biometric Characteristics

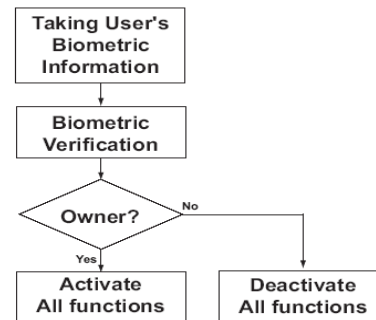


Figure 3.2 Biometric Identification Process [Ijiri 2006]

Comparing with the existing security solutions, biometric security approaches provide distinct advantages in personal identification and verification for mobile commerce and service applications. The rest of this section presents an overview of the current existing biometric technologies and solutions.

3.2. Existing Biometric Technology and Solutions

There are four types of biometric-based security technologies for mobile user identification. They are: a) fingerprint recognition, b) voice identification, c) face recognition, and d) iris recognition.



Figure 3.3: Fingerprint sensor on a PDA

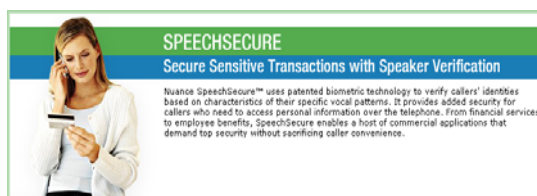


Figure 3.4: Voice identification on a mobile phone

(a) Fingerprint recognition:

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 them, 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 neighboring minutiae is used as methods for personal identification. A template is created out of minutiae points extracted from fingerprint. The mobile phone owner's template is created and stored in the mobile phone itself, in an encrypted form. The templates are, on an average, of 250 bytes. It usually ranges between 40 and 1000 bytes. During the process of fingerprint authentication, the mobile phone matches the features of a live fingerprint

against the template stored in phone. First, the live fingerprint is obtained and translated into a minutiae template. Next, this template is compared with the template stored in the phone. A match between these two templates leads to a successful authentication [Jensen 2006]. Figure 3.3 shows the fingerprint sensor mounted on a PDA.

(b) 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. For example, an identification card based security system is open for any one who has a valid ID card; it doesn't necessarily check whether the person holding the card is the right one or not. Similarly, a password based security system is not very secure if any other person knows the password. However, a voice based biometric security system positively identifies the individuals and separates one person from the other. It is capable to verify whether the person providing the voice inputs is the authorized person or not. It does so by comparing the voice input sample with a reference biometric, which is known as "reference voiceprint" [Markowitz 2000]. Figure 3.4 shows voice identification product offered by a major player.

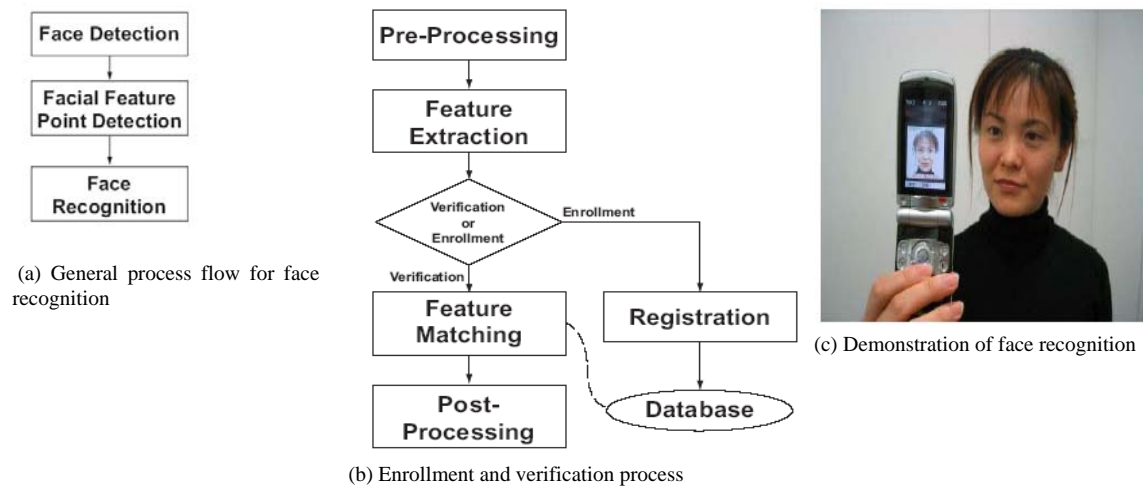


Figure 3.5 Face Recognition Work Flows and Demo [Ijiri 2006]

c) Face recognition:

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. In [Ijiri 2006], a face recognition system has been developed by a research team to process captured a facial image. The system is used for user face verification in two steps. Firstly, the system identifies the facial region based on the given image. And then, it detects the corner points of eyes and mouth. Figure 3.5(a) shows the system process flow, in which a user does not require to adjust a facial image exactly to a pre-defined fixed point. Instead, the user only needs to take the picture using a mobile device to ensure his or her facial image

is completely captured. The system workflow process for face enrollment and verification is given in Figure 3.5(b). Pre-processing and feature extraction are the common steps in Enrollment and verification process. It only takes about a second to complete. During enrollment, the extracted features are stored in the Database for registration. During verification, the extracted image is compared against the image stored in database [Ijiri 2006]. Figure 3.5(c) and Figure 3.6 show a demo of a user's facial registration by taking a picture using a mobile phone with built in digital camera and ARM9 processor.



Figure 3.6: Iris Recognition Technology Samples
<http://www.xvista.co.uk/html/our-solution/> and <http://www.oki.com/en/press/2006/z0623e.html>

d) **Iris Recognition:**

Iris recognition is another effective biometric security approach. The Iris is the colored part in the eye, located behind the cornea, surrounding the pupil. Iris recognition technology is built around the uniqueness of each iris. The irises are different even in identical twins. Irises capture characteristics like rings, fibers, pits, freckles and many others. The iris scanner can read information about these characteristics and store the data in 'IrisCode'. The current technology can differentiate between a still picture of the eye and the live eye while scanning. The pupil in the live eye makes small and continuous fluctuations; however, the pupil in the picture of an eye cannot. Hence, iris recognition is considered as the most reliable biometric element for securing mobile phones. During an enrollment process, multiple images of a user's iris are captured. With the user's approval, the 'IrisCode' image, which best represents the iris, is stored in an image database. During the verification process, the user's iris is scanned again and compared against the iriscode stored in the database. The iris recognition based security technology in [Sanderson 2000] provides an option of storing iriscode for both irises, so that during verification, the user is required to scan both eyes. A failure in matching both irises can trigger a security alarm or lockout the mobile phone. This is very useful in the areas where higher security restrictions are applied. Figure 3.6 shows the usage of Iris scanning technology.

TABLE 3.1 A Comparison Between Different Biometric Security Solutions [Applied Biometrics 2007]

Attributes VS. Different Security Solutions	Finger print based	Voice Identification	Face Identification	Iris Recognition
Types of Biometric	Image based	Voice based	Image based	Image based.
Required Hardware	Fingerprint sensor hardware	Any standard telephone	Digital camera	Digital camera
Affecting Factors	- Cleanliness and the pressure of the fingers. - Severe injury of fingers	- Ages and behavior like cold, and mood - Surrounding noise/sound	Lighting, weather, and coverage of the face.	Usage of reading glasses, sun glasses, and health issue with eyes can affect Iris recognition
Accuracy (Success Rate)	High or very high (up to 81%)	Medium (N/A)	Medium High (69%)	Very High (up to 96%)
Limitations	The quality of fingerprint images	Input voice quality and users' speech patterns	Facial image quality	Capturing the iris image may need some practice.
Ease of Use	High	High	Medium	Low
Cost	Low	Low	Low	High

3.3. Discussions

Table 3.1 provides a comparison between different biometric security techniques and solutions based on the number of factors. Table 3.2 provides the list of major players involved in creating biometric security for mobile device access.

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. 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>).

TABLE 3.2: Major Players in Biometric Security Technologies

Major Players	Biometric	Product name	Major Applications	When Introduced
Fujitsu	Fingerprint	MBF320 Fingerprint sensor	Provides security to PDAs, PCs, notebooks and tablet PCs.	August, 2006
HP	Fingerprint	iPAQ PDA	PDA equipped with fingerprint sensor. Provides secured accesses to emails, contacts, tasks, calendar and other related features.	September, 2005
Toshiba	Fingerprint	G500 and G900	Fingerprint scanner secures a phone against unwanted accesses. It also doubles up as a touch-sensitive scroll interface.	February, 2007
Hitachi & Authentec	Fingerprint	W51H mobile phone with AES1510 fingerprint sensor	Used to secure smart phone data and to authorize payments made by mobile phones with contact less near-field communication technology.	2005
Nuance Communications	Voice	SpeechSecure	Helps to fight against fraud and identifies theft for phone-based service applications.	March, 2004
Voice Security Systems	Voice	Voice Protect	Voice protect provides security that dramatically reduces fraud and can insure ones property from use, if stolen, or obtained fraudulently.	March, 2004
Vodafone	Face Recognition	904SH	Face recognition feature for enhanced security and privacy protection.	March, 2006
OMRON Corporation	Face Recognition	Face Recognition Sensor	The technology has been designed to protect personal and confidential information even for lost/stolen mobile phones.	February, 2005
xVista	Iris scanning	Iris recognition scanner	Iris recognition scanner to match 1 in 7 billion, and offers unbeatable protection against fraud.	June, 2006
Oki Electric industry	Iris scanning	Iris scanning middleware	Highly accurate user authentication (error rate: 1/100,000) for mobile devices by a regular embedded camera (with visible light).	July, 2007

To cope with the existing limits, next generation of security solutions are needed. For biometric identification, there are three future development directions.

- **Fusion of Biometric with different technologies:** One of future developments of biometric security solutions is to combine different technologies. For example, combining biometric security with RFID technology is one of the enhancements [20]. The fusion between the two technologies brings an extra security mean for mobile commerce applications, like mobile banking and payment systems.
- **Live Face identification:** Due to the limitation of existing biometric face identification technologies, it is possible for an illegitimate user to show the still picture of a legal mobile user during a face image capture process. A “liveness detection” solution, by 2-D Fourier spectra analysis based on the face images, has been provided to deal with this issue in [Li 2004]. This solution is capable to differentiate between a fake face and a live face using vein map of faces taken from a ultra-violet camera, although this mechanism is expensive. In this solution, after capturing multiple pictures of a mobile user’s face very rapidly, the system calculates the standard deviation of frequency from each image. If the face was faked using a picture, the standard deviation between each image will be negligible. But, with the live face, the standard deviation will be noticeable.

- ***Fusion of multiple biometric techniques:*** Integrating different biometric techniques is another future direction. For example, integrating public key infrastructure (PKI) with biometric security provides an integrated reliable security for mobile devices. A typical example is described in [Gao 2005], where voice identification is combined with PKI for a peer-to-peer payment solution. Combining fingerprint and iris scan on a single mobile device provides an integrated approach, which offers multi-level biometric security solutions to mobile users.

4. New Key-based Approaches to Mobile Access Security

This section discusses specific security issues on mobile, and reviews contemporary solutions and new research results. In addition, major players in mobile device cryptography are summarized. Furthermore, it compares the effectiveness of the newer solutions.

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, and d) very limited inputs. To deal with these, there are several approaches to using key-based security techniques.

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

A brute-force approach uses symmetric or/and 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. Authentication is performed using the A3 algorithm based on the private key stored in the SIM card, and a random number obtained from the provider network. Encryption and decryption are implemented using A5 and A8 based on the private key in a SIM card. 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 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. Some typical examples are explained below.

A) Cryptographically Protected Objects (CryPO)

A clever alternative approach to securing data exchanged among mobile systems is proposed in [Wilhelm 1997]. The system uses Cryptographically Protected Objects (CryPO) to control the security at the object-level. CryPO requires a Tamper-Proof Environment (TPE) on the mobile device, whose primary purpose is to store a private key, which is not known even for the mobile user. CryPO uses a 2-phase protocol that transfers objects to and from the mobile device in 2 phases - Initialization, and Usage.

In the Initialization phase, the device manufacturer publishes the public key of the device. The private key is never published, and is not known even to the owner of the device. The device manufacturer also sends the authentication certificate to the Object User. The mobile user may be anyone; not necessarily the owner of the device. In the Usage phase, the Object User sends a request to the Object Provider with the identification of the object that needs to be accessed and certificated. The Object Provider encrypts the object using the public key provided by the Object User.

The advantage with this approach is that the Object User cannot decrypt the object due to the lack the private key. He downloads the object into the mobile device. Only the mobile device with the private key can decrypt the object. The main problem with CryPO is that it is nearly impossible to create a Tamper-Proof Environment on any device. If the device is lost, any user can decrypt a downloaded object.

TABLE 4.1: Two Comparisons between RSA and ECC

(a) A Key-Size Comparison between ECC and RSA

(b) An Energy Consumption comparison between RSA and ECC

ECC Key Size	RSA Key Size	Ratio (ECC / RSA)	Time to Break ECC key (MIPS years)	Signature Energy Cost (million Joules)		Key Exchange Energy Cost (million Joules)		
				Sign	Verify	Client	Server	
163	1024	1:6	$\sim 10^4$					
256	3072	1:12	$\sim 10^8$	RSA (1024)	304.00	11.90	15.40	304.00
384	7680	1:20	$\sim 10^{11}$	ECDSA (160)	22.82	45.09	22.30	22.30
512	15360	1:30	$\sim 10^{78}$	RSA (348)	2302.70	53.70	57.20	2302.70

B) Elliptical Curve Cryptography (ECC)

ECC is a typical result of improving the existing cryptographic algorithms for mobile device and access security. As an alternative to RSA, Elliptical Key Cryptography [DeviceForge.com 2004] is an implementation of asymmetric key cryptography, and is well suited for securing mobile devices. ECC is an improvement over Discrete Logarithm cryptography. According to Table 4.1 (a) in [Mohammed 2001], for the same level of security, RSA requires considerably more bits for the key than ECC. With smaller keys, mobile device processors can perform arithmetic operations much faster, and consume less battery energy. In a battery consumption studies in [Wander 2005], the authors compare the two competing public key mechanisms (RSA and ECC) in 2 different key lengths that provide the same security.

As shown in Table 4.1 (b) [Wander 2005], the ECC algorithm is 13 times more efficient for signing while comparing RSA (1024) with ECDSA (160). In addition, ECDSA has much less energy costs than RSA on the server side for key exchanges. Figure 4.2

provides a comparison of processing times between different RSA and ECC algorithms in signature generation, encryption, and decryption times. 2048 bits are used for Raw RSA, RSA with OAEP, and RSA with PKCS1. 256 bits are used for ECC based ECIES. Clearly, ECC based ECIES is very efficient for key generation, and the disadvantage of its long encryption/decryption times is offset by its comprehensive functionality.

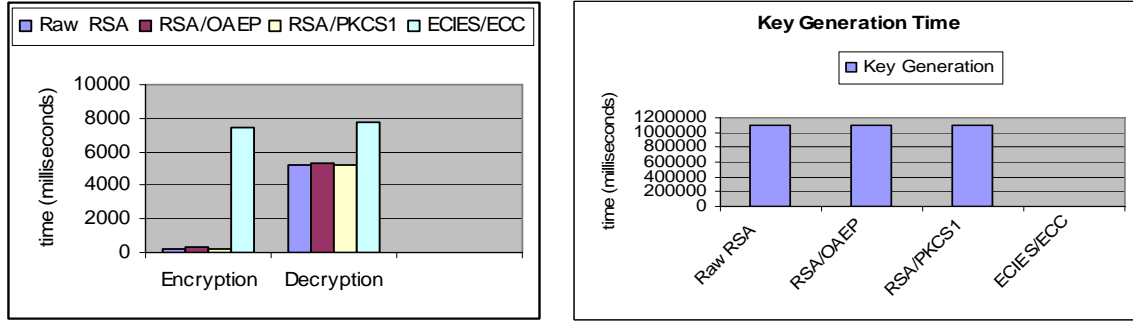


Fig. 4.2: A Comparison of Processing Times between RSA and ECC

TABLE 4.3: Plain RSA Signature Timings (milliseconds)

Processor Speed(MHz)	Key Length (bits)			
	1024	2048	4096	8192
PI-233	40.3	252.7	1741.7	12490.0
PIII-500	14.6	85.6	562.8	3873.3
PIII-700	9.2	55.7	377.8	2617.5
PIII-933	7.3	43.9	294.7	2052.0
PIV-1.2GHz	9.3	58.7	401.2	2835.0

TABLE 4.4: SAS Signature Timings (milliseconds)

Processor Speed (MHz)	Key Length (bits)			
	1024	2048	4096	8192
PI-233	13.3	52.4	322.5	2143.4
PIII-500	9.1	46.3	302.0	2070.2
PIII-700	8.5	45.1	299.0	2059.6
PIV-1.2GHz	8.5	45.4	299.0	2061.0

(C) Server-Aided Signatures (SAS)

Since computing public key signatures is a CPU intensive operation, the server-aided signatures is to an effective approach to offloading intensive security computations to a trusted server side [Ding 2007]. In this approach, the public signature is split into two parts, with one part computed on the server and the other part computed on mobile devices. Each part, by itself, is useless. Only the recombination of the two parts makes a secured signature that allows for certification and non-repudiation. The authors in [Ding 2007] show that using a partially trusted server is more secure than using a fully trusted server, because a fully trusted server implies a single-point of failure. A single fully secure server would likely hold private information about all users, thus compromising them all in case of a hack. Another related solution to offload intensive processing is called Offline/Online cryptography, or SignCryption [Zhang 2005].

The authors in [Ding 2007] have compared the performance of SAS signature timings with the performance of plain RSA signatures. Based on their comparison results in Table 4.3 and Table 4.4, SAS signature generation is faster than plain RSA generation. The slower the processor is, the bigger is the difference between the two signature generation time. For example, for 1024 bits on a 233 MHz processor, RSA takes 40.3 ms (Table 4.3), but SAS takes only 13.3 ms (Table 4.4). On the other hand, for faster processors, the difference is not so significant. This suggests that SAS is not very efficient for high-end devices. However, in a network made up of heterogeneous devices,

using SAS is still worthwhile because it requires less computing power on mobile devices.

Major Players:

Some discussed mobile access security solutions have been commercialized. Table 4.5 lists the major players in mobile security devices. Navastream has specialized phones with strong cryptographic solutions over GSM networks. The supported algorithms are AES, TwoFish, and Diffie-Hellman. Checkpoint Software has a mobile security product (PointSec Mobile) for PDAs and Smart phones. It supports real-time encryption for data stored on mobile devices. PointSec managed devices can exchange data among themselves securely, via Bluetooth or IrDA. Microsoft has a product (Enhanced Cryptographic Provider) implements the CryptoAPI interface to support both symmetric key and asymmetric key cryptographic algorithms. CryptoCell by Discretex, as an embedded security device, supports the RSA, ECC and DH asymmetric public key algorithms, and the AES, DES/Triple-DES, RC4 symmetric key algorithms. Until now, there is no commercialized Offline/Online Cryptography or Server-Aided Cryptography technology.

TABLE 4.5: A List of Major Players

Major Players	Product	Algorithms supported
Navastream (www.navastream.com)	CryptoPhone 200 CryptoPhone G10	AES, TwoFish, Diffie-Helman
Checkpoint Software (www.checkpoint.com)	PointSec Mobile	AES, DES, 3DES, RSA, Diffie-Hellman
Microsoft Corporation	Enhanced Cryptographic Provider	AES, DES, RSA
Discretex (www.discretex.com)	CryptoCell	RSA, ECC, Diffie-Hellman, AES, DES, 3DES, RC4

4. Conclusions

The paper discusses the importance and the concepts of mobile security for mobile accesses, and covers the existing mobile security solutions and technologies for mobile phones. In particularly, the paper reviews and compares the existing key-based security solutions. Furthermore, the paper also presents, compares, and analyzes the bio-information based security solutions for mobile phones. Here are two major conclusion remarks based on this survey.

- Bio-information based security solutions provide a big hope to cope with the current mobile security issues. The fingerprint and voice recognition biometrics are low-cost and easy-to-use solutions on the mobile device, but they are not always accurate. On the contrary, Iris scanning provides highly accurate results, but it is a high cost solution. For mobile applications with higher security requirements, it may be a good idea to use multiple biometric-based security technology for future mobile devices to achieve mobile security at different levels.
- Innovative key-based cryptography algorithms also can bring effective mobile security solutions to cope with the current limitations of mobile devices. For example, to achieve the same level of security, the ECC algorithms use fewer bits than RSA. Hence, ECC solutions require fewer bits and use less power of mobile devices. A comparison of new ECC cryptography techniques shows that two-key cryptography should be used judiciously, because they do consume more resources than single-key cryptography. Specialized hardware is an option but it is not better than using improved algorithms.

In spite of the limited resources of mobile phones, some security solutions have been developed recently. More cost-effective mobile security solutions are still needed to assure to security of mobile accesses and user privacy.

6. References

- [Applied Biometrics 2007] Applied Biometric, “Biometric Comparison Table”, Retrieved on September 11, 2007 at <http://www.appliedbiometrics.co.uk/biometrics/>.
- [Dedo 2004] Douglas Dedo, “Windows Mobile-Based Devices and Security: Protecting Sensitive Business Information”, Microsoft Corporation April 2004.
- [DeviceForge.com 2004] DeviceForge.com, “An Introduction to Elliptical Curve Cryptography”, July 20, 2004. Retrieved at <http://www.deviceforge.com/articles/>.
- [Ding 2007] X. Ding, D Mazzochi, and G Tsudik, “Equipping Smart Devices with Public Key Signatures”, ACM Transactions on Internet Technology (TOIT), 2007.
- [Gao 2005] Jerry Gao, Jacky Cai, Kiran Patel and Simon Shim, “A wireless payment system”, Proceedings of 2nd International Conference on Embedded Software and Systems, 2005.
- [Grecas 2003] Constantinos F. Grecas, Sotirios I. Maniatis and Iakovos S. Venieris, “Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration”, Mobile Networks and Applications, Volume 8, 2003.
- [Ijiri 2006] Yoshihisa Ijiri, Miharuru Sakuragi and Shihong Lao Sensing, “Security Management for Mobile Devices by Face Recognition”, Proceedings of the 7th International Conference on Mobile Data Management, IEEE Computer Society, 2006.
- [Jansen 2006] Wayne Jansen, Ronan Daniellou, and Nicolas Cilleros, “Fingerprint Identification and Mobile Handheld Devices: An Overview and Implementation”, National Institute of Standards and Technology. March 2006.
- [Li 2004] Jiangwei Li, Yunhong Wang, Tieniu Tan, A.K.Jain2., “Live Face Detection Based on the Analysis of Fourier Spectra”, Proceedings of SPIE, 2004.
- [Markowitz 2000] Judith A. Markowitz. “Voice Biometrics”, Communications of the ACM Vol. 43, Issue 9, Pages: 66 – 73, September 2000.
- [Mulliner 2006] C.R. Mulliner, “Security of smart phones”, Master’s thesis submitted to University of California, Santa Barbara, June, 2006.
- [Mohammed 2001] E Mohammed, A E Emarah, and K El-Shennawy, “Elliptic Curve Cryptosystems on Smart Cards”, Proceedings of IEEE International Carnahan Conference on Security Technology, 2001.
- [Perakslis 2005] C. Perakslis and R. Wolk, “Social acceptance of RFID as a biometric security method.” IEEE Volume, Issue, 8-10, June 2005 Page(s): 79 – 87.
- [Sanderson 2000] S.Sanderson and J.H.Erbetta, “Authentication for Secure Environments Based on Iris Scanning Technology”, IEEE Colloquium on 2 March 2000.
- [Wander 2005] A. S. Wander, N Gura, H Eberle, V Gupta, and S C Shantz, “Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks”, Proceedings of 3rd IEEE International Conference on Pervasive Computing and Communications, 2005.
- [Wilhelm 1997] Uwe G. Wilhelm, “Increasing Privacy in Mobile Communication Systems using Cryptographically Protected Objects”, Verlässliche IT-Systeme, 1997.
- [Zhang 2005] Fangguo Zhang, Yi Mu, and Willy Susilo, "Reducing Security Overhead for Mobile Networks," The proceedings of 19th International Conference on Advanced Information Networking and Applications (AINA'05), Vol.1, 2005.