ISSN No. 0976-5697

Volume 6, No. 8, Nov-Dec 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Mobisecure using DSA

Ms.Pranoti Panchal
Department of Computer Engineering
G. H. Raisoni college of Engineering and Management
Pune, Maharashtra, India

Abstract: There are many benefits of mobile devices one among them is it is available to everyone, wherever and whenever we want. Use of these devices is still new and methodology for security in the data transfer between them does not still give confidence and trust to users. Hence without an efficient security mechanism, a mischievous user is able to fetch information from other users by intervening the communication and using them as they want, which can be fraud or can cause damage and inconvenience to the possessor of the information. There are other ways to send information like e-mail broadcast, e-commerce or some financial transactions. Hence it is required that both sender and receiver of the information should sign the document and convert the transaction a digital one, allowing greater reliability to the transaction. This paper identifies the mechanisms that can be used as digital signatures and certification to obtain the electronic security system in Mobile River devices and proposes a platform for the implementation of the digital signature in mobile devices to protect from different MIMs

Keywords: DSA, SHA1, PRNG, Digital Signature, QR code.

I. INTRODUCTION

Invention of computers and computer networks was done in 70's, they were very expensive at first and their operation was very difficult to understand. As this technology was getting used by research agencies like Universities and Military Institutes there was a great concern for data protection and security. This got changed in 80s with two advancements in engineering. The first advancement was the invention and development of microprocessors with greater processing ability with lower price, and the second advancement was LANs involving supply of computers in local networks with high speed. With these advancements it became necessary to create some rules for this technology use to ensure its safety as the technology and networks used by researchers began to be used by business people as well for business transactions, banking transactions, building purchases and many more. Later revolution started with the advent of mobile devices and the Internet. Mobility of devices became more popular when mobile telephones got launched. This invention roused much more interest among crowd in few years its usage spread worldwide. Due to this society got transformed and the number of mobile telephone subscribers improved internationally.

With all this advent there comes methodology for security in the information transfer between entities which is not giving assurance and faith to users. Hence there is a requirement of a security tool or mechanism through which mobile devices can communicate.

II. CRYPTOGRAPHY

Digital signature is created by encrypting a message or its representation. In encryption of message secret key is used belonging to participants involved in communication. For improving efficiency, message digest is preferred than message for encryption.

The steps of the digital signature mechanism are as follows:

1) The sender of the message calculates message digest and then encryption is done on digest using the sender's private key. Hence digital signature is made. [1]
2) The sender sends the digital signature along with the message to receiver.
3) The recipient receives the data, decodes the digital signature using the sender's public key, and generates the sender's message digest one more time.
4) The receiver calculates a message digest from the message data received and verifies that the message digest received and message digest created are the same. [1]

If the digital signature gets verified, the receiver of the message identifies that the message received had not been changed throughout communication and also identifies that the message is sent by body that claims to have sent it. A digital signature provides integrity of the message and also authentication. A digital signature also provides evidence of source and if the transmitter of the message knows the secret key, it provides significant proof that the sender is the initiator of the message.

III. ALGORITHMS USED IN DSA

Digital signature procedure comprises of three algorithms:

1) A key generation algorithm which chooses a private key at random from a set of possible private keys. The algorithm produces private key and a equivalent public key.
2) A signing algorithm that, which generates a signature

if message and private key is given.

3) A signature verifying algorithm that either accepts or rejects a message when message, public key and a signature is given to it.

A. Key Generation Algorithm

Key generation in DSA involves two phases. First phase involves selection of parameters of algorithm. These parameters can be shared with various users of the implemented system. Second phase involves computation of private and public keys which are used in cryptography. Encryption of message or data and decryption of the same is done while in communication using public key and private keys generated here.

For parameter generation SHA1 (Secure Hash Algorithm) is used. In SHA1 whole message is converted into small sets of data which is also referred as message digests. After creating message digests PRNG (Pseudo Random number Generator) is used to generate random numbers from the same digests.

B. Security and attacks of network

In old days highly skilled software engineers use to hack details of communications as only they were technically sound to do that. But nowadays it has become very easy to become hacker and steal information from data communication by using many tools available on internet. These attacking tools and open networks communications have raised an amplified need for network shield and dynamic safety policies.

The most effective way to protect a network from an outsider outbreak is to close the network entirely from the outdoor world. Using a closed network can provide connectivity only for trustworthy parties and websites and it will not definitely allow a link to outsider public networks and by doing this it will limit the dealings among them.

There are several types of attack in a network as listed below:

Eavesdropping: Normally the majority of communication done in network is not in encrypted format or clear text format, which allows invaders or hackers to invade in communication, gain access for data in open network and interpret the traffic. When the attacker or invader is checking communication in LAN without getting anyone to know about it, it can be called as sniffing or snooping.

Data Modification: When an invader checks your data, the next step is to change it. When an attacker changes the information from the read communication Sender or recipient may know get to know about it. Sometimes there is no requirement of data confidentiality in communication but no one wants to get data changed while in communication [5]. For example while exchanging data for sales you do not want the details like price, quantity or billing information to be altered.

Identity Spoofing (IP Address Spoofing): In most of the networks operating systems uses the IP address of a system to identify a valid communicating entity. In some cases it is likely for an IP address to be incorrectly assumed which is nothing but identity spoofing. An invader or attacker might also use additional programs to create IP packets that looks like to originate from lawful addresses inside the network.

Once the access is received for the network with a valid IP address the attacker or invader will be able to update, recreate, or edit the information. The attacker can also try for some other types of attempts of Password-Based Attacks. This clearly indicates that access for network is totally dependent on user name and password. If intruder is able to gain access for network and resources it is very easy to hack login credentials and transmit the data on behalf of trustworthy entity.

Denial-of-Service Attack: In this attack use of computer or network is prevented by valid users.

Man-in-the-Middle Attack: When two entities are communicating and some third entity is able to actively monitor, catch or master your communication in transparent way then it is nothing but Man-in-the-middle attack.

Sniffer Attack: An attack done in communication using an application or device which is able to scan, monitor, and capture network data communications and read packets involved in network.

C. Barcodes

Barcodes are figures that can be read using camera based devices and laser can be scanned using electronic medium. Barcodes are used to encode the information like as product numbers, serial numbers and also batch numbers. Barcodes helps in automatically identifying and tracking products in shopping malls and also in supply chains.

Two-dimensional (2D) barcodes: These are Compact, high-capacity 2D symbolic structures. These represents all GS1 keys and attributes.

QR(Quick response code) Codes is a type of 2D barcode The QR Code system is fast, readable and have great storage capacity when compared with UPC barcodes. This additional benefit makes it more popular outside the automotive industry. It has many applications like product tracking, document management, item identification, time tracking, general marketing, and many more.

A QR code consists of black dots or structures (square dots) put in a square structure of grid on a white background. It can be interpret by an imaging tool like a camera and can be processed using ReedSolomon error correction unless the image or structure is appropriately interpreted. The necessary information is then extracted from structures present in both horizontal and vertical components of the QR representation.

IV. IMPLEMENTATION STRATEGY SHOWING RESULT

The system is proposed in such a way that a workstation

and mobile device is connected through data cable. When communication between them takes place the implemented security scheme prevents the system from MIM attack. Here a security system is implemented wherein signature creation is done and using this verification is performed. In this system implementation RSA algorithm is used along with SHA1 for hashing. System software is implemented on workstation and on mobile device. For login credentials on the mobile device QR codes are used in system implementation. Mathematical details and the details of the implemented application system is described below in equations and with snapshots.

Figures and working mechanism is explained below:

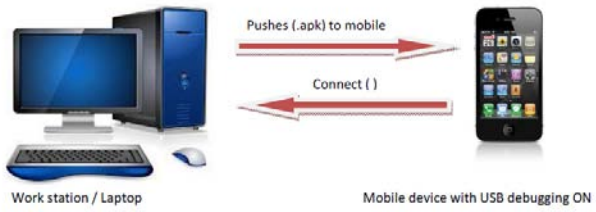

Figure 1. Diagram showing communication between workstation and mobile device.

At first a workstation and a mobile device is connected using a wired connection, USB cable in this case. A GUI is run on workstation through which a file can be selected for encryption and that file can be sent to mobile device then.

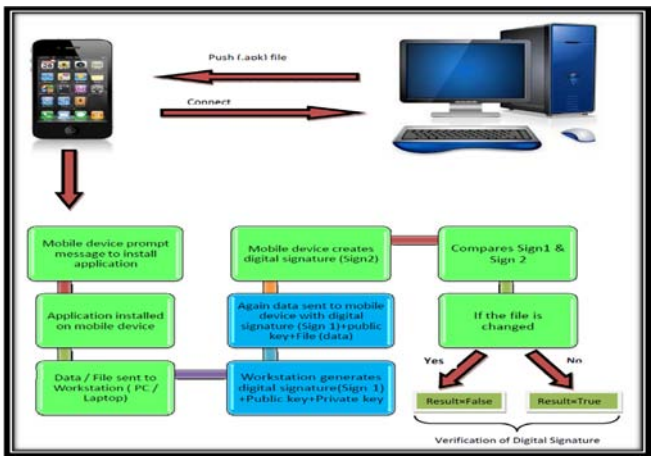

Figure 2. Diagram showing generation and verification of keys in Workstation and in mobile device.

Encrypted file and signature are pushed to mobile device. Below diagram shows the complete process to be followed for generating signature and pushing it to mobile device.

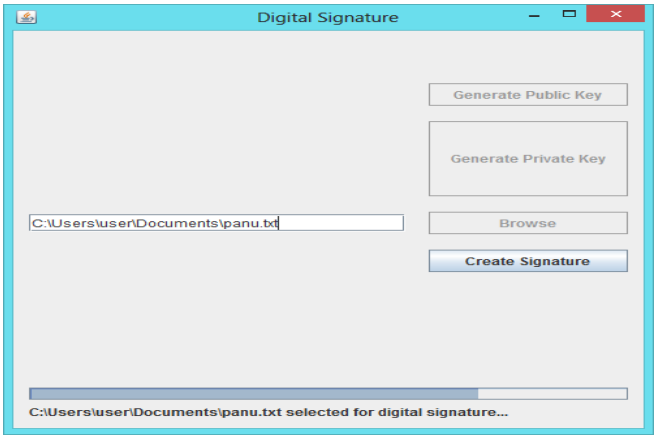

Figure 3. GUI on workstation for creating signature.

Once the file is sent to mobile device there comes pop up from application installed and one more signature is generated on mobile device. For logging into the mobile device user has to login using QR code.

Figure 4. Example of two dimentional QR code.

Only limited users have authority to login into application using QR code. System administrator defines the user list for accessing the application. Signature generated from workstation is compared with signature generated on mobile device. If the signature matches then notification comes that Signature matched and data is not altered. If there is data alteration in between the network communication then signature does not match and notification comes that data is altered in communication.

A. Mathematical Model

This paper is using DSA algorithm for Generating signature, Encrypting data and for verification of signature.
DSA:
It involves two phases for Key generation. Parameter generation and key generation. For parameter generation SHA1(Secure Hash Algorithm) used to create message digests for a given message[3]. SHA1 is chosen and not the SHA as SHA1 is more secure and strong when compared with SHA.

- Key length L and N has to be selected first. This is the cryptographic strength of the key, which is to be generated. As per the DSS constraint L should

be a multiple of 64 and should be in between 512 and 1024.

- An N-bit prime q is chosen where N is less than length of hash output, or it could be equal to the length of hash output.
- An L-bit prime modulus p is chosen in such a way that p–1 is a in multiples of q.
- A number g is chosen in such a way that its multiplicative order modulo(p) is q.
- The parameters of algorithm (p, q, g) can be given to different system users.

Using these parameters in second phase of key generation public key and private key is generated. x is chosen using a random method PRNG (Pseudo Random Number Generator) where

$$0 < x < q$$
$$y = g^x \bmod p$$

Public key is (p, q, g, y) and private key is x.
Once public key and private key is generated the next step is to encrypt the data. User is provided with the option to browse a file from workstation on GUI. Once the file is selected by user data from file is signed by following below steps.

- Assume H as a hash function and assume m the message.
- A random value k is generated per message. Where $0 < k < q$.
- Calculate next $r = (g^k \bmod p) \bmod q$ unless $r = 0$.
- Then calculate $s = k^{-1} (H(m) + xr) \bmod q$ unless $s = 0$.
- The signature generated is (r, s).

After creating signature sign1 on workstation the file is sent from workstation to mobile device. Mobile device receives the public key, encrypted file and signature. Mobile device creates new signature sign2 now. Next step is comparing and verifying signature created on workstation sign1 and signature created on mobile sign2. The steps followed for verifying the signatures sign1 and sign2 are given below:

- The signer of data computes $s = k^{-1}(H(m) + xr) \bmod q$
- Thus
  $k \equiv H(m)s^{-1} xrs^{-1}$
  $\equiv H(m)w + xrw \pmod q$

Asg has order q(mod p) we have

$gk \equiv g^{H(m)w} g^{xrw}$
$\equiv g^{H(m)w} y^{rw}$
$\equiv g^{u1} y^{u2} \pmod p$

- At the end DSA follows its correctness from
  $r = (g^k \bmod p) \bmod q$
  $= (g^{u1}y^{u2} \bmod p) \bmod q$
  $= v$

Hence the signature is verified with the use of Hash function and PRNG.

Hash Function:

Hash function is an algorithm that maps data sets of variable length to data sets of a fixed length. e.g. a person's details, could be hashed to a single integer. The values given as output by a hash function are hash values, hash codes, hash sums, checksums or simply hashes.
Hash tables:
Hash functions are mainly used in hash tables, to quickly locate a data record (e.g., a dictionary definition) when key list or search key is given. In particular, the hash function is used to map the search key to an index. The index outputs a specific location in the hash table where the respective record should be stored. Hash tables, in turn, are utilized to implement associative arrays and dynamic bands.

Typically, the domain of a hash function which includes the set of possible keys is larger than its range, and so it maps number of different keys to the same index. Thus, each slot of a hash table is linked implicitly or explicitly with a set of records, rather than a single record. For this understanding, each slot of a hash table is called a bucket, and hash values are called bucket indices.

SHA-1
SHA-1 is a cryptographic hash function which produces a 160-bit hash value. A SHA-1 hash value is typically shown as a 40 digits hexadecimal number. SHA means"secure hash algorithm". The four SHA algorithms do have different structures and are differentiated as SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 algorithm is very alike to SHA-0. But it corrects an error in the original SHA hash specification that led it to major weakness. The SHA-0 algorithm was not embraced by many applications. SHA-2 on the other side considerably differs from the SHA-1 hash function. SHA-1 is the most extensively used of the existing SHA hash functions, and is used in several widely used applications and protocols.

V. RESULTS AND DISCUSSION

Mobisecure using DSA was tested in real environment where system was installed on mobile devices having android operating system. In Xperia Z (C6602) model it took very less time to generate keys and transfer file to mobile device and again validate the keys. The duration is more because it also involves human intervention. This mechanism was also tested on Samsung galaxy grand GT-I9082 and HTC Desire 816G dual sim, Karbonn A15+. The difference in the duration to compute the result is due to the configuration of the device like RAM, cache and its internal or external memory. It also depends on the camera autofocus facility as this paper are uses it for scanning the QR code for login purpose.

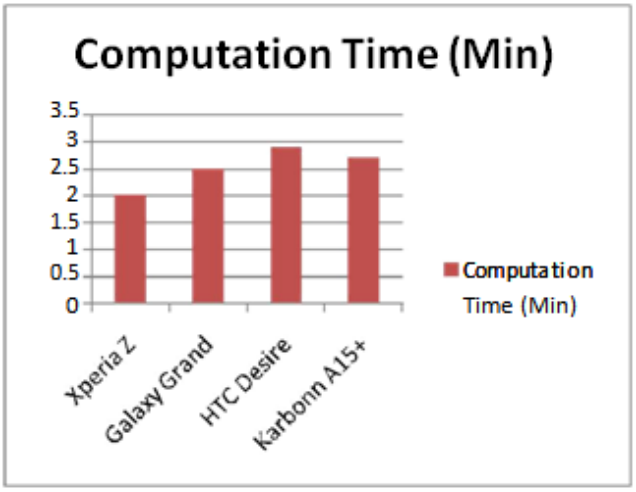

Fig. 5 Comparative analysis of time required for generation and verification of keys.

Fig 5 denotes the difference between computation time taken by different mobile devices. Time taken for running the application is inversely proportion to mobile device configuration. As good the configuration of mobile device will the lesser the computation time.

VI. CONCLUSION

This paper shows that security can be ensured using signature creation and verification in android mobile devices when connected in a wired network. Along with wired networks it is also necessary to ensure the same security using the same mechanism in wireless network. So implementation of signature creation and verification to ensure security in communication between android mobile device and workstation is future work.

VII. ACKNOWLEDGEMENT

The electronic signature is essential to offer non repudiation services which make secure e-commerce possible [2] [1]. As different technologies and infrastructures have been produced with the intention of implementing mobile signature processes. Using various digital signature algorithms, communication in mobile devices, this also can be made as secure as other devices with the use of Digital signature. Digital signature algorithms can be the foundation for a great batch of future inquiry as it provides security and helps in understanding of data alteration while in communication.

VIII. REFERENCES

[1] Cristian UDREA. IT&C Security Master. Department of Economic Informatics and Cybernetics. The Bucharest University of Economic Studies. ROMANIA. “Mobile Solution for Digital Signature”

[2] G Luiz Castelo Branco LG Electronics de So Paulo Ltda. South Central America R and D Lab. Open OS Team , ”A Digital Signature for Mobile Devices: A New Implementation and Evaluation” , Windows Mobile 2011.

[3] Antonio Ruiz-Martnez, Daniel Snchez-Martnez, Mara Martnez-Montesinos and Antonio F. Gmez-Skarmeta University of Murcia, Department of Information and Communications Engineering , ”A Survey of Electronic Signature Solutions in Mobile Devices” , 2007.

[4] Xuhua Ding, Daniele Mazzocchi, Gene Tsudik. , ”Experimenting with Server-Aided Signatures”, in In Proceedings of Network and Distributed System Security Symposium (NDSS2002),San Diego, 2002.

[5] Public Key Cryptography Standards(PKCS), No.1, RSA Encryption standard in

http://www.rsasecurity.com/rsalabs/pkcs.

[6] Jos Manuel Forns Rumbao, Department of Telematic Engineering, Seville University, Seville, ”Digital Signature Platform on Mobile Devices” , Spain (2011).

[7] Min Zheng, Mingshen Sun, John C.S. Lui Computer Science and Engineering Department The Chinese University of Hong Kong, ”[6] DroidAnalytics: A Signature Based Analytic System to Collect, Extract, Analyze and Associate Android Malware”, 2013.

[8] Hiroki Kuzuno ,Satoshi Tonami Intelligent Systems Laboratory, SECOM, Tokyo, Japan, ”Signature Generation for Sensitive Information Leakage in Android Applications” , 2013.

[9] Florian Nentwich, Engin Kirda, and Christopher Kruegel Secure Systems Lab, Technical University Vienna , ”Practical Security Aspects of Digital Signature Systems”,jun 2006.