A Survey on Key Exchange Mechanism Using Mobile Agent

Shalini Parashar[1], Dr. Dinesh Kumar[2]
[1]*Shri Ram College of Engineering & Management, Palwal*
[2]*Department: Computer Science & Technology, SRCEM Palwal*

***Abstract*- The spectacular growth of the Internet has spawned an increased awareness of an interest in security issues. Although security has been considered in the design of the basic Internet protocols, many applications have been and are being designed with minimal attention paid to issues of confidentiality, authentication, and privacy. Often cryptographic algorithms and protocols are necessary to keep a system secure, particularly when communicating through an untrusted network such as the Internet. Where possible, use cryptographic techniques to authenticate information and keep the information private (but don't assume that simple encryption automatically authenticates as well). Generally you'll need to use a suite of available tools to secure your application. Cryptographic protocols and algorithms are difficult to get right, so do not create your own. Instead, where you can, use protocols and algorithms that are widely-used, heavily analyzed, and accepted as secure. When you must create anything, give the approach wide public review and make sure that professional security analysts examine it for problems. In particular, do not create your own encryption algorithms unless you are an expert in cryptology. Key exchanges any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. This paper's objective is to study proposed key exchange protocols for mobile environment. Mobile agent is a software object that migrates through many nodes of a heterogeneous network of computers under its own control in order to perform task using resources of these nodes, during the past several years; mobile agent has received significant attention. In this paper, we compare the computational efficiency of various authentication protocols and implement RSA using mobile agents.**

***Index Terms*- Key Exchange, Cryptography, RSA algorithm, Mobile agent, AGLET.**

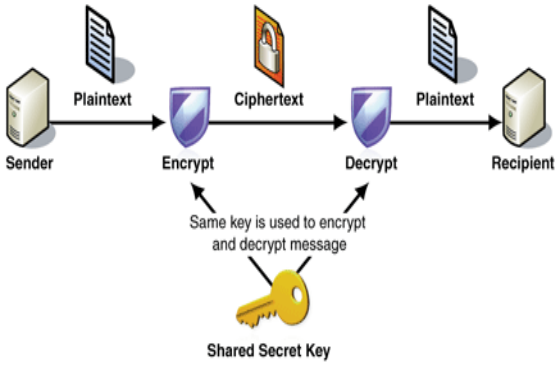
I. INTRODUCTION

Key exchange is a technique in cryptography by which the secret keys are exchanged between senders and receivers for the purposes of encryption and decryption of messages respectively. RSA is used to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm because one of them can be given to other. Mobile agents are agents that can physically travel across networks and perform tasks on machines that provide agent hosting capability. A software agent is a program that can halt itself, ship itself to another computer on the network, and continue execution at the new computer. The key feature of this kind of software agent is that both its code and state are mobile. Agents are autonomous because once you start them; they decide where they will go and what they will do. This allows processes to migrate from computer to computer, for processes to split into multiple instances that execute on different machines, and to return to their point of origin. We have found that mobile agents reduce network traffic, provide an effective means of overcoming network latency, and perhaps most importantly, through their ability to operate asynchronously and autonomously of the process that created them, help us to construct more robust and fault tolerant systems.

II. CRYPTOGRAPHY

Cryptography is almost referred to Encryption, which is the process of converting the PLAINTEXT into the CIPHERTEXT.

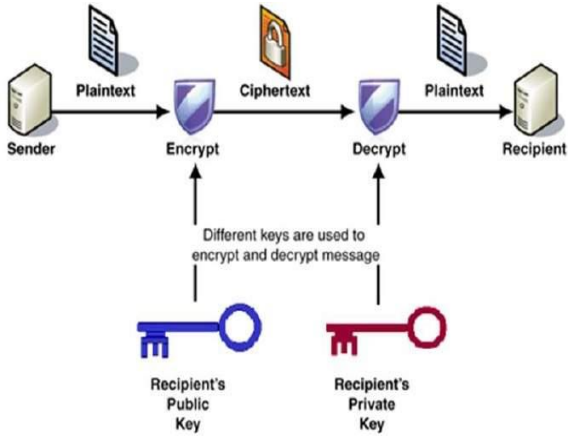
TYPES OF CRYPTOGRAPHY
SYMMETRIC KEY CRYPTOGRAPHY



In a Symmetric key cryptography, the sender and receiver of a message share a single or a common key which is used to encrypt and decrypt the message. A Secret Key Algorithm are also called symmetric Algorithm.

It uses the same key to encrypt and decrypt data. The most popular Symmetric key system is the DATA ENCRYPTION STANDARD (DES)

ASYMMETRIC KEY CRYPTOGRAPHY



Asymmetric key cryptography also called Public key cryptography. Asymmetric key Cryptography uses Public and Private Keys to Encrypt and Decrypt data. These keys are interchangeable, in the sense if Key A Encrypts a message, then the Key B can Decrypt it, and if Key B Encrypt a message, then the Key A can Decrypt Key B.

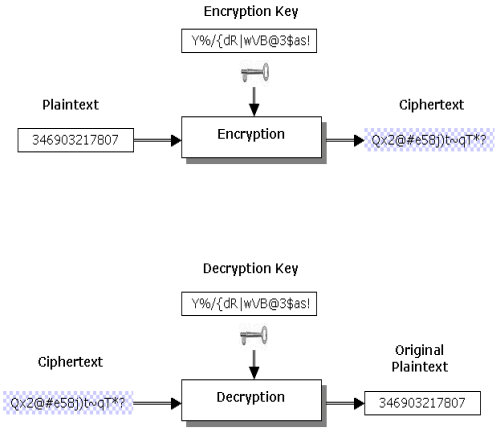
DATA ENCRYPTION AND DATA DECRYPTION

DATA ENCRYPTION

Data Encryption is the process of converting the Plaintext or any other type of data into a encoded form, that is only decoded by the decryption key.

DATA DECRYPTION

Data Decryption is the process of Converting the encoded data into the plaintext data or in the original data.



III. What Is RSA?

RSA (Rivest–Shamir–Adleman) is one of the first practical public-key cryptosystems and is widely used for secure data transmission. In such a cryptosystem, the encryption key is public and it is different from the decryption key which is kept secret (private). In RSA, this asymmetry is based on the practical difficulty of the factorization of the product of two large prime numbers, the "factoring problem".

The acronym RSA is made of the initial letters of the surnames of Ron Rivest, Adi Shamir, and Leonard Adleman, who first publicly described the algorithm in 1978. Clifford Cocs an English mathematician working for the British intelligence agency Government Communications Headquarters (GCHQ), had developed an equivalent system in 1973, but this was not declassified until 1997. A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value.

The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, and if the public key is large enough, only someone with knowledge of the prime numbers can decode the message feasibly. Breaking RSA encryption is known as the RSA problem. Whether it is as difficult as the factoring problem remains an open question.

RSA is a relatively slow algorithm, and because of this, it is less commonly used to directly encrypt user

data. More often, RSA passes encrypted shared keys for symmetric key cryptography which in turn can perform bulk encryption-decryption operations at much higher speed.

Steps for the algorithm in RSA

Each user generates a public/private key pair by:

1. Selecting two large primes at random - p, q
2. Computing their system modulus N=p.q
   - note ø(N)=(p-1)(q-1)
3. Selecting at random the encryption key where $1<e<ø(N)$, $gcd(e,ø(N))=1$
4. Solve following equation to find decryption key d $e.d=1 \bmod ø(N)$ and $0 \le d \le N$
5. Publish their public encryption key: KU={e,N}keep secret private decryption key: KR={d,p,q}

EXAMPLE: Select primes: p=17 & q=11

6. Compute $n = p*q = 17 \times 11 = 187$
7. Compute $ø(n)=(p-1)(q-1)=16 \times 10=160$
8. Select e : gcd(e,160)=1; choose e=7
9. Determine d: $de=1 \bmod 160$ and $d < 160$ Value is d=23 since $23 \times 7=161= 10 \times 160+1$
10. Publish public key KU={7,187}
11. Keep secret private key KR={23,17,11}
12. Sample RSA encryption/decryption is:
13. Given message M = 88 (nb. 88<187)
14. Encryption: $C = 88^7 \bmod 187 = 11$
15. Decryption: $M = 11^{23} \bmod 187 = 88$

RSA Key Exchange

Algorithm using mobile agents here we are trying to implement RSA, with the help of mobile agent as mobile agents are not using so far and there is problem in RSA that if any interrupt occur on the path of key exchange the rsa hault its processing. So by using mobile agents we are trying to overcome from this problem so that ,RSA will be able to appropriate action according to the problem in its working environment .Then it need no help operation from user .

IV. MOBILE AGENT

Mobile agents are the basis of the emerging technology which makes it easier to design, implement and maintain distributed systems mobile agents have the unique ability to transport themselves from one system in a network to another. We found that mobile agents reduce network traffic, overcome network latency and most importantly their ability to operate asynchronously and autonomously. Each of the machines should have ASDK; the agent execution environment preinstalled which provides efficient mobile agent development and execution environment. In the execution environment an agent can hide its code and data integrity and also its owner identification. The aglet model allows the proper and easier use of the agents created. The aglet model helps in setting up proper infrastructure through which we can use and take advantage of the agents.

Basic Elements:

- Aglet
- Context
- Identifier
- Creation
- Cloning
- Dispatching
- Retraction
- Activation and Deactivation Disposal

V. PROBLEM IDENTIFICATION

Several issues are identified on most of the currents approaches. The algorithm takes too much time as infinite exponentiation factoring is used in RSA. The algorithm either reveals the secret data or not strong enough for off-line attacks, server spoofing attacks, replay attacks. Normally, Breaking RSA Encryption is called as the RSA Problem.RSA is a Slow Algorithm, because of this; RSA is less used to encrypt user data.

Need of mobile Agent in RSA Optimization

RSA is a slow method as compared to other data transmission.

In RSA the security factor is also required; these two points are the use of Mobile Agent came in existence.

In Computer Science, a Mobile Agent is a Composition of software and also data which is able to move from one computer to another computer autonomously and it continue its execution on the destination computer.

The key Feature of mobile agent is that it code and state both are mobile.

VI. CONCLUSION

The use of Mobile Agents appears to offer certain advantages for client-server computing but as we've noted in the above systems, it also raises some difficult issues with respect to efficiency, flexibility and security. We will be easily able to find a good or a better and efficient way of key exchange keys Five Basic steps between the client and the server will be optimized. Exchange keys using the mobile agent's implementation. These issues have an effect on an agent's ability of mobility. Many important issues such as how agents determine the available resources/services on a machine it transferred to, mobile agent system-to-OS interaction, the use of persistent storage, and support for failure were either briefly discussed. Mobile agent based approach have not been used so far to a great extent.

VII. ACKNOWLEDGEMENT

I would like to express my gratitude to my HOD "Dr. Dinesh Chaudhary" for his support, guidance and helps throughout this research .The Research on "KEY EXCHANGE MECHANISM USING MOBILE AGENT" has been given to me as part of curriculum in two years master's degree in computer science & engineering. I have tried my best to present this information as clearly as possible using the basic terms. I will fail my duty if I don't acknowledge esteemed scholarly guidance, assistance and knowledge.

REFERENCES

[1] [The possibility of Non-Secret digital encryption J. H. Ellis, January 1970.
[2] Non-Secret Encryption Using a Finite Field MJ Williamson, January 21, 1974.
[3] Thoughts on Cheaper Non-Secret Encryption MJ Williamson, August 10, 1976.
[4] New Directions in Cryptography W. Diffie and M.
[5] E. Hellman, IEEE Transactions on Information Theory, vol. IT-22, Nov. 1976, pp: 644–654.
[6] https://en.wikipedia.org/wiki/