Secure Communication using RSA Algorithm for Network Environment

Amrita Jain
Department of Information Technology
IET DAVV, Indore (M.P), India

Vivek Kapoor, Ph.D
Department of Information Technology
IET DAVV, Indore (M.P), India

ABSTRACT
Secure communication in network environment is primary requirement to access remote resources in a controlled and efficient way. For validation and authentication in e-banking and e-commerce transactions, digital signatures using public key cryptography is extensively employed. To maintain confidentiality, Digital Envelope, which is the combination of the encrypted message and signature with the encrypted symmetric key, is also used. This research paper has proposed to develop a hybrid technique using Symmetric & Asymmetric key cryptography. It will also include Message authentication code to maintain integrity of message. Therefore, proposed model will not only help to maintain confidentiality and authentication of message and user but integrity of data too. Java technology has been proposed to validate the performance of proposed model in context of message length, key length, cipher text length and computational time for encryption and decryption.

Keywords
Hybrid Secure Communication, RSA, MAC, Symmetric Key.

1. INTRODUCTION
In the current era significant computing applications have emerged in recent years to simultaneously connect millions of users to share content, form social groups and communicate with their contacts. Network Environment is the key soul such applications. To maintain security in such applications, Security mechanisms usually involve more than a particular algorithm or protocol for encryption & decryption purpose and as well as for generation of sub keys to be mapped to plain text to generate cipher text. It means that participants be in possession of some secret information (Key), which can be used for protecting data from unauthorized users. Thus basic purpose of this model is too developed within which security services and mechanisms can be viewed. The main purpose of this project is to provide an efficient way to user send or receive message over a secured channel.

To maintain confidentiality and integrity of content is primary focus of proposed model. This model integrate RSA algorithm along with Diffie Hellman Key Exchange Algorithm.

There are various security algorithms are available but still they have scope of improvement. For Example RSA encryption can only provide confidentiality not integrity of content. Authentication can be achieved but on the cost of big key exchange overhead. The complete study concludes to develop a security mechanism consisting confidentiality, authentication and integrity on single platform

2. LITERATURE SURVEY
A method of encryption that combines two or more encryption schemes and includes a combination of symmetric and asymmetric encryption to take advantage of the strengths of each type of encryption is known as Hybrid Encryption.

RSA is a cryptosystem for public-key encryption, and is widely used for securing sensitive data, particularly when being sent over an insecure network such as the Internet.

RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Public-key cryptography, also known as asymmetric cryptography, uses two different but mathematically linked keys, one public and one private. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This attribute is one reason why RSA has become the most widely used asymmetric algorithm. It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage.

RSA derives its security from the difficulty of factoring large integers that are the product of two large numbers Multiplying these two numbers is easy, but determining the original prime numbers from the total -- factoring -- is considered infeasible due to the time it would take even using today's super computers.

The public and the private key-generation algorithm is the most complex part of RSA cryptography. Two large prime numbers, p and q, are generated using the Rabin-Miller primarily test algorithm. A modulus n is calculated by multiplying p and q. This number is used by both the public and private keys and provides the link between them. Its length, usually expressed in bits, is called the key length. The public key consists of the modulus n, and a public exponent, e, which is normally set at 65537, as it's a prime number that is not too large. The e figure doesn't have to be a secretly selected prime number as the public key is shared with everyone. The private key consists of the modulus n and the private exponent d, which is calculated using the Extended Euclidean algorithm to find the multiplicative inverse with respect to the totient of n. Considering arithmetic modulo n, let's say that e is an integer that is co prime to the totient φ(n) of n. Further, say that d is the multiplicative inverse of e modulo φ (n). These definitions of the various symbols are listed below for convenience:

n = a modulus for modular arithmetic

φ (n) = the totient of n

e = an integer that is relatively prime to φ(n)

[T his guarantees that e will possess a multiplicative inverse modulo φ(n)]

d = an integer that is the multiplicative inverse of e modulo φ(n)

The computational steps for key generation are

1. Generate two different primes' p and q

2. Calculate the modulus $n = p \times q$

3. Calculate the totient $\varphi(n) = (p - 1) \times (q - 1)$

4. Select for public exponent an integer e such that $1 < e < \varphi(n)$ and $\gcd(\varphi(n), e) = 1$

5. Calculate for the private exponent a value for d such that

$d = e^{-1} \bmod \varphi(n)$

6. Public Key = [e, n]

7. Private Key = [d, n]

Furthermore, The Diffie–Hellman key exchange algorithm solves the following dilemma. Alice and Bob want to share a secret key for use in a symmetric cipher, but their only means of communication is insecure. Every piece of information that they exchange is observed by their adversary Eve. How is it possible for Alice and Bob to share a key without making it available to Eve? At first glance it appears that Alice and Bob face an impossible task. It was a brilliant insight of Diffie and Hellman that the difficulty of the discrete logarithm problem for F∗ p provides a possible solution.

3. PROBLEM STATEMENT

The major problem with existing cryptographic scenario is, can't achieve authentication and confidentiality along with integrity in single step. In PKI encryption and decryption perform with different key where private key is non-sharable entity. As per the Asymmetric Key Cryptography if we encrypt the message with private key, anyone can decrypt the message by using its public key. Here, we can achieve authentication but cannot maintain the confidentiality. Furthermore, if wee encrypt the message by public key, only intended recipient can decrypt the message. It helps to maintain the confidentiality but cannot authorize sender. To overcome the above problem we use to perform public key encryption after private key. So, only intended receiver would be able to decrypt the message and also authentic the sender by decrypting the received cipher message with public key.

Subsequently, there is a procedure to maintain authentication and confidentiality by implementation digital envelop for communication.

A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication.

A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.

Rivest, Shamir and Adleman (RSA) Public-Key Cryptography Standard (PKCS) #7 governs the application of cryptography to data for digital envelopes and digital signatures.

A digital envelope uses two layers for encryption: Secret (symmetric) key and public key encryption. Secret key encryption is used for message encoding and decoding.

Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication.

Either of the following methods may be used to create a digital envelope:

- Secret key encryption algorithms, such as Rijndael or Twofish, for message encryption.
- Public key encryption algorithm from RSA for secret key encryption with a receiver's public key.

A digital envelope may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data. An example of a digital envelope is Pretty Good Privacy (PGP)

popular data cryptography software that also provides cryptographic privacy and data communication authentication. A digital envelope is also known as a digital wrapper

4. PROPOSED APPROACH

The proposed solutions will not only give a way to establish secure communication but it will also help to improve level of encryption by reducing security overhead. System does not required any external system interface for development. A block represeantation of proposed solution is shown in figure 1 and 2.

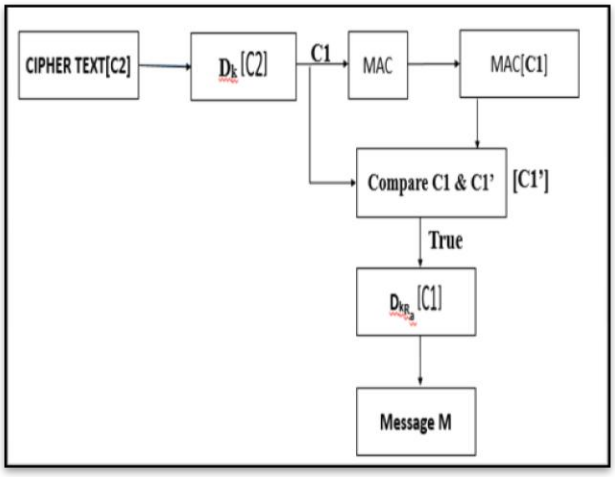

Figure 1: Encryption Process

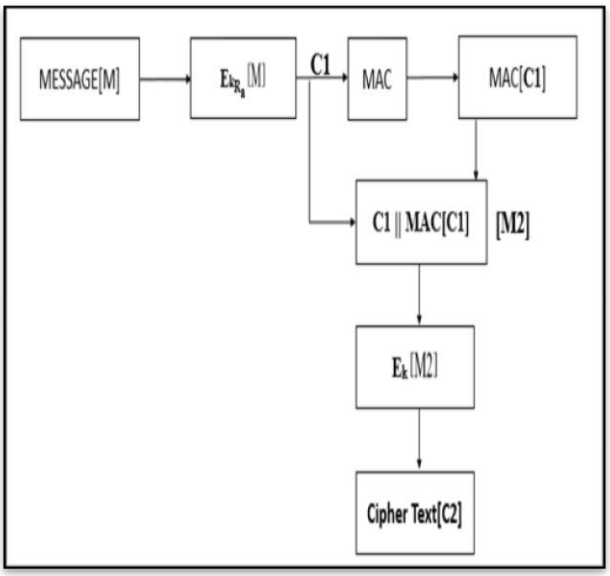

Figure 2: Decryption Process

Expected Outcomes

The complete study explores the block representation of encryption and decryption process. Proposed work can be implement using java technology to estimate the performance of security mechanism

In order to develop proposed solution following assumptions will be consider for performance evaluation and secure message transmission

1. Maximum data block size for encryption = 128bit / 256bit / 512 bit

2. Maximum Key size for RSA = 128 bit

3. Maximum Key size for Diffie Hellman = 64bit

4. Maximum Key size for MAC = 36bit

It is observe that, variation in message size may be reason for variation in security overhead.

There is need to evaluate performance on multiple message sample on following parameters.

1. Encryption Time for RSA

2. Decryption Time for RSA

3. Encryption Time using Symmetric Key Algorithm

4. Decryption Time using Symmetric Key Algorithm

5.Total time consume in complete encryption and MAC padding

6.Total time consume in complete decryption with MAC verification

7. Total size increase of encrypted packet

8. Total size increase of decrypted

5. CONCLUSION

This work is used to analyse the existing problem of accurate network situation awareness in real time. The size of information generated by any monitoring tool is very large and hence required complex processing. Fusion of this information is used to derive a decision for vulnerability detection. In this work a novel ICARFAD based assessment mechanism is proposed for improved detection of security situations and taking timely response. It consist of three phase; information collection, assessment and response and feedback. All the data passes through a repository to hold the decisions.

Pattern is also extracted for better measurement of situations. This work uses various metrics to calculate the correct behaviour of the system. At the initial level of this work approach seems to provide effective results in near future.

6. FUTURE WORK

Some problems and concepts that remain unaddressed can be performed in future. Such as with the help of pre-emptive approach more information can be added for exact timely analysis of network situations & its successful assessment with high accuracy. It can also be used for quantitative & qualitative analysis etc.

7. ACKNOWLEDGMENTS

The authors wish to acknowledge SDBCT administration for their support & motivation during this research. The authors would also like to thank anonymous referees for their many helpful comments, which have strengthened the paper. They also like to give thanks to Mrs. Vandana Kate & Dr. Suresh Jain for discussion regarding the intrusion systems & for producing the approach adapted for this paper.

8. REFERENCES

[1] Rongrong Xi, Shuyuan Jin, Xiaochun Yun and Yongzheng Zhang, "CNSSA: A Comprehensive Network Security Situation Awareness System", in International Joint Conference of IEEE TrustCom, ISSN: 978-0-7695-4600-1/11, doi: 10.1109/TrustCom.2011.62, 2011.

[2] Wang, C. Yao, A. Singhal and S. Jajodia, "Network Security Analysis Using Attack Graphs :Interactive Analysis of Attack Graphs using Relational Queries", in proceedings of IFIP WG Working Conference on Data and Application Security (DBSEC), 11.3 pages 119-132, 2006.

[3] Mr. Marc Grégoire and Mr. Luc Beaudoin, "Visualisation for Network Situational Awareness in Computer Network Defence", in proceedings of visualisation and the common operational picture meeting RTO-MP-IST-043, Paper 20. 2008.

[4] White Paper on, "Public Safety and Homeland Security Situational Awareness", in ESRI, February 2008.

[5] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, "Cyber SA: Situational Awareness", in Cyber Defense University of Wisconsin, 2009.

[6] Rostyslav Barabanov, Stewart Kowalski and Louise Yngström, "Information Security Metrics", DSV Report series No 11-007, Mar 25, 2011

[7] Pallavi Vaidya and S. K. Shinde, "Application for Network Security Situation Awareness", in International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012), IJCA, ISSN: 0975 – 8887, 2012.

[8] Xiu-Zhen Chena, Qing-Hua Zhenga, Xiao-Hong Guana,b, Chen-Guang Lina, Jie Sun, "Multiple behavior information fusion based quantitative threat evaluation", in Elsevier Journal of Computers & Security , ISSN: 0167-4048 ,doi:10.1016/j.cose.2004.08.009,2005. pp 218-231

[9] Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia, "An Attack Graph-Based Probabilistic Security Metric", in National Institute of Standards and Technology Computer Security Division; Concordia Institute for Information Systems Engineering, Montreal, Canada.

[10] Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, and Laurie Graffo, "Security Metrics Guide for Information Technology Systems", in NIST Special Publication 800-55, July 2003.

[11] William Streilein, Kendra Kratkiewicz, Michael Sikorski, Keith Piwowarski, Seth Webster, "PANEMOTO: Network Visualization of Security Situational Awareness through Passive Analysis", in

Workshop on Information Assurance United States Military Academy, Proceedings of the IEEE, 2007.

[12] Rongzhen FAN, Mingkuai ZHOU, "Network Security Awareness and Tracking Method by GT", in Journal of Computational Information Systems, Binary Information Press, ISSN: 1043-1050, Vol. 9: Issue 3, 2013.

[13] Igor Kotenko and Andrew Chechulim, "Attack Modelling and Security Evaluation in SIEM System", in International Transaction of System Science and Application, SIWN Press,, ISSN:2051-5642, Vol. 8, Dec 2012.

[14] Bon K. Sy, "Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive IDS", in Elsevier Journal of Information Fusion, ISSN: 1566-2535, doi:10.1016/j.inffus.2009.01.001, 2009.

[15] Timothy Shimeall, Sidney Faber, Markus DeShon and Andrew Kompanek, "Using SiLK for Network Traffic Analysis", in CERT R Network Situational Awareness Group, Carnegie Mellon University. September 2010.

[16] William Yurcik, "Visualizing NetFlows for Security at Line Speed: The SIFT Tool Suite", in 19th Large Installation System Administration Conference (LISA '05), 2005.

[17] Xiaoxin Yin, William Yurcik and Michael Treaster, "VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness", in ACM, doi: 1-58113-974-8/04/0010, Oct 2004.

[18] Xiaoxin Yin, William Yurcik and Adam Slagell, "The Design of VisFlowConnect-IP: a Link Analysis System for IP Security", in National Center for Advanced Secure Systems Research (NCASSR), 2010.

[19] Ji-Bao Lai, Hui-Qiang Wang, Xiao-Wu Liu and Ying Liang, "WNN-Based Network Security Situation Quantitative Prediction Method and Its Optimization", in Journal of computer science and technology, Vol. 23, Issue 3, ISSN: 0222:0230, Mar 2008.

[20] SunJun Liu, Le Yu and Jin Yang, "Research on Network Security Situation Awareness Technology based on AIS", in International Journal of Knowledge and Language Processing, ISSN: 2191-2734, Volume 2, Number 2, April 2011.

[21] P. Mell and K. Scarfone, "Improving the Common Vulnerability Scoring System", in proceedings of IET Information Security, doi:10.1049/iet-ifs:20060055, 2007.