DESIGN AND DEVELOPMENT OF NON-SERVER PEER 2 PEER SECURE COMMUNICATION USING J_K-RSA CRYPTO SYSTEM

Sulaiman AlMuhteb[1], Padmavathamma Mokkala[2]

[1]Research Scholar, Department of Computer Science, S.V.University, Tirupathi
[2]HOD, Department of Computer Science, S.V.University, Tirupathi

Abstract

Wireless Portable Device such as Mobile, Tablet and PDA's are considered to be the most common communication devices in recent days. Recently, Portable Device such as Tablet's and mobile phones are not only used for casual greetings but also using for business such as sending and receiving important data like social security numbers, bank account details and passwords. Public key cryptography is a proven security solution, which can be used to secure the mobile communications. Several researchers have proposed server-based architectures public key cryptography solution to secure the mobile communications. Third party servers were used to check the certificates, authenticating the communicating parties, key distribution, etc.

This paper proposes and implements a non-server such as Peer 2 Peer architecture public key cryptography to secure the mobile communications. The proposed implementation of public key cryptography can provide confidentiality, authentication, integrity and non-repudiation security services needed for mobile communication. Compared with server based architecture, non-server based architecture has lower risk and the security has been improved, to avoid many kinds of attacks

Keywords— *Cryptography, Public key cryptography, peer to peer, confidentiality, authentication, integrity and nonrepudiation, Portable device communication security*

----------***----------

1. INTRODUCTION

Today, Wireless Device such as mobile phones, PDA's and Tablet PC's are considered to be the most common communication devices in history. The majority of them are sending and receiving SMS texts, or making calls, it is sometimes used to exchange sensitive information between communicating parties. In some cases however, this data may also include very private information reserved for the personal viewing of the legal recipient. Nowadays, the visibility of security applications is wide the term security, presented in the scholar papers, side by side, with terms; confidentiality, integrity, authenticity, non-repudiation, privacy and data protection. It may not be exaggerating if we say e-communication life equal to security, have significant impact on consumers' perception about e-banking security.

Public key cryptography is a proven solution, which can be used to secure mobile communications. The usage of public key cryptography can provide the confidentiality, authentication, integrity and non-repudiation security services needed to secure mobile communications. Due to the limitation of the mobile devices resources, implementing a public key cryptography solution to secure peer to peer communication has become a challenge. This paper proposes an alternative solution to secure the peer to peer mobile communications in regards to confidentiality, authentication, and integrity and non-repudiation security services. The proposed solution is developed and tested on the real mobile phone devices.

2. PURPOSES

The objectives of this paper are: to identify the appropriate technique for peer-to-peer mobile communications security to propose an alternative solution for securing mobile communications; to develop and test the proposed technique in regards to confidentiality, authentication, integrity and nonrepudiation services.

- What are the existing end-to-end mobile communication security solutions weaknesses?
- How can we develop the end-to-end mobile communication security solution which guarantees the confidentiality, integrity, authentication and nonrepudiation security services?
- How can we provide the end-to-end mobile communication security without depending on mobile network operator or third party?
- How can we develop a solution for end-to-end mobile communication security that is implementable by individuals as well as by the commercial ones?

3. RESEARCH METHODOLOGY

In this paper, we initiated with overview, the current mobile communication security solutions, and discussed the challenges of public key cryptography implementation in non-server architecture, followed by a proposed mobile security solution. This solution implements public key cryptography in non-server architecture. Finally, we discussed the proposed solution security and the potential risks.

This research is conducted in as organized further:

- CURRENT SOLUTIONS.
- NON-SERVER ARCHITECTURE VERSUS SERVER ARCHITECTURE.
- PUBLIC KEY CRYPTOGRAPHY IMPLEMENTATION IN NON-SERVER ARCHITECTURE CHALLENGES.
- PUBLIC KEY GENERATION OF J_K-RSA.
- PUBLIC KEYS STORAGE OF J_K-RSA..
- PUBLIC KEY DISTRIBUTION OF J_K-RSA- KEY EXCHANGE SESSION.
- SENDERS AUTHENTICATING USING OF J_K-RSA.

3.1 Current Solutions

Many researches have proposed solutions to secure the mobile phone communication by using public key cryptography. However, the majority of the solutions are server architecture and the mobile operator or service provider will control the servers. The servers in such architecture are controlling the cryptographic key generations and key distributions and authenticate the users. One of the main reasons for not implementing public key cryptography in non-server architecture is the restricted resources (that is, computing power and storage capacity) in the mobile phone devices. The second important reason is the user's authentication scheme. How can the user authenticate the sender entity in non-server architecture systems?

3.2 Non-Server Architecture Versus Server Architecture

Most of the mobile communications security solutions that are based on public key cryptography rely on the mobile phone network operator or service provider as part of the proposed solutions. Generally, the server architecture solutions needs additional hardware (that is, servers) and as a result, needs qualified staff to maintain the servers. Moreover, server architecture mobile security systems user has to get the mobile network operator or the service provider's approval, because it depends on their servers. Besides, the overhead cost of communication is increased due to users need to access the servers in many cases such as uploading and downloading the cryptographic keys[1]. We do not expect that the mobile operators will provide security services to the transmitted data through the SMS service for individuals, at least not in the near future

On the other hand, non-server architecture mobile communications security solutions are implementable for individuals due to its independency from the mobile phone network operator or service provider. Thus, the user does not need to make any agreement with the mobile phone network operator or service provider. As a result, all the cryptographic operations are achieved on the user's mobile phone. Terms of overhead cost of communication is less than server architecture system, due to discard in the communication between the user and the server. Most of the current non-server mobile security systems are based on symmetric cryptographic algorithms.

For example, CryptoGraf[2] messaging software is used to encrypt messages with AES algorithm within the mobile phones without requiring any server.

3.3 Public Key Cryptography Implementation in Non-Server Architecture Challenges

In server architecture mobile phone security system, the server is used to do two main tasks; managing the cryptographic keys (that is, key generation, key storage and key distribution) and users' authentication. Thus in non-server architecture, users have to handle these tasks by themselves. These tasks are difficult to handle by the mobile phone devices because of the fact that most popular public key cryptography algorithms, demand a high power computing, which is not available in the mobile phone devices. Thus, using public key cryptography algorithms on the mobile phone will cause negative effects on the mobile phone performance (that is, slow in response, wasting time). As a result, many of the researchers proposed using a server structure for the mobile phone security systems. Nevertheless, when the public key cryptography operations are achieved on the mobile phone, it will be possible to implement the public key cryptography in nonserver architecture mobile phone security systems. Further, discussions for the public key cryptography operations are achieved by the server.

3.4 Public Key Generation of J_k-RSA.

Public key cryptography algorithms require a lot of complex calculations and needs high computational power, which is not found in most mobile phones. Usually, the most cryptographic operation that consumes the computing power is the key generation. To overcome this obstacle, the selected algorithm should have a high speed and should not demand high computing ability.

3.5 Public Keys Storage

In the case of the non-server architecture mobile security systems, the number of users will be somehow small, furthermore, the number of keys will be a bit limited, and thus, it is possible to store the keys on the user's mobile phone. The size of the public key for the user does not exceed 256 bytes, meaning that one mega byte may store more than four thousands keys, thus, each user can be satisfied with less than one mega byte. In addition, one mega byte storage is not counted, compared to the current phone memory sizes. Furthermore, most of today's wireless phones are designed to deal with extra memory, thus, the storage capacity of the mobile phone is no longer a problem.

3.6 Public Key Distribution

In non-server architecture, users have to exchange the public keys among them. The users have to request the needed key from their partners directly; in this case the partners would

send their public keys via encrypted and signed messages. The users can check the originality of the received keys by verifying the signature and then keep them in encrypted format for later usage. Not until this time, there is no need to have access to the server in order to get the partners' keys when needed. The problem is in the first communication, when the users don't have their partners' public keys and as a result, they can neither decrypt nor verify the encrypted and signed messages. To solve this problem, a key exchange session can be used for the purpose of key exchange at the first time.

4. PROPOSED SCHEME FOR PUBLIC KEY CRYPTOGRAPHY IMPLEMENTATION IN NON-SERVER ARCHITECTURE

In such schemes, there are two main problems; the selected public key cryptography algorithm must have low demand of power computing to achieve the cryptographic operations. We have to find a public key cryptography algorithm that can run fast enough on the mobile phones and achieve all required cryptographic operations without negative effects on the mobile phone's performance; the main problem is how the user can authenticate the sender in first contact. In this section we discuss the selected public key cryptography algorithm as well as the proposed scheme for exchange cryptographic keys for first time.

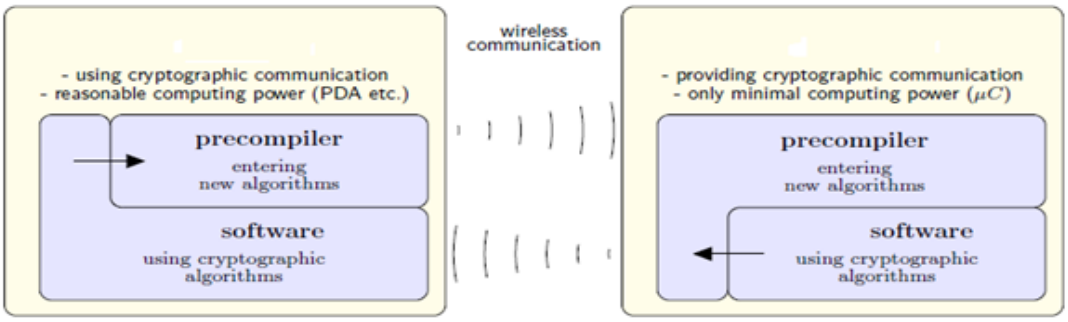

Figure 1. Non-server architecture mobile security system

4.1 Selected Public Key Cryptography Algorithm – J_K-RSA Cryptosystem

RSA [3,4] are considered as the most popular public key cryptography algorithms. In the literature, they reported many weaknesses on RSA, they stated RSA is slow; RSA is not secure if the same message is encrypted to several receivers, to completely break RSA one needs to find the prime factors. In practice, RSA has proved to be quite slow, especially for key generation algorithm. Furthermore, RSA is not well suited for limited environments like mobile phones and smart cards without RSA co-processors, because it is hard to implement large integer modular arithmetic on such environments. a new standard was approved for public key cryptography called Jordan Totient function RSA is J_K-RSA[5,6] crypto system. Preliminary experimental results show the advantages of J_k-RSA over RSA, such as, at similar security level, the speed of J_k-RSA is much faster than that of RSA; the key generation is more than 20 times faster.

J_k-RSA has been proposed to speed up RSA implementations; J_k-RSA implementations require two major operations: squaring reduction and multiplication reduction. The benefit of J_k-RSA is lower computational cost for the decryption and signature primitives, provided that the CRT (Chinese Remainder Theorem) is used. Better performance can be achieved on single processor platforms, but to a greater extent on multiprocessor platforms, where the modular exponentiations involved can be done in parallel.

J_k- RSA Cryptosystem:

Implementing new Public Key Cryptosystems which was an extend variant analyzed in using the properties of Jordan Totient function J_k-RSA modulus so that it consists of r primes p1,p2,--------, pr instead of the traditional two primes p and q.

Compute $N=\prod_{i=1}^{r} p_i = p_1.p_2.....p_r$ and

$$J_K(N) = n^k \prod_{p|k} (1-p^{-k}) = (p_1^k-1)(p_2^k-1)-----(p_r^k-1)$$

$$= \prod_{i=1}^{r} (p_i^k - 1)$$

Choose a random integer $e< J_K(N)$ such that gcd $(e, J_k(N)) = 1$.

Compute the integer d Which is the inverse of e i.e, $ed = 1 \pmod{J_k(n)}$

Encryption Process: For a given plain text '**m'** which belongs to 'Z_N ' the encryption algorithm is the same as that of the original RSA

Ciphertext $c = m^e \bmod N$

Decryption Process: In order to decrypt a cipher-text *c*:

For a given cipher text '**c'** which belongs to 'Z_N ' the decryption algorithm is the same as that of the original RSA

Decryption message (plain text) $m = c^d \bmod N$

4.2 Keys Exchange Session Using Diffie-Hellman

We proposed to implement public key cryptography on the mobile phone by using Jordan Totient on RSA algorithm. Which is a J_k-RSA public key cryptography, mobile phones will be able to achieve all cryptographic operations such as key generation, encryption /decryption and signing /verifying without relying on the third party's server. The users will also gain the confidentiality, authentication, integrity and non-repudiation security services for their mobile phone communication. However, the problem of how the communicating parties authentic each other appears. Although, the problem has been faced in first contact only; meaning that when they did not have each other's public keys. To solve this problem, we proposed to use key exchange session to exchange the public key between them. The key exchange session is used in the proposed system. Diffie-Hellman[7] algorithm is used to make agreement on a temporary key that is used with encrypt the public key and exchange it with the partners

Figure 2 illustrates the key exchange session steps. Mobile User X can start the key exchange session immediately after he/she generates his/her public keys and add Mobile User *Y* contact information to his/her contacts list.

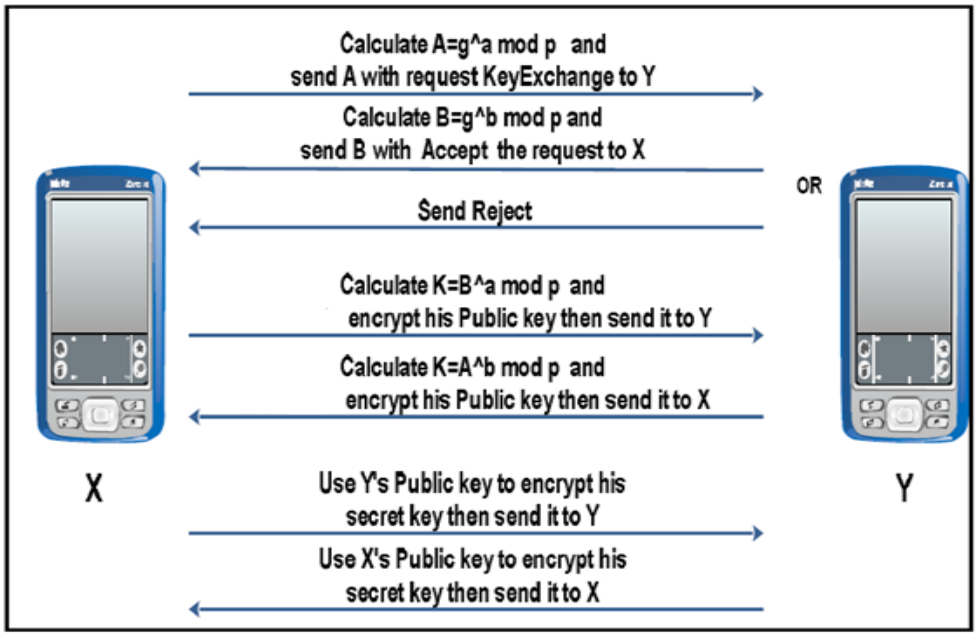

Fig 2 The key exchange session steps between mobile user X and Y

He/she can start the key exchange session by calculating the value of A, depending on the secretly generated value a, and the shared secret parameters g and p (that is, g and p are fixed by the mobile application).

$$A=g\text{^}a \bmod p$$

He/she then sends the value of A, with request to start key exchange session. Mobile User Y can reject the session if he/she is not ready to go through the key exchange session steps. He/she can also accept the request; if so, he/she must calculate the value of B depending on the secretly generated value b and the shared secret parameters g and p and send it back to Mobile User X with accept message.

$$B=g\text{^}b \bmod p$$

Mobile User X will be able to calculate the value of K once he/she receives the value of B from Mobile User Y. Mobile User Y also will be able to calculate same key K, depending on the value of A, which has already been received from Mobile User X in the request message. Thus, Mobile User users X and Y will obtain the same secret key and then, they can use it for one time only to encrypt their public key and exchange it. For next key exchange session, users can use Jk-RSA public keys to encrypt and sign the new cryptographic keys before exchanging them.

To analysis this case, we will focus on the keys exchange between two mobile users, mobile user X and mobile user Y, and the potential risks of intercepting the messages by the attacker mobile user Z. The first message is the request message for the keys exchange. The first message sent from Mobile user X to mobile user Y holds the value of A. Assuming that the attacker mobile user Z manages to capture this message, he/she will be unable to obtain the value of key K by only depending on the value of Mobile User A. The second message is the reply message which is sent from Mobile User Y to Mobile User X. this message is to accept the exchange of keys and it contains the value of

B. Assuming that the attacker Mobile User Z manages to capture this message, he/she will not be able to obtain the value of key K because, the value a is kept secret; this value is only known by user Mobile User X, as well as the value of b which is kept secret by user Mobile User - Y. In addition, the lack of knowledge of Diffie-Hellman algorithm parameters g and p will make the calculation of the key K value impossible. The third and fourth messages are the encrypted messages using the J_k-RSA keys algorithm, which hold the users' public keys. Even if the attacker could capture the messages, he/she will fail to decrypt them and will not know the users' J_k-RSA public keys because of lack of knowledge of the value of key K. Moreover, the attacker Z will fail to start a key exchange session because of lack of knowledge of the Diffie-Hellman parameters and port number; also the solution will reject his request because his contact number is not in the contacts list. Therefore, the user will be confident after the completion of the keys exchange session that the process has been made with the right person. In addition, even if the attacker Z successfully impersonates one of the parties, he/she will fail to complete a successful keys exchange with the other user due to lack of knowledge of the Diffie-Hellman parameters that are needed to complete the process of making agreement on a shred secret key with the other user

The key exchange stage is only a temporary stage needed only in the first contact between the users. Once the key exchange has been successfully accomplished, the next stage will start, which is, exchanging encrypted messages. This stage is permanent and fixed. At this stage, users will be able to send and receive the encrypted and signed messages. They will also be able to exchange new updates for the current keys in encrypted and signed messages. As a result, they will be able to verify the identity of the sender of any message and they can ignore any spurious message. Since the attacker fails to benefit from any of the captured messages during the keys exchange session, in the process of violation of the privacy of any party to the communication, he will not be able to decrypt the captured encrypted messages later. Thus, we can say that the proposed non-server security scheme for mobile communications is capable of providing a high level of security for users. It guarantees provision of the confidentiality, integrity, authentication and nonrepudiation security services.

5. SENDERS AUTHENTICATING

For authentication purpose, both partners' have to sign a messages that they are going to send with their private key. The recipients will be able to verify the signature by using the public key which they already received during key exchange session. Thus, the users will be able to make certain, the identity of the sender within their mobile phones, without need to access the third party severs. If both communicate for the first time, both will require exchanging the keys, using key exchange session. As mentioned earlier, the first time key exchange did not reach the level of challenge and the solution is to create key exchange session with some additional security techniques.

6. CONCLUSIONS

The demand for mobile security has become increasingly important because of the increasing applications, built for mobile phone. Besides on that fact, this paper discussed the impact of implementing public key cryptography on the non-server architecture, in the literature, there were several approaches used to implement public key cryptography. However, none of these approaches used non-server rchitecture. In this paper, public key cryptography implementation for non-server architecture mobile security system has been proposed. J_k-RSA algorithm is selected for public key cryptography implementation. The proposed solution security and the potential risks have been discussed.

REFERENCES

[1]. Ari Juels and Jorge Guajardo, http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/kegver/kv-extended.pdf
[2]. http://www.cryptograf.com
[3]. RSA, http://www.cryptool.org/images/ct1/presentations/RSA/RSA-Flash-en/player.html
[4]. Online RSA example, http://www.gax.nl/wiskundePO/
[5]. Prof. Padmavathamma , "New Variant Cryptosystem based on Jk-RSA Cryptosystem" published in the International Journal of Computer Engineering ,Vol.1 No.2 July-December 2009, pp 145 – 150.
[6]. Prof. Padmavathamma , "New Variant Digital Signature schemes based on Jk-RSA Cryptosystem" published in the International Journal Computation Intelligence Research Application, July-December 2009.
[7].http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange