RESEARCH ARTICLE OPEN ACCESS

A New Framework for Secure M-Commerce

Ali Mirarab and Abdol-Reza Rasouli Kenari
Electrical and Computer Department, Qom University of Technology, Qom, Iran

Abstract
By combining the wireless network and E-commerce, suppliers can provide a more convenient and quicker service on a human scale for their customers. The main advantages of such services are their high availability, independence of physical location and time. Mobile commerce raises a number of security and privacy challenges. However, security has always been the key issue for the development of mobile E-commerce, which is more vulnerable than the traditional E-commerce mode. . In order to solve the problem of security gap in the transmission of mobile E-commerce information, a framework based on J2ME/MIDP is proposed, which combines double layer encryption schemes, stego-image and secure XML messages which transferred between the mobile terminal and the server. Our method provide strong secure and invisible communication with high security and high operating efficiency that compatible with many types of mobile terminal.
Keywords: *M-Commerce Security, ECC, J2ME/MIDP, J2EE, Random LSB Steganography, XML, Double Layer Encryption.*

I. Introduction

With the development of mobile technology and the extensive use of intellectual mobile terminal, the mobile E-commerce has become a brand new method for the business activity for both individuals and enterprises. By combining the wireless network and E-commerce, suppliers can provide a more convenient and quicker service on a human scale for their customers [3]. Mobile commerce (m-commerce) is providing commercial services that are accessible by using mobile devices, typically a mobile terminal. The main advantages of such services are their high availability, independence of physical location and time [6].

Mobile commerce raises a number of security and privacy challenges. However, security has always been the key issue for the development of mobile E-commerce, which is more vulnerable than the traditional E-commerce mode. The broadcast nature of the wireless communication and increased popularity of wireless devices introduce serious security vulnerabilities. Mobile users and providers must be assured of the correct identity of the communicating party; user and signaling data must be protected with confidentiality and integrity mechanisms.

Despite the fact that operators are announcing or rolling out Wireless Applications Protocols (WAP), I-mode and java-based information, the platforms have gaping security holes. In order to solve the problem of security gap in the transmission of mobile E-commerce information, a framework based on J2ME/MIDP is proposed, which combines double layer encryption schemes, stego-image and secure XML messages which transferred between the mobile terminal and the server.

II. Related Work

In this section, we present counter measure solutions that have been proposed to securing M-Commerce.

Pan Tiejun et al. [1] proposed a secure solution which is based on WPKI with Bluetooth earphone. Authors present a solution in which the mobile commerce security is enhanced by using Wireless Public Key Infrastructure (WPKI). An WIM (WAP Identity Module or Wireless Identification Module) Bluetooth earphone with ESAM (Embedded Secure Access Module) is connected to the Smartphone by Bluetooth interface for ensuring the end to end security ability between user and mobile commerce service providers and storing private data, give the architecture of mobile commerce security system based on WPKI with Bluetooth earphone, design the function of each roles in the system.

Pan Tiejun et al. [2] present an approach in which the mobile security is enhanced by an isolated external electronic security key (eKey) with a security enhancement mechanism. They propose an advanced mobile security solution and related security methodology based on distribute key without changing hardware configuration of the mobile devices. The solution consists of the UE (User Equipment), an electronic security key (eKey) which is connected to the mobile device by adaptable interface for enhancing the UE security ability and storing private data, CA with digital certification and web server which provides the M-commerce services.

UE communicates with web server and CA via wireless mobile net and Internet. UE communicates with eKey via adapted interface (e.g., COMM, USB and Bluetooth). Authors believes M-commerce security is enhanced by using external security key and specified policies including user confidentiality, mutual authentication, data integrity and confidentiality. Furthermore, the design of eKey is given which put emphasis on the hardware security solution and the communication mechanism between main controller and security module. In this way, the M-commerce security problem is solved to a certain extent.

Feng TIAN et al. [3] proposed a double layer encryption schemes based on WAP, in order to solve the problem of security gap in the transmission of mobile E-commerce information through WAP gateway, which combines with WAP security architecture and mobile E-commerce security architecture. The data is encrypted with the public key of application server on the mobile terminal firstly, and then the encrypted data is encrypted again with WTLS in the wireless network and TLS/SSL in wired networks, which realizes the double layer encryption transmission. The digital signature and verification based on elliptic curve cryptography are adopted in this system, which can fast verify the identity of both parties.

Suzhen Wang et al. [4] proposed the solution of security vulnerability in mobile E-commerce based on the "double encryption model". In this model, each symmetric encryption algorithm, public key encryption algorithm and message digest algorithm owned by mobile terminals and content servers has a priority, the most widely used algorithm has the highest priority; the second widely used algorithm has a second priority, and so on. This solution can reduce the communication cost of the encryption consultations between mobile terminals and servers, shorten the time internal of consultations, and increase the connection speed and security degree in mobile E-commerce transaction. This solution has built a secure channel between mobile terminal and content server because the data is protected in the whole process of transmitting, so the solution has solved the weak point that the WAP gateway be able to see clearly of the message.

Pratiksha Y. Pawar et al. [5] presented security of these systems using Random LSB steganography and cryptography method. The proposed method is more safe and secure instead of using either steganography or cryptographic method. They shows secure and invisible communication in M-banking as well as e-banking. In this paper instead of direct sending information, it is encrypted first using encryption algorithm and then this encrypted information is processed to hide into an image using a password so that stego-image contains hidden message which is not in plaintext form. Another important point is that encrypted information is hidden into an image using "Random LSB Steganography" that is embedding data in non-sequential LSB insertion pattern so that it is unintelligible and difficult to detect. The stego-image is put on a web site then the URL of the web site is sent to the user. After receiving the URL, the user downloads the picture by a special program. The user can extract information from the picture only if the password entered is correct. This information will be in encrypted form user will decrypt it using the decryption algorithm so that user will get required information. The proposed scheme has been implemented using J2EE language for e-banking and J2ME language for m-banking. The method implementation supports all java enabled mobiles for m-banking application.

Dalia nabil Kmal et al. [6] aims to present some suggestions to improve m-commerce security and limit the m-commerce drawbacks. These suggestions related to the following functional: End-to-End Transport Layer Security by Java 2 micro edition/ mobile information device profile (J2ME/MIDP). Using J2ME/MIDP to mobile communication overcome the security challenges faced with WAP technology, but securing the XML messages transferred between the mobile terminal and the server would give high level of integrity for the data itself not for the physical connection.

III. Proposed Framework

In our method instead of direct sending information in plaintext form. We are encrypting this information using "ECC" algorithm and then encrypted information is hidden into the picture by using password and "Random LSB Steganography algorithm". This stego-image is placed in another website and address of that website is sent to user. User downloads the picture from website. User extracts information from picture by using password then user gets information in encrypted form.

J2ME provides several levels of security, such as class loader, byte code verifier, and security manager. These security levels protect client systems from unreliable programs. The security advantages of J2ME over WAP are end-to-end security, less use of network and content-based encryption.

End-to-end security: J2ME supports end-to-end encryption, authentication, and verification. In WAP, a request from a wireless device is encrypted in WTLS and this request needs to be decrypted as Transport Layer Security (TLS) data. While this conversion takes place, the data is unencrypted making it highly vulnerable. J2ME does not need a gateway between the device and the server. This allows J2ME to provide end-to-end security. There is no conversion of data from WTLS to TLS, thereby eliminating the chance of the data being unencrypted at any point of time.

Less use of network: J2ME allows data to be processed locally, unlike WAP that needs to connect to the network for any kind of data processing. This feature in J2ME in turn reduces the possibility of data loss or theft.
Content-based encryption: J2ME applications process data before sending it across a network. A J2ME application can set the security policy based on the content.
The proposed suggestion aim to secure XML messaging between a J2ME/MIDP wireless front end and a JSP page back end. XML digital signature technology can help to implement lightweight and flexible security solutions for wireless Web services applications. XML is becoming a major data exchange protocol in the world of Web services. XML messages that drive Web services often need to go through multiple intermediaries before they reach destinations. So, it is important that we secure the communication content from end to end. The best way to do it is to ship an XML document and its security information (such as signatures, digests, keys, and so on.) altogether as a single document. Handling the XML digital signature in MIDP applications IBM alpha Works develops a Java package called XML Security Suite, which supports the latest XML digital signature specification. As known, to handle XML digital signatures, the wireless devices being used need to support the following functions: Read and write data from/to an XML document and Sign the message and verify the signature. These functions require a cryptography API that is not part of the current MIDP specification. The bouncy castle crypto APIs is an open source, lightweight cryptography package for the Java platform. It supports a large number of cryptography algorithms and provides an implementation for JCE. Because Bouncy Castle is designed to be lightweight, it can run from J2SE to J2ME (including MIDP) platforms. It is the only complete cryptography package that runs on MIDP. Together XML digital signature specification and the usage of several different Bouncy Castle key generators, encoding engines, digital signature singers, and a digest engine.

3.1 Encryption Algorithm

This mobile E-commerce security system adopts a double layer encryption schemes in its data transmission and provides a safe transmission for its data. We use Elliptic Curve Cryptography in order to encrypt data. The security transmission process is as shown in figure 3:
1) The terminal encrypts XML message M0 to get M1 with the public key PA of application server, then encrypts M1 with the key Ke1, and gets M2.
2) The message M2 decrypts with Ke1 and gets the encrypted file M1.
3) The message M1 encrypts by Ke2 and gets M3
4) Then this encrypted information is processed to hide into an image using a password so that stego-image contains hidden message which is not in plaintext form (explained in next section) and then sends it to the application server.
5) The application server will decrypts M3 with Ke2 and get M1, then decrypts M1 with its own private key dA and gets the cleartext M0.

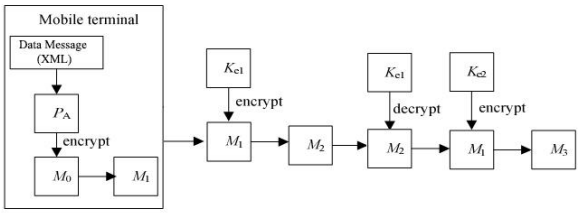

Fig. 1 Encryption Algorithm Process.

3.2 LSB Steganography

Image compression techniques are extensively used in steganography. Among the two types of image compressions, lossy compression and lossless compression, lossless formats offer more promises. Typical examples of lossless compression formats are CompuServe's GIF (Graphics Interchange Format) and Microsoft's BMP (Bitmap) [13]. In this work, for e-banking we are using BMP format and for m-banking we are using GIF format.
When images are used as carrier in Steganography they are generally manipulated by changing one or more of the bits of the byte or bytes that make up the pixels of an image. The message is stored in the LSB of one color of the RGB value. A BMP is capable of hiding quite a large message.
The amount of information that can be hidden in GIF images is less as compared with BMP Images. Embedding information in GIF images using LSB technique results in almost same as those of embedding in BMP.

This method hides information in the least significant bits of pixels. In this method each byte of information is hidden in two pixels. For hiding information a byte is divided into an eight bits. By using password two pixels are selected in which a byte of information is hidden. An algorithm in [1] is used to select pixels to hide data.
In this algorithm image is segmented into n block of m pixels. A block is selected according to password and the information is hidden in an empty pixel of this block. The algorithm for selecting a block and an empty pixel in that block as follows:
If the selected block starts with the pixel number x and has m pixels then the number of last pixel is x+m-1. This algorithm uses an array of size m+1 for remembering empty pixels of current block. This array contains the number of pixels having no data. The last cell of the array is the total empty pixels in the current block. According to the password, an empty pixel is selected and the last empty pixel number is copied to this array cell. After this operation the total number of empty pixels on the block decreases by one. This method is also used for selecting a block to hide the information in itself. After selecting the pixels we hide a byte within them. Each pixel has three colors (RGB), and the information is stored in the LSB of these colors.

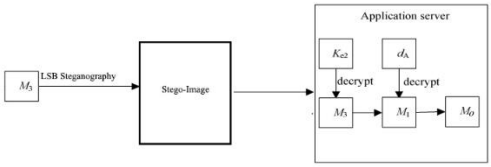

Fig. 2 LSB Steganography process.

IV. Experimental Work

The application we designed and implemented provides a prototype solution for securing sensitive data. This section presents a brief discussion of the design starting with the client environment and moving on to the server environment. In this paper we are describing implementation of M-Commerce service.

A. The Client Environment

On the client side we used the J2ME wireless toolkit 1.0.4 [6] provided by Sun. The wireless toolkit is a set of tools that provide J2ME developers with the emulation environments, documentation, and examples to develop MIDP-compliant applications. Developers are thus able to check the valid operation of their applications before deploying them on actual physical devices. The MIDP application is packaged inside a Java archive (JAR) file, which contains the application class and resource files. This JAR file is actually downloaded to the physical device (mobile terminal) along with the Java application descriptor file. In the client environment user sends request, receives

B. The Server Environment

To benefit from a pure Java solution, we implemented the server-side application in accordance with the J2EE specifications [5]. Servlet classes are packaged in a web archive (WAR) file and deployed on the J2EE application server. We used the J2EE reference implementation server version 1.3.1 provided by Sun. The database server we used is the Oracle 11g.

The Java Servlets communicate with the database using the well-known Java database connectivity (JDBC) API and the new javax.sql package. Some of the services addressed by the javax.sql package are connection pooling, distributed transactions and data source retrieval using logical names. Instead of loading the specific JDBC driver each time we want to connect to the database, we used the Java naming and directory interface (JNDI) to retrieve the data source using its logical name from a JNDI-complaint directory service on the J2EE server.

In the server environment there is authentication Servlet to authenticate client, service Servlet which provides services requested by client like account balance, transaction, ministatement, cheque etc. This environment also contains encryption program and LSB encoding program.

V. Conclusions

An ideal solution of mobile commerce security vulnerabilities is to develop the end to end security model, which protects each weak link in mobile e-commerce transaction process to ensure the data from the transfer point to the final destination is entirely safe. Always there is no perfect secure system, especially in m-commerce since the mobile communication system and all its applications still in the childhood level. But also the mobile wireless hackers and crackers still in the same level. Using J2ME/MIDP to mobile communication overcome the security challenges faced with WAP technology, since there is no decryption and encryption performed in the WAP proxy server.

Our framework has the following advantages:
1. This method is compatible with many types of mobile terminal.
2. In this method before steganography in the picture, encrypted information is encoded by double layer encryption therefore if person manages to extract information from the picture he will not be able to decode it without having the key.
3. In this method the information is never placed on the internet. Thus, the possibility of disclosure of information is very low.
4. In this method use of combination of steganography and cryptography provides strong secure and invisible communication.
5. High security: The adoption of double layer encryption schemes, on one hand, solves the security problem thoroughly exposed in the WAP gateway data information decrypting and the encrypting process; on the other hand, the ECC public key system is obviously superior to RAS&DSA. The decryption time for ECC and RSA&DSA's comparison is as shown in figure3.

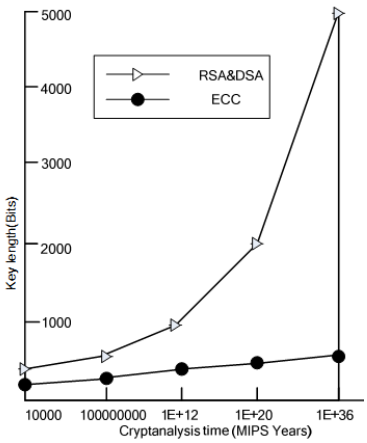

Fig. 3 Decryption time comparison of ECC and RSA&DSA.

6. Easier implement for the system: This plan does not need to add any devices in mobile terminal, application server or system reconfiguration.
7. High operating efficiency: ECC is much faster than RSA and DSA for its application of elliptic curve crypto under the same resources, especially fit for the low calculating mobile terminal. In document [8], the encryption and decryption performance comparison on 8 bits' smart card about RSA and ECC is as shown in table 1.

Table 1: Performance comparison of RSA and ECC

Time	CPU: Atmega 128.8MHZ	
	RSA1024	ECC168
Encryption Speed (ms)	10000	0.39
Decryption speed (ms)	400	8.15

8. Small storing space: The storing size for ECC's key and system parameter is much smaller than RSA and DSA. 160 bits' ECC has the same security extension with 1024 bits' RSA and DSA, and 210 bits' ECC the same with 2048 bits' RSA and DSA, which is specially designed for relatively small storing devices.

References

[1] P. Tiejun, Zh. Leina, "New Mobile Commerce Security Solution Based on WPKI," 2012 International Conference on Communication Systems and Network Technologies, Rajkot, pp. 485-488, May 2012.
[2] P. Tiejun, Zh. Leina, F. Chengbin, H. Wenji, F. Leilei, "M-commerce Security Solution Based on the 3rd Generation Mobile Communication," 2008 International Symposium on Computer Science and Computational Technology, Shanghai, pp. 364-367, Dec. 2008.
[3] F. Tian, H. Xiao-bing, Y. Wei, " Study of WAP Mobile E-commerce Security on WPKI," 2009 Second International Symposium on Electronic Commerce and Security, Nanchang, pp. 3-6, May 2009.

[4] S. Wang, L. Fan, "A solution of mobile E-commerce security problems," 2010 2nd International Conference on Education Technology and Computer (ICETC), Shanghai, pp. 188-192, June 2010.
[5] Pawar, Pratiksha Y., S. H. Gawande, and D. G. Deotale. "M-Commerce Security Using Random LSB Steganography and Cryptography", International Journal of Machine Learning and Computing, Vol. 2, No. 4, August 2012, pp. 427-430.
[6] Dalia nabil Kmal. "Build A Framework to Optimize M-Commerce Security", Tikrit Journal of Pure Science, Vol. 15, Issue. 2, 2010, pp. 123-127.

Ali Mirarab received the M.C.S. degrees of Information Technology. He passed BA has in Tehran University in field of IT engineering. His research interests are in various aspects of IT fields especially security and cloud computing**.**

AbdolReza Rasouli Kenari received the Ph.D. from UTM in 2011 and M.C.S. degrees from the Islamic Azad University in 2006 in Computer Engineering. He is currently Head of Graduate Studies at Qom University of technology. His research interests are in various aspects of data mining and security.