Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 1, January 2016, pg.226 – 232

Android Mobile Security using Secure Hash Algorithm

Ms. Pranoti Panchal, Prof. Savitri Patil
Department of Computer Engineering, G. H. Raisoni College of Engineering and Management, Pune, Maharashtra, India
pranotipanchal@gmail.com, savithri3010@gmail.com

Abstract— Mobile devices are easily accessible to everyone now days. Mobile technology is upgrading every day hence data transfer security is the basic threat, for which highly secured mechanism is required to avoid fraudulent access to any confidential data or information. Like e-mail broadcast, e-commerce or some financial transactions it is required that both sender and receiver of the data or information should sign the document and convert it digitally, making data transfer more reliable. This paper highlights the means of digital signature mechanisms & its certifications to implement it easily in mobile devices to protect from MIM and fraudulent access to any confidential data or information.

Keywords— QR Code, DSA, PRNG, SHA1, Digital Signature

INTRODUCTION

When in 70's computers & its networks were invented, they were very complicated to understand & costly as well. Later this technology was used by universities for educational purpose & for military applications data security has became a serious concern. This scenario has changed when in 80's two major engineering inventions was done. The first was microprocessors having more process capability & lower cost impact, and the second was LANs having high speed data transfer capabilities in local networks. These inventions made it necessary to create regulations for this technologies safe use by researchers & business people in day to day business activities, like banking, purchases and many more. Later due to revolution in mobile industry has made mobile devices smarter with the help of internet & 3G services. This advancement in the mobile technology has made access to all internet related services handy & that too with less cost with optimum speed, which has become milestone in this segment of industry, which has been accepted by users undoubtedly, resulting increased market for smart phone users.

Now this technical optimization has also attracted by some bad intensions which has raised a point of data / information security. Also increased cases of fraudulent practices have become serious concern for financial, economical, educational fields, which was having major reliability for data / information transfer on this technology. This has laid a foundation to invent more secure & reliable ways / methodologies to ensure data / information transfer.

CRYPTOGRAPHY

Digital signature is nothing but an encrypted message or its representation. When communication content is locked in a secret key it is called as encryption. For improved efficiency of encryption massage digest is considered instead of massage.

The digital signature mechanisms steps are as follows:

1) Using sender's private key, massage digest is calculated followed by encryption on the digest. This is nothing but a digital signature. [1]
2) Receiver receives a digital signature with a message from sender.
3) After receipt of data, by using senders public key receiver decodes the digital signature & hence senders message digest is generated again, at receivers location.
4) From the received message data, message digest is calculated by receiver, & it is verified that message data created & received is the same. [1]

Verified digital signature gives confirmation to receiver that received message is not altered during communication; also it confirms that it has been shared by the same authority who has claimed to send it. Authentification & integrity of message is ensured by digital signature. Evidence of source & Authentification of sender is ensured by digital signature.

DSA BY USING ALGORITHMS

Digital signature is nothing but a sequence of three algorithms:

1) A key generation algorithm – is nothing but selecting one private key from the set of possible private keys. Due to this algorithm a private key along with its public key is generated.
2) A signing algorithm – if a message & private key is given this generates a digital signature.
3) A signature verifying algorithm – This is a accepting or rejecting mechanism for message when public key, signature & message is given to it.

A. A Key Generation Algorithm

Key generation in DSA involves two stages. First stage comprises of selection of algorithm parameters. These parameters can be given to variety of users of the implemented system. Second stage involves cryptographic computation of private and public keys. Encryption & decryption of message or data in communication is done using public and private keys generated here.

Parameter is generated using SHA1 (Secure Hash Algorithm). In SHA1 consists of message's conversion in small data sets known as message digests. Once message digest is created, using PRNG (Pseudo Random number Generator) we can generate random numbers from same digest.

B. Network Security & attacks on it

Old era was having limited skill set & knowledge levels so that it was not so easy or frequent to breach data / information during communication stage, but now a days this widespread information source has given skill & knowledge to almost everyone, who can easily became a hacker & source the information for personal purpose. This has highlighted the requirement of shielded networks & resisted for static safety policies.

To protect a network from an outsider threats is to close all loops of the entire network from the outdoor world. This closed network can give connectivity only for trustworthy participants and websites and it will not allow to any link to outsider public networks and by thus restricts the dealings among them.

Several types of network attacks are enlisted below:

Eavesdropping: Major communication done in open network is not always encrypted or has clear text format in it, this allows invaders to invade in communication, gain access to data / information in open network and interpret nature of communication. When an invader is scrutinizing communication in LAN without getting anyone to notice, it is called as sniffing / snooping.

Data Modification: When a hacker refers your data, the next immediate step is to alter it. It is not so frequent that if a hacker makes alterations in a data, it will come to notice of a sender or receiver. It may happen that there is no requirement for confidentiality of data in communication but no one wants to get changes done in data in communication [5]. For example while exchanging sales data you do not want the details like price, quantity or billing details to be changed in between.

Identity Spoofing (IP Address Spoofing): To validate communicating entity most of the operating systems refers IP address. In few cases it may possible for an IP address to be incorrectly assumed & this is called as identity spoofing. An hacker may also use additional programs to create fake IP packets that looks like to original lawful address from inside the network.

Hence if a fake IP address is validated in system then hacker can easily update, recreate, or manipulate the information. The hacker can also try for some Password-Based Attacks. This precisely indicates the relation in networks, user name and password. If hacker gets access to network and its resources it is very easy to hack login credentials and manipulate the data on behalf of trusted entity.

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

Man-in-the-Middle Attack: When two participants are communicating and some third entity is able to actively monitor, manipulate or take hold of the communication in transparent way then it is called as Man-in-the-middle attack.

Sniffer Attack: It is an attack on communication using an application or device or program which is able to scan, monitor, and capture network data from communications and read message digests involved in network.

C. Barcodes

Barcodes are figures which can accessed or read by using having camera and laser can be scanned using electronic medium. Using barcodes we can encode the information like product numbers, serial numbers and also batch numbers. Also barcodes helps in automatically identifying and tracking products in shopping carts of malls and also in supply chains operations.

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

QR(Quick response code) Codes is nothing but a type of 2D barcode, The QR Code system is fast, readable and have great storage capacity as compared to with UPC barcodes. This additional benefit makes it more popular outside the automotive industry. It has many applications like material tracking, document management, identification of items, time tracking, general marketing etc.

A QR code is comprising of black square dots structure of grid on a white background. It can be easily interpreted by an imaging tool like a camera and can be processed using Reed Solomon 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.

IMPLEMENTATION STRATEGY SHOWING RESULT

The proposed system here is in such a way that a workstation (Laptop, Desktop) and mobile device is connected through a data cable. When communication between these two devices is done then the implemented security scheme prevents the system from MIM attack. Here a security system is implemented once signature creation is done and using this verification process is completed. In this system for hashing implementation RSA algorithm is used with SHA1. Recommended software is implemented on both workstation and on mobile device. For login credentials on the mobile device QR codes are used in system.. Mathematical module and application systems details of the implementation are described below in equations with respective screen snaps.

Working mechanism is described as bellow:

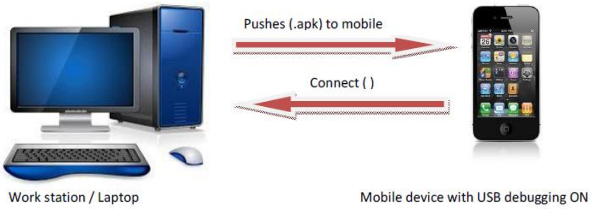


Fig. 1 Schematic for communication in workstation and mobile device.

At first a workstation and a mobile device is connected using a wired connection like data cable for this case. As a GUI is run on workstation we can select a file for encryption and that file can be sent to mobile device later.

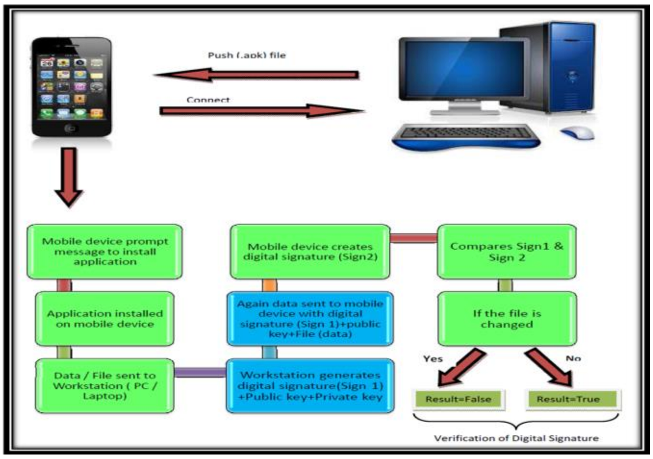
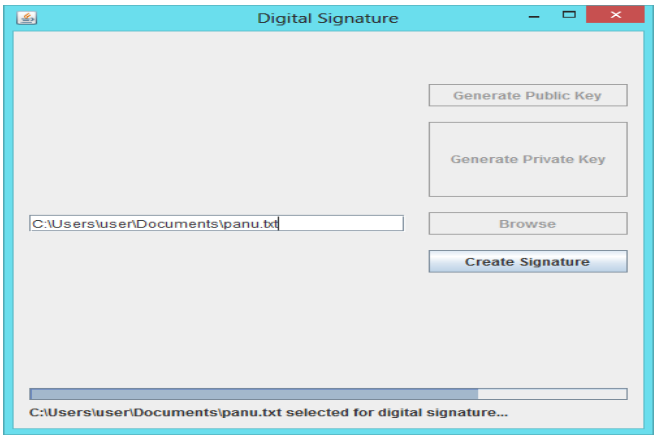

Push (.apk) file
Connect
Mobile device prompt message to install application
Application installed on mobile device
Data / File sent to Workstation (PC / Laptop)
Mobile device creates digital signature (Sign2)
Again data sent to mobile device with digital signature (Sign 1)+public key+File (data)
Workstation generates digital signature(Sign 1) +Public key+Private key
Compares Sign1 & Sign 2
If the file is changed
Yes
No
Result=False
Result=True
Verification of Digital Signature

Fig. 2 Schematic showing flow chart for generation and verification of keys in Workstation and in mobile device.

Encrypted file and signature are sent to mobile device.

Below schematic shows the complete process to be followed for generating signature and sending it to mobile device.



C:\Users\user\Documents\panu.txt

C:\Users\user\Documents\panu.txt selected for digital signature...

Fig. 3 GUI on workstation for creating signature.

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

Fig. 4 QR Code

Only limited users has authority to login into application using QR code. An administrator defines the user list for accessing the application. A workstation signature generated is compared with signature generated on mobile device. If both the signature matches then notification comes that Signature matched and data is unaltered. If there is data changed in between the network while communication then signature does not match and notified that data is altered in communication.

A Mathematical Model

For generating signature this paper uses DSA algorithm. The same algorithm is used for Generation of signature, encryption of data and for verifying signature as well.

DSA:

There are two phases of Key generation in DSA algorithm. Key generation and Parameter generation. In first step of parameter generation message is converted into message digests using Secure Hash Algorith1 (SHA1)[3]. There is SHA algorithm as well similar to SHA1 but it is not chosen here as more strong and secure way is using SHA1.

For progressing on key generation L and N are selected firstly for key length. Doing this ensures key's cryptographic strength. There is constraint of DSS that L is multiple of and ranges from 512 to 1024.

- A variable q is selected which is N-bit prime where N is smaller compared to hash output length or it is equal to hash output length.
- A variable p is selected which is A L-bit prime modulus p and selection is done is a way where p–1 is a in the multiples of q.
- q is chosen in a way where its multiplicative order modulo(p) is q.
- The selected algorithmic parameters (p, q, g) could be given to various users of system.

These parameters are used in Key generation, second phase of DSA algorithm wherein private key and public ky are generated. PRNG (Pseudo Random Number Generator) is used for selecting a value of x where

$$0 < x < q$$

$$y = gx \bmod p$$

Here Public key set is (p, q, g, y) and private key set is x.

Once both the keys namely private key and public key is generated it comes to next process of encrypting the data from message. System user is given an option to select a file from system using workstation GUI. Once the file is browsed and chosen by user, signing of the message is done by processing below no of steps.

- Assume H as hash function & m as the message.
- A random integer k is generated for each individual message. Where $0 < k < q$.
- r is calculated next as $r = (gk \bmod p) \bmod q$ until
  $r = 0$.
- Sis calculated as $s = k-1\ (H(m) + xr) \bmod q$ until
  $s = 0$.
- Signature generated using above steps is (r, s).

On workstation signature is created and let's assume it as sign1. Sign1 is sent from workstation to android mobile device. Android mobile device receives the encrypted file, public key and signature. Android mobile device receives sign1 and creates its own signature sign2. Next process is of comparing signature sign1 with signature sign2 and verifying that whether they match or not. The process followed for comparing and verifying the signatures sign1 and mobile device signature sign2 are listed below:

- The signing entity of message computes

$s = k-1(H(m) + xr \quad) \bmod q$

- Thus
  $k \equiv H(m)s-1\ xrs-1$

  $\equiv H(m)w + xrw \pmod q$

Since g has order q(mod p) we get

$$gk \equiv gH(m)w\ gxrw$$

$$\equiv\ gH(m)w\ yrw$$

$$\equiv\ gu1\ yu2\ (\mathrm{mod}\ p)$$

- In the end of process DSA follows

$r = (gk \bmod p) \bmod q$

$= (gu1yu2mod\ p) \bmod q$

$= v$

Hence the signatures sign1 and sign2 are verified using Hash function (SHA1) and Pseudo Random Number Generator (PRNG).

Hash Function:
It is nothing but an algorithm which can map data set of inconsistent length to data set of a consistent or fixed length. e.g. an organization’s details can be hashed into a single integer. Hash function might give hash codes, checksums, hash values, hash sums as outputs.

Hash tables:
Hash tables use hash functions for quickly locating records in database when search keys or key list are provided. Hash functions are mainly used for mapping search keys to indexes. The index gives output of a path or specific location where the required and respective record is stored.

There is concept of bucket or bucket indices in hash tables. Some hash values are referred to as bucket indices in cases where various numbers of keys are referring to the same index. The concept is also used in scenarios where has tables are linked with number of records than a single number of record.

SHA-1
It is a hash function used in cryptography which can produce 160-bit hash value. SHA is ‘Secure Hash Algorithm’. It is typically seen as a hexadecimal number of digits. There are four varieties of SHA algorithms with different structures namely SHA-0, SHA-1, SHA-2, and SHA-3. SHA-1 algorithm is similar to SHA except it corrects error from SHA-0. The error corrected was a major weakness of SHA – 0. Because of weakness in SHA – 0 the algorithm is not used by many applications. SHA-2 is also very popular and different from SHA -1. Among all SHA algorithms SHA-1 is the most popular hash function and is widely used in many applications.

RESULTS AND CONCLUSION

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

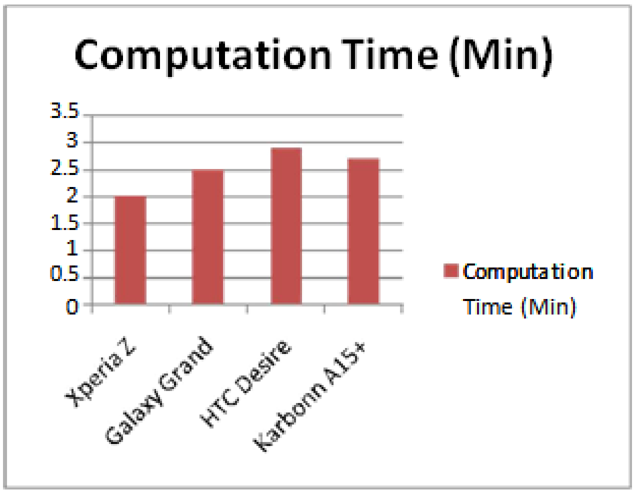


Fig. 5 Comparative analysis of time required for generation and verification of keys.

Fig 5 highlights the computation time difference taken by different mobile devices. Time taken for running the application is directly proportional to mobile device's superior configuration. As good the configuration of mobile device is it will take lesser computation time.

CONCLUSIONS

This paper indicates that security can be confirmed using signature creation and its verification in android mobile devices when connected in a wired network. With wired networks it is also mandatory to ensure the same security using the same mechanism in wireless network. So signature creation and verification to ensure security in communication between android mobile device and workstation is wirelessly is future scope of work.

ACKNOWLEDGEMENT

The electronic or digital signature is essential to offer non disclaimer services which make secure e-commerce possible [2] [1]. Different technologies and infrastructures have been used with the intention of implementing mobile signature processes more effectively. Using various permutations & combinations of digital signature algorithms, communication in mobile devices can also be made as secure as other devices with the use of Digital signature. Digital signature algorithms can be the base for a great bunch of future inquiry as it provides security and helps in understanding of data manipulation while in between communication.

REFERENCES

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.
[2] Cristian UDREA. *Mobile Solution for Digital Signature* IT&C Security Master. Department of Economic Informatics and Cybernetics. The Bucharest University of Economic Studies. ROMANIA.
[3] G Luiz Castelo Branco LG Electronics de So Paulo Ltda. *A Digital Signature for Mobile Devices: A New Implementation and Evaluation* South Central America R and D Lab. Open OS Team, Windows Mobile 2011.
[4] Antonio Ruiz-Martnez, Daniel Snchez-Martnez, Mara Martnez-Montesinos and Antonio F. *A Survey of Electronic Signature Solutions in Mobile Devices* ,Gmez-Skarmeta University of Murcia, Department of Information and Communications Engineering , 2007.
[5] 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.
[6] Public Key Cryptography Standards(PKCS), No.1, RSA Encryption standard in
http://www.rsasecurity.com/rsalabs/pkcs.
[7] Jos Manuel Forns Rumbao, *Digital Signature Platform on Mobile Devices* , Department of Telematic Engineering, Seville University, Seville, Spain (2011).
[8] Min Zheng, Mingshen Sun, John C.S. Lui ”[6] *DroidAnalytics: A Signature Based Analytic System to Collect, Extract, Analyze and Associate Android Malware,* Computer Science and Engineering Department The Chinese University of Hong Kong, 2013.
[9] Hiroki Kuzuno ,Satoshi Tonami *Signature Generation for Sensitive Information Leakage in Android Applications*, Intelligent Systems Laboratory, SECOM, Tokyo, Japan, 2013.
[10] Florian Nentwich, Engin Kirda, and Christopher Kruegel Secure *Practical Security Aspects of Digital Signature Systems* , Systems Lab, Technical University Vienna , jun 2006.