International Journal of the Physical Sciences Vol. 6(4), pp. 930-938, 18 February, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS10.680
ISSN 1992 - 1950 ©2011 Academic Journals

Full Length Research Paper

Securing peer-to-peer mobile communications using public key cryptography: New security strategy

Sameer Hasan Al-Bakri[1,4], M. L. Mat Kiah[1,4], A. A. Zaidan[2,4], B. B. Zaidan[2,4] and Gazi Mahabubul Alam[3]*

[1]Faculty of Computer Science and Information Technology, University Malaysia, 50603, Kuala Lumpur, Malaysia.
[2]Faculty of Engineering, Multimedia University, 63100, Selangor Darul Ehsan Cyberjaya, Malaysia.
[3] Faculty of Education, University of Malaya, 50603, Kuala Lumpur, Malaysia.
[4]Network and Communication Security Group, ICT and Computational Science Research Cluster, University of Malaya, 50603 Kuala Lumpur, Malaysia.

Accepted 17 January, 2011

Mobile phones are considered to be the most common communication devices in history. Recently, mobile phones are not only used for casual greetings but also, sending and receiving important data such as, 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 (that is, P2P), 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.

Key words: Public key cryptography, NTRU, peer to peer, confidentiality, authentication, integrity and non-repudiation, mobile communication security.

INTRODUCTION

Today, mobile phones are considered to be the most common communication devices in history. The demand for such device is tremendous, as in, the second quarter of 2009, there were more than 4.3 billion mobile subscribers worldwide compared to 3 billion mobile subscribers in 2008 and 2.5 billion mobile subscribers in 2007 (GSMWorld, 2009a). 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.

*Corresponding author. E-mail: gazimalamb@yahoo.com, gazi.alam@um.edu.my. Tel: + 603-7967 5077. Fax: + 603-7967 5010.

Some mobile networks such as GSM networks use different security algorithms called A3, A5 and A8. An A3/A8 algorithm is implemented in the Subscriber Identity Module (SIM) cards and in the GSM network authentication centers. The A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy; the algorithm is implemented in both the handset and the base station subsystem (BSS) (GSMWorld, 2009b).In September 2003, a group of researchers introduced a practical cipher text-only cryptanalysis for GSM encrypted communication, and launched active attacks on the GSM protocols. They describe a cipher text-only attack on A5/2 that merely requires a few dozen milliseconds of encrypted off-the-air cellular conversation to find the correct key in less than a second on a personal computer (Barkan et al., 2008). It is clear that the transmitted data through the mobile networks is unsecured. GSM

networks were not designed to transmit sensitive information. Therefore, security was not considered in its implementation (Zhao et al., 2008). As the amount of products and services offered via the Internet grows rapidly, privacy, copyright and security are very important issues (Abomhara et al., 2010; Ahmed et al., 2010, Alam et al., 2010).

Nowadays, the visibility of security applications is wide (Zaidan et al., 2010g); the term security, presented in the scholar papers, side by side, with terms; confidentiality, integrity, authenticity, non-repudiation, privacy and data protection (Nabi et al., 2010). It may not be exaggerating if we say e-life equal to security, researcher state many words on the role played by security on the life. Raad et al. (2010), Yass et al. (2010), Zaidan et al. (2010a, b, c) say “only protected transaction, have significant impact on consumers’ perception about e-banking security. Zaidan et al. (2010d, e, f), Hmood et al. (2010) said “Privacy and security are very important issues being discussed in the literature, on the current use of ICT”. 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, integrity and non-repudiation security services. The proposed solution is developed and tested on the real mobile phone devices.

Research objectives

The objectives of this research work 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 non-repudiation services.

Research questions

1. What are the current end-to-end mobile communication security solutions weaknesses?
2. How can we develop the end-to-end mobile communication security solution which guarantees the confidentiality, integrity, authentication and non-repudiation security services?
3. How can we provide the end-to-end mobile communication security without depending on mobile network operator or third party?
4. 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?

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 four phases as organized further:

Phase one

1. Current solutions.
2. Public key cryptography in non-server architecture.
3. Non-server architecture versus server architecture.

Phase two

1. Public key cryptography implementation in non-server architecture challenges.
2. Public key generation.
3. Public keys storage.
4. Public key distribution.
5. Senders authenticating.

Phase three

1. Proposed scheme for public key cryptography implementation in Non-server architecture.
2. Selected public key cryptography algorithm.
3. Native Title Research Unit (NTRU) experiment on the real mobile phone device.
4. Authentication problem.
5. Key exchange session.

Phase four

1. Proposed scheme security.
2. Keys exchange session.
3. Exchanging encrypted messages.

CURRENT SOLUTIONS

Many researches have proposed solutions to secure the mobile phone communication by using public key

cryptography (Hassinen and Markovski, 2003; Hassinen, 2006; Kuen, 2008). 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 (Kuen, 2008; Zhao et al., 2008) and key distributions and authenticate the users (Kuen, 2008; Jimale, 2008). 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?

Public key cryptography in non-server architecture

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. 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 messaging software is used to encrypt messages with AES algorithm within the mobile phones without requiring any server (Wu and Tan, 2009).

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 (Hassinen et al., 2006; Jimale, 2008; Wu and Tan, 2009). 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) (Kuen, 2008). As a result, many of the researchers proposed using a server structure for the mobile phone security systems (Jimale, 2008; Kuen, 2008; Toorani and Shiras, 2008). Nevertheless, when the public key cryptography operations are achieved on the mobile phone, it will be possible to implement the public key cryptography in non-server architecture mobile phone security systems. Further, discussions for the public key cryptography operations are achieved by the server.

Public key generation

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 (Jimale, 2008). To overcome this obstacle, the selected algorithm should have a high speed and should not demand high computing ability.

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 (in many cases, exceed 8 giga byte). Furthermore, most of today's phones are designed to deal with extra memory, thus, the storage capacity of the mobile phone is no longer a problem.

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.

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.

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.

Selected public key cryptography algorithm

RSA and elliptic curve cryptosystems (ECC) are considered as the most popular public key cryptography algorithms. In the literature, they reported many weaknesses on RSA, they stated RSA is slow; (Kurosawa et al., 1995) 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 (Yu et al., 2005), because it is hard to implement large integer modular arithmetic on such environments. RSA also requires longer keys in order to be secure compared to some other cryptosystems like elliptic curve cryptosystems (ECC). ECC is faster than RSA (Vincent et al., 2010; Chung et al., 2007), ECC-160 has 6× smaller key-size than RSA-1024 and can generate a signature 12 times faster than RSA (Balitanas et al., 2008). ECC is faster, and occupies less memory space than an equivalent RSA system (Kapoor et al., 2008), ECC generates asymmetry keys pair faster than RSA (Alanazi et al., 2010a, b), ECC is more efficient than the ubiquitous RSA based schemes because ECC utilizes smaller key sizes for equivalent security (Sriram et al., 2010). Security wise, ECC is stronger than RSA (Kute et al., 2009). In 2009, a new standard was approved for public key cryptography called NTRU crypto system. Preliminary experimental results show the advantages of NTRU over RSA, such as, at similar security level, the key size of NTRU is less than a quarter of that of RSA, and the speed of NTRU is much faster than that of RSA; the key generation is more than 200 times faster (Shen et al., 2009). However, when comparing NTRU with RSA and ECC, the speedup is large: up to 1300 times faster than 2048-bit RSA and 117 times faster than ECC NIST-224, when comparing the number of encryptions per second (or up to 1113 times faster than 2048-bit RSA when comparing the data throughput)(Hermans et al., 2010). The computation power required by RSA, ECC and ElGamal is too high for some applications such as smart cards and mobile personal device. These features and more, made NTRU forefront on the mobile environment. NTRU is the first secure public key cryptosystem not based on factorization or discrete logarithm problems (Challa et al., 2007).

The NTRU algorithm was approved by the IEEE in February 2009 as a public key algorithm with standard 1363.1 (NTRUCryptosystem, 2009). Unlike RSA and ECC, no successful attack has been recorded to break the security of this algorithm (Rahma and Hussein, 2009). NTRU provides the same level of security provided by RSA, in addition, the most important advantage of this algorithm is the ability to work in limited computing capability environments. The benefit of using this algorithm in the mobile phone devices is that, it works efficiently and does not have a bad affect on the performance of the mobile phone devices.

In 2009, made an experiment on the performance of enhanced NTRU-251 and compared it with RSA-1024 in the mobile java emulator. The results of their experiment are shown in Table 1. The results that they got show that the time of key generation for NTRU is less 200 times that the time of key generation for RSA, and the time of encryption is almost 3 times less, and the time of

Table 1. Preliminary experimental results (Wu and Tan,2009).

Operation	NTRU-251 (ms)	RSA-1024 (ms)
Key generation	9617	2090509
Encryption	515	1505
Decryption	1132	35102

Table 2. NTRU pair keys generation operation test.

Nokia N70 (ms)	Nokia N73 (ms)	Nokia N93 (ms)	Nokia 5800 Xpress music (ms)
142	77	53	29

decryption is about 30 times less. Thus NTRU is more reasonable for public key cryptography implementation on the mobile phone devices.

NTRU experiment on the real mobile phone device

Unlike the papers reported in the literature, they used java emulator to test the performance of the algorithms; we test NTRU in the real mobile devices. In our experiment, four of Nokia devices, to test the NTRU speed was selected; Nokia N70, N73, N93 and Nokia 5800 Xpress Music. The Nokia N70 belongs to the second generation (2G) of Nokia mobile devices and it operates with symbian operating system v8.1a. It has ARM9 CPU with a 220 MHz clock rate. In addition, it has 22MB internal memory and supports extension memory from MMC type. Nokia N73 is from the third generation (3G) and operates with the developed version of symbian operating system, which is Symbian OS v9.1. This model has Dual ARM 9 CPU with 220 MHz clock rate. N73 has 42 MB internal memory and 2 GB Mini SD, as extended memory. Nokia N93 which belongs to the third generation (3G, has Dual ARM 11 CPU with 332 MHz clock rate. It also operates with the symbian operating system v9.1. This model has 50MB internal memory and 2 GB Mini SD as extended memory. Finally, Nokia 5800 Xpress Music which is the most modern among them, belongs to the fifth generation (5G), and operates with the Symbian OS v9.4. This model has ARM 11 CPU with 434 MHz clock rate. It also has 81MB internal memory with 16GB Mini SD as extended memory (Nokia, 2009).

We performed tests on key generation, encryption and decryption, as well as signing and verifying operations for one hundred times and then calculated the average of time required for each operation. The NTRU key strength is NTRU 251 which is equivalent to RSA 1024. Table 2 shows the key generation operation elapsed time on the real equipment. From the results, we noticed that NTRU algorithm performed very well on the mobile devices and there were no negative effects on the mobile devices' performance due to the small time required for the key generation.

The tests results of NTRU on real equipment such as Nokia N70, N73, N93 and Nokia 5800 Xpress Music showed that the mobile device was able to achieve this operation in less than one second. This is In comparison with one of the best SMS security solutions, (Kuen, 2008) who applied the PKI on the mobile phone environment by using the RSA algorithm. The solution tests were carried out on the mobile phone Nokia N95 (ARM 11 Dual CPU with 332MHz CPU Clock Rate) to generate RSA pair keys with 1024 bit key length. The elapsed time was around eighteen seconds. In our test, we used Nokia N93, which has the same computing ability to Nokia N95, (that is, ARM 11 Dual CPU with 332MHz CPU Clock Rate). But the operation, generating NTRUEncrypt pair keys with length 251, which is equivalent in security level to RSA 1024, is done within 53 ms. This means that, our proposed solution is faster by about 340 times than Kuen's solution.

From the results above, note that NTRU does not require high computing ability, which makes it the best alternatives for mobile devices. Figure 1 shows the proposed public key cryptography implementation in non-server architecture based on NTRU algorithm.

Authentication problem

We proposed to implement public key cryptography on the mobile phone by using NTRU algorithm. With NTRU 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

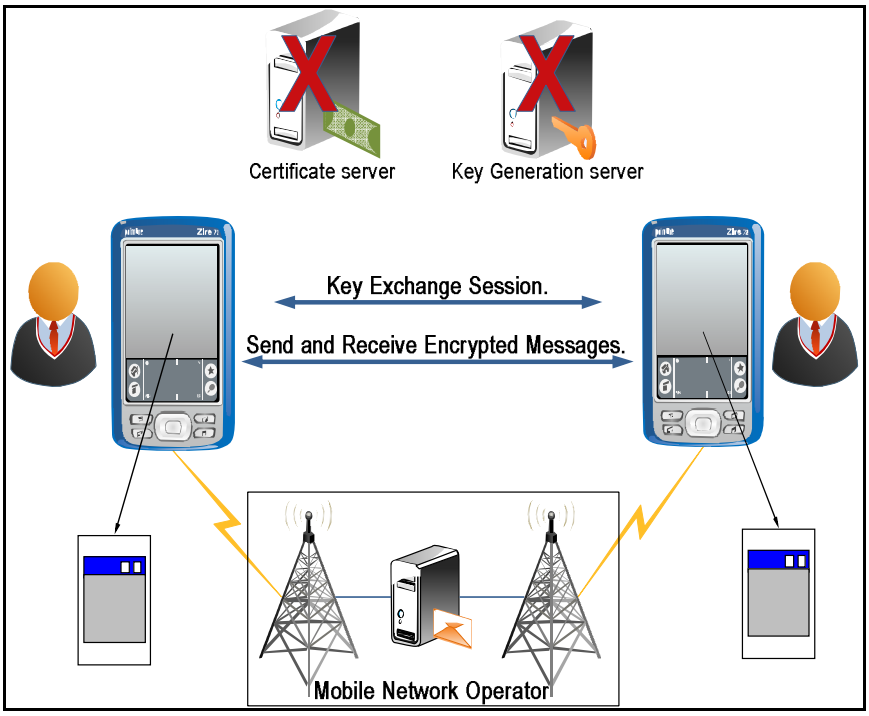

Figure 1. Non-server architecture mobile security system.

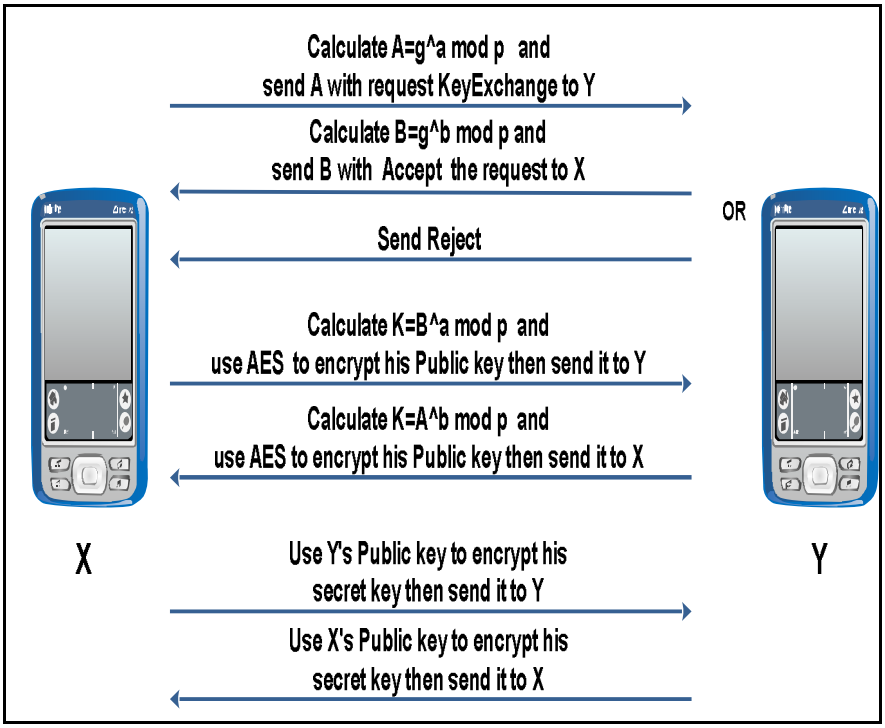

Figure 2. Key exchange session and exchange secret messages.

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 algorithm is used to

make agreement on a temporary key that is used with AES-Rijndael to encrypt the public key and exchange it with the partners.

Key exchange session

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

He/she then sends the value of A, with request to start key exchange session. 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 X with accept message.

B=g^b mod p

User X will be able to calculate the value of K once he/she receives the value of B from user Y. user Y also will be able to calculate same key K, depending on the value of A, which has already been received from user X in the request message. Thus, 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 NTRU public keys to encrypt and sign the new cryptographic keys before exchanging them.

PROPOSED SCHEME SECURITY

Here, we discuss the various stages of the proposed solution and the potential risks, furthermore, discuss will highlight how to protect the users from risks. The proposed scheme has two main stages: the exchange of cryptographic keys and the exchange of encrypted messages, safely.

Keys exchange session

The potential risks lies in assuming that the attacker is able to capture the exchanged messages during the keys exchange session. To analysis this case, we will focus on the keys exchange between two users, X and Y, and the potential risks of intercepting the messages by the attacker Z. The first message is the request message for the keys exchange. The first message sent from X to Y holds the value of A. Assuming that the attacker 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 A. The second message is the reply message which is sent from Y to X. this message is to accept the exchange of keys and it contains the value of B. Assuming that the attacker 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 X, as well as the value of b which is kept secret by 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 key K and AES-Rijndael algorithm, which hold the users' NTRU public keys. Even if the attacker could capture the messages, he/she will fail to decrypt them and will not know the users' NTRU 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.

Exchanging encrypted messages

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 non-repudiation security services.

CONCLUSION

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 architecture. In this paper, public key cryptography implementation for non-server architecture mobile security system has been proposed. NTRU algorithm is selected for public key cryptography implementation. The results for NTRU tests on real equipment have been presented. The proposed solution security and the potential risks have been discussed.

ACKNOWLEDGEMENTS

This research has been funded from University of Malaya under grant number UM.C/625/1. The author would like to acknowledge his supervisor, Dr. Miss Laiha Mat Kiah for her notes and unlimited support. Thanks also go to all contributors in this research, in particular, Prof. Gazi Mahabubul Alam. Special thanks go to the reviewers for their great comments to improve this article.

REFERENCES

Abomhara M, Khalifa OO, Zakaria O, Zaidan AA, Zaidan BB, Alanazi HO (2010). "Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview." J. Appl. Sci., 10(15): 1656-1661.

Ahmed MA, Kiah MLM, Zaidan BB, Zaidan AA (2010). "A Novel Embedding Method to Increase Capacity and Robustness of Low-bit Encoding Audio Steganography Technique Using Noise Gate Software Logic Algorithm." J. Appl. Sci., 10(1): 59-64.

Alam GM, Kiah MLM, Zaidan BB, Zaidan AA, Alanazi HO (2010) "Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study." Sci. Res. Essays, 5(21): 3254-3260.

Alanazi HO, Jalab HA, Alam GM, Zaidan BB, Zaidan AA, (2010a). "Securing Electronic Medical Records Transmissions over Unsecured Communications: An Overview for Better Medical Governance." J. Med. Plants Res., 4(19): 2059-2074.

Alanizi HO, Kiah MLM, Zaidan BB, Zaidan AA, Zaidan Alam GM (2010b). "Secure Topology for Electronic Medical Record Transmissions." Int. J. Pharmacol., 6(6): 954-958.

Barkan E, Biham E, Keller N (2008). Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. J. Cryptol., 21(3): 392-429.

Balitanas M, Robles RJ, Kim N, Kim T, (2009). "Crossed Crypto-scheme in WPA PSK Mode." Proceedings of BLISS 2009, Edinburgh, GB, IEEE CS.

Challa N, Pradhan J (2007). Performance Analysis of Public key Cryptographic Systems RSA and NTRU. IJCSNS Int. J. Comput. Sci. Netw. Security, 7: 87-96.

Chung, YF, Huang KH, Lai F, Chen TS (2007). ID-based digital signature scheme on the elliptic curve cryptosystem. Comput. Standards Interfaces, 29(6): 601-604.

GSM World (2009a). GSM Security Algorithms. Retrieved 2-9-2009, from http://www.gsmworld.com/our-work/programmes-andinitiatives/fraud-and-security/gsm_security_algorithms.htm.

GSM World (2009b). Market Data Summary (Q2 2009). Retrieved 2-9-2009, from http://www.gsmworld.com/newsroom/marketdata/market_data_summary.htm.

Hassinen M, Markovski S (2003). Secure SMS messaging using Quasi group encryption and Java SMS API. In: SPLST'03, Finland.

Hassinen M (2006). Java based Public Key Infrastructure for SMS Messaging. Inf. Commun. Technol., ICTTA'06. 2(1).

Hermans, J, Vercauteren F, Preneel B (2010). Speed records for NTRU. Topics Cryptol., CT-RSA: 73-88.

Hmood AK, Jalab HA, Kasirun ZM, Zaidan AA, Zaidan BB (2010b). "On the accuracy of hiding information metrics: Counterfeit protection for education and important certificates." Int. J. Phys. Sci., 5(7): 1054-1062.

Kapoor V, Sonny V, Abraham Singh R (2008). "Elliptic Curve Cryptography." ACM Ubiquity, 9(20): 20-26.

Kute VB, Paradhi PR., Bamnote GR (2009). A Software Comparison of RSA and ECC. Int. J. Comput. Sci. Appl., 2(1): 43-59.

Kurosawa K, Okada K, Tsujii S (1995). Low exponent attack against elliptic curve RSA. Adv. Cryptol.—Asiacrypt', 95: 376-383.

Nabi MSA, Kiah MLM, Zaidan BB, Zaidan AA, Alam GM (2010). Suitability of SOAP Protocol in Securing Transmissions of EMR Database." Int. J. Pharmacol,, 6(6): 959-964.

Nokia (2009). Device comparison from http://www.forum.nokia.com/Tools_Docs_and_Code/deviceComparison.xhtml?dev=[N70,N93i,N73,5800_XpressMusic]http://www.forum.nokia.com/Tools_Docs_and_Code/deviceComparison.xhtml?dev=%5bN70,N93i,N73,5800_XpressMusic%5d.

NTRUCryptosystems. About us. 2009 18-02-2009 [cited 2009 10-06-2009]; Available from: http://www.ntru.com/about/pr_20090218.htm.

Raad M, Yeasin NM, Alam GM, Zaidan BB, Zaidan AA (2010). "Impact of spam advertisement through email: A study to assess the influence of the anti-spam on the email marketing." Afr. J. Bus. Manage., 4(11): 2362-2367.

Rahma AMS, Hussein QM (2009). A New Attack on NTRU Public Key Cryptosystem Depend on Using Public Key and Public Information.

Shen X, Du Z, Chen R (2009). "Research on NTRU Algorithm for Mobile Java Security Scalable Computing and Communications." Eighth International Conference on Embedded Computing. SCALCOM-EMBEDDEDCOM'09. IEEE Comput. Soc., pp. 366-369.

Sriram VSS, Dinesh S, Sahoo G (2010). Multiplication Based Elliptic Curve Encryption Scheme with Optimized Scalar Multiplication (MECES). Int. J. Comput. Appl., 1(11): 65-69.

Toorani M, Shiras AAB (2008). SSMS - A Secure SMS Messaging Protocol for the M-Payment Systems.

Vincent OR, Folorunso O, Akinde AD (2010). Improving e-payment security using Elliptic Curve Cryptosystem. Electron. Commerce Res., 10(1): 27-41.

Wu S, Tan C (2009). A High Security Framework for SMS. Paper presented at the Biomedical Engineering and Informatics, 2009. BMEI '09. 2nd Int. Conf., pp. 1-6.

Yass AA, Yaseen NM, Alam GM, Zaidan BB, Zaidan AA (2010). "SSME Architecture Design in Reserving Parking Problems in Malaysia." Afr. J. Bus. Manage., 4(18): 3911-3923.

Yu W, He D, Zhu S., (2005). Study on NTRU decryption failures. Inf. Technol. Appl., (2): 454-459.

Zaidan AA, Zaidan BB, Alanazi HO, Gani A, Zakaria O, Alam GM (2010a), "Novel approach for high (secure and rate) data hidden within triplex space for executable file." Sci. Res. Essays, 5(15): 1965–1977.

Zaidan AA, Zaidan BB, Taqa AY, Mustafa KMS, Alam GM, Jalab HA (2010b). "Novel Multi-Cover Steganography Using Remote Sensing Image and General Recursion Neural Cryptosystem." Int. J. Phys. Sci., 5(21): 3254-3260.

Zaidan BB, Zaidan AA, Taqa A, Alam GM, Kiah MLM, Jalab HA (2010c). "StegoMos: A Secure Novel Approach of High Rate Data

Hidden Using Mosaic Image and ANN-BMP Cryptosystem." Int. J. Phys. Sci., 5(11): 1796-1806.
Zaidan AA, Karim H, Ahmed NN, Alam GM, Zaidan BB (2010d). A New Hybrid Module for Skin Detector Using Fuzzy Inference System Structure and Explicit Rules. Int. J. Phys. Sci., 5(13): 2084-2097.
Zaidan AA, Ahmed NN, Karim, H.Abdul, Alam GM, Zaidan BB (2010e) .Increase Reliability for Skin Detector Using Backprobgation Neural Network and Heuristic Rules Based on YCbCr. Sci. Res. Essays, 5(19): 2931–2946.
Zaidan AA, Karim H, Ahmed NN, Alam GM, Zaidan BB (2010f). A Novel Hybrid Module of Skin Detector Using Grouping Histogram Technique for Bayesian Method and Segment Skin Adjacent-Nested Technique for Neural Network. Int. J. Phys. Sci., 5(14) (In press).
Zaidan AA, Ahmed NN, Karim H, Alam GM, Zaidan BB (2010g). "Spam Influence on the Business and Economy: Theoretical and Experimental Study for Textual Anti-spam Filtering Using Mature Document Processing and Naïve Bayesian Classifier." Afr. J. Bus. Manage., 5.
Zhao S, Aggarwal A, Liu S (2008). Building Secure User-to-user Messaging in Mobile Telecommunication Networks. WirelessTelecommun. Symp., WTS 2008: 151-157.