IMPLEMENTATION OF METHODS FOR TRANSACTION IN SECURE ONLINE BANKING

Kashif Ruman, Dr H.D. Phaneendra
P.G Student: I.S.E Dept., Professor.,CS&E Dept.,
National Institute of Engineering,
Mysore, India.
Kruman364@gmail.com, hdphanee@yahoo.com

***ABSTRACT*- Security is a concept similar to being cautious or alert against any danger. Network security is the condition of being protected against any danger or loss. Thus safety plays a important role in bank transactions where disclosure of any data results in big loss. We can define networking as the combination of two or more computers for the purpose of resource sharing. Resources here include files, database, emails etc. It is the protection of these resources from unauthorized users that brought the development of network security. It is a measure incorporated to protect data during their transmission and also to ensure the transmitted is protected and authentic.**

Security of online bank transactions here has been improved by increasing the number of bits while establishing the SSL connection as well as in RSA asymmetric key encryption along with SHA1 used for digital signature to authenticate the user.

Keywords—Network Security, Digital signature, RSA, Security Attacks, Encryption, Certificate.

I. INTRODUCTION

Network can been defined as any set of interlinking lines resembling a network of roads parallel and interconnected system, also computer network can be simply defined as a system of interconnected computers. Security can be defined as the need to protect one or more aspects of network‘s operation and its permitted use for e.g. accessing, checking behavior, performance, having privacy and confidentiality. Network Security requirements can be Local or Global accordingly to their scope, depending upon the networks or purpose of design and deployment. The important aspect in judging security solutions include ability to meet the specified things, computing resources needed, quality, sustainability and economic considerations.

Security Attacks compromises the data security. Active attacks can be defined as active attempts made to alter the data on security leading to modification, redirection, or destruction of data, systems or links. Another type of attack is Passive attacks which involve simply getting access to link of device and obtain data. Security threats can be defined as the threats that have the potential for violating security rules. Security Mechanism is a mechanism that detects/ locates/ identifies/prevents/ recovers from various security attacks. We should have a Security Service that improves security and makes use of the security mechanisms.

The Internet is an integral part of our daily routines, and the proportion of people who expect to be able to manage their banking accounts anywhere, anytime is constantly increasing. So due to this enormous growth of online transactions Internet banking has become a very crucial and important component of any financial institution‘s strategy. Information about financial institutions, their users, and their fund transactions is, by necessity, extremely sensitive. So the Internet banking system should have provision to solve the issues related to authentication and non-repudiation, so that only authorized people can access an Internet banking account, and the information viewed must remain private and it should not be modified by others. For confidentiality and integrity, we have Secure Sockets Layer which has been defined as the defacto Internet banking standard, and for authentication and non-repudiation, no good scheme has become predominant yet.

II. LITERATURE SURVEY

Networking can be defined as the creating a group of acquaintances and associates and keeping it active through regular communication for mutual benefit. We can simply say that networking relies on the question "How can I help?" and not with "What can lI achieve from it?" .It provides the protection of the resources from unknown users, which brought the development of network security.

It can be said as procedure put in place to protect data during their transmission and also to ensure the transmitted is protected and authentic. A threat can be defined in many ways such as gaining access to the network by an unauthorized party, to better understand the various types of threats to security; the definition of security requirement is inevitable.

A. Cryptography and different Types of Security Algorithms

Cryptography can be defined as science of writing in secret code. Between the contexts of any process to process communication, involves some of the specific security requirements like:

- Authentication: It is the process of finding the identity of the user who is genuine and has access to resources.
- Confidentiality: Ensuring that no other is able to access the data except the authorized user
- Integrity: Assuring the reception that the message obtained has not been changed or tampered in any circumstances from the original.
- Non-repudiation: A process to prove that the sender/receiver has really sent/received this message.

There are several different ways of classifying cryptographic techniques. The algorithms can be majorly classified in 3 ways:

- Secret Key Cryptography (SKC): In this type of algorithm it uses a common key for encryption and decryption at the sender and receiver end respectively.
- Public Key Cryptography (PKC): In this type of algorithm it uses different key for encryption and another key for decryption at the sender and receiver end respectively.
- Hash Functions: In this type of algorithm uses a mathematical transformation techniques to irreversibly "encrypt" the data.

B. *Digital Signature Using RSA*

In the RSA algorithm for digital signature process, we have the private key that is used to encrypt only the plain text. Then encrypted message becomes the digital signature and is attached to the original data contained.

C. *Security Attacks*

Security attacks on network can be classified in terms of passive and active attacks. In case of passive attack it access the information from the system, but doesn‘t harm the information or resource in the system. An active attack on the other side will make changes in the system and diverts the ongoing operation.

A **passive attack** is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The main aim is to gain information about the target and no data is changed on the target.

An **active attack**, hacker is attempting to break into the system. During the attack, the intruder will introduce data into the system as well as potentially change data within the system.

D. *SHA (Secured Hash Algorithm)*

SHA the is cryptographic hash function. The different algorithms of SHA are *SHA 0*, *SHA 1*, *SHA 2*, and *SHA 3*. Here SHA-0 is the original version of the 160-bit hash function under the name "SHA", SHA-1 can be termed as, it is very much similar to SHA-0, but changes has been incorporated where it alters the original SHA hash specification to overcome its drawbacks, and SHA-2 was published in 2001, and this algorithm is very much different from the SHA-1 hash function.

The most widely used algorithm is SHA-1 compared to all other existing SHA hash functions, and is employed in several widely used applications and protocols.

III. SYSTEM REQUIREMENTS AND SPECIFICATION

It provides a description of the various factors that affect the system and its requirements.

A. *System Perspective*

The secure system is aimed towards providing a service to users to trust servers before any request can made, and various methods have been implemented to detect fake servers and alert users about such systems and carry out communication in a secure manner.

B. *System Function*

The primary function of the system is to issue a certificate first to registered servers based on some credentials (like IP address, port number, kind of service being offered by server etc.) For obtaining this, the server has to interact with CA (Certificate Authority). Here the assumption is that CA is legitimate and fully trusted. User requests server for a certificate before trusting it and later verifies it for its authentication. In case of fake certificate detected, it is immediately reported to CA.

C. *Functional Requirements*

Functional requirements are those that refer to the functionality of the system. That is, what services it will provide to the client. Nonfunctional or supplementary requirements pertain to other information needed to produce the correct system and are detailed separately.

- ➢ User has to request Server for Certificate and Public Key of CA after registration with server
- ➢ User has to request Server for Certificate and Public Key of CA after registration with server.
- ➢ User tries to detect whether Server or CA communicating with it is fake.
- ➢ User communicates with Server or CA in highly secured manner.
- ➢ Server provides a service to Users to do online secure transactions.

IV. SYSTEM ANALYSIS

The task of system analysis is to identify limitations of the existing system and to establish in detail what the proposed system will do. The main aim of the system analysis phase is the specification of what the system needs to do to meet the requirements of end users.

A. *Existing System*

The main aim of secure socket layer is to provide security between server and client, which includes the confidentiality that is the data should be kept secret, provide message integrity means the message should not be altered, and authentication where only authorized user have provision to access the data. SSL obtains these type of security by using encryption, digital signatures and certificates.

The sensitive and confidential information such as pin number, social security numbers, and other important credentials are protected by using cryptography. Confidential data is encrypted with various different mechanisms across public networks to obtain the confidentiality if not an unauthorized user will able to obtain all the necessary data that is being sent between a server and a client they can see and use that information. Here the SSL protocol obtain the details of the encryption for network as it will be able to track where the data is being transmitted. The existing system uses SSL communication with 128 bits & RSA Encryption with 1024 bits maximum.

Drawbacks of the existing system

1. Lesser the number of bits, more vulnerable to attack
2. Susceptible to collision attack

B. *Proposed System*

The project system architecture is shown below. Client interacts with server and gets required service. Certificate authority issues certificate to the server. The server‘s certificate will be later verified by the client before any transaction is being done and by the certificate authority upon requisition by the client.

Features

1. SSL communication with 256 bits
2. RSA encryption with 2048 bits (this improvement in RSA provides more security to personal data)

In this paper, as the result of analysis of existing system unique secret key extraction from the received request based on the inspiration of RSS in base paper is made possible. Once the key obtained is unique and different private communication secured for maximum by defeating the intention of the intruder in knowing the secret key.

V. SYSTEM DESIGN

This gives overall flow of the project and algorithm used in the design.So in this phase Implementation can be said as a stage in software development where the software design is realized. The objects that are identified in the design stage are implemented, and a function which manipulates these objects is realized.

A. Structure Chart

Here the project is divided into three modules and sub-modules of each module are shown in the Fig 1.

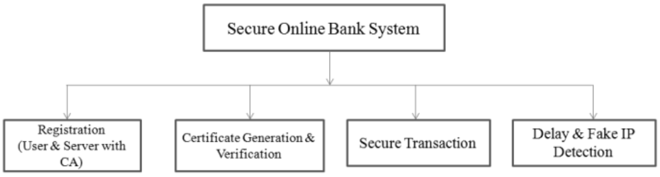
Secure Online Bank System
Registration (User & Server with CA)
Certificate Generation & Verification
Secure Transaction
Delay & Fake IP Detection

Fig 1 Structure chart

Registration Module: User should be registered with the bank server and bank server should register with the Certificate Authority before requesting for any kind of service.

Certificate Generation and Verification: User and Certificate Authority verifies the certificate (i.e. whether the that the given certificate is genuine or fake)

Secure Transaction: Here we carry out the transaction that is secure communication between the entities.

Delay & Fake IP: To detect whether Server / CA is legitimate or fake, detection of delay being introduced during transmission due to fake node(s) in the network.

B. Sequence Diagram

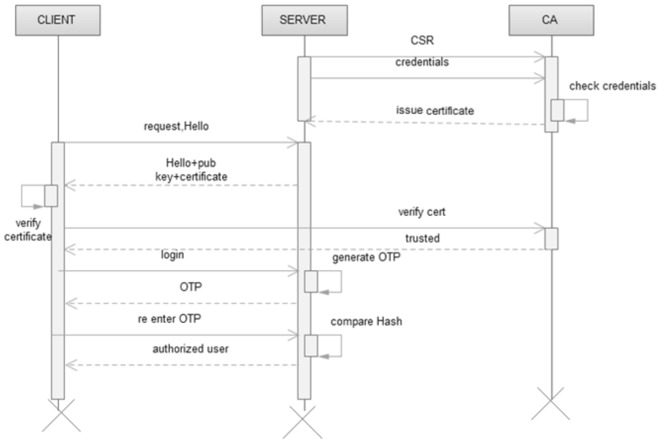

Fig 2.Sequence diagram

As shown in the above fig 2, server first gets the certificate from the server. Client sends a hello packet to the server and server in turn sends the public key and certificate issued by CA. Client verifies certificate with the help of CA before trusting the server. When it is completely sure that server is not fake, client proceeds to carry out a transaction in a secure manner.

VI. CONCLUSION AND FUTURE ENHANCEMENTS

A. Conclusion

In this paper we analyzed various security threats for computer networking, various loop holes of present networking. These threats overcame by various methodologies for securing the network through cryptography and encryption. Effort was made to find out the security aspect of Networking and it was overcome by means of Cryptography and Encryption by using improved RSA algorithm and also increased number of bits in SSL connection.

Even though key generation time is more compared to that of present situation, security can be guaranteed which is more important than key generation time in the current scenario.

B. Future Enhancements

Presently, the system will support two rounds of certificate. In future it can be increased. The various types of attacks can be detected in future. Different methods can be adopted as a measure of security attack.

Greater level of security can be provided by using multiple encryption, following multiple levels for an authentication or by strengthening the encryption key by increasing the number of bits.

REFERENCES

[1]. Christos K. Dimitriadis, ‖Analyzing the Security of Internet Banking Authentication Mechanisms‖2007 ISACA

[2]. S.R. Subramanya and byung K. YI ‖Digital signatures‖, IEEE March/April 2006.

[3]. Weeks, Stephen. Understanding Trust Management Systems. IEEE Symposium on Security andPrivacy. 2001.

[4]. O. Dandash, Internet banking payment protocol with fraud prevention, 2007 22nd International International Symposium on Computer and Information Sciences.

[5]. YAHALOM, R.; Trust Relationships in Secure Systems-A Distributed Authentication Perspective. Washington, DC 1993.

[6]. Data Hiding and Retrieval, A.Chakrabarti, Proceedings of IEEE International conference on Computer Intelligence and Computer Network held at Bhopal from 26-28 Nov, 2010.

[7]. Neal Koblitz ―A Course in Number Theory and Cryptography‖ Second Edition Published by Springer-Verlag.

[8]. T Morkel, JHP Eloff ― ENCRYPTION TECHNIQUES: A TIMELINE APPROACH‖ published in Information and Computer Security Architecture (ICSA) Research Group proceeding.

[9]. By Klaus Felten ―An Algorithm for Symmetric Cryptography with a wide range of scalability‖ published by 2nd International Workshop on Embedded Systems and Industial IT.

[10]. Vyshali Rao K P, Adesh N D , A V Srikantan, Client Authorization and Secure Communication in Online Bank Transactions

[11]. Majdi Al-qdah & Lin Yi Hui―Simple Encryption/Decryption Application in International Journal of Computer Science and Security, Volume (1) : Issue (1).