International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 - 5161

Available at http://inpressco.com/category/ijcet

Research Article

Carapace for Intranet Security of Data Communication Layer

Premchand Ambhore[Á*], B B Meshramr[B] and Archana Wankhade[Ć]

[Á]Computer Science and Engineering , Amravati University, Amravati, India
[B]Computer Engineering Department, VJTI Mumbai, India
[Ć]Information Technology Government College of Engg.Amravati (M.S.) India

Accepted 15 Nov 2014, Available online 01 Dec 2014, **Vol.4, No.6 (Dec 2014)**

Abstract

Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity. All modern cryptographic system are based on Kirchhoff's principle of having a publicly known algorithm and a private or secret key. Many cryptographic algorithms use complex transformations involving substitutions and permutations to transform the plain text into cipher text. However, if quantum cryptography can be made practical, the use of one pads may provide truly unbreakable cryptosystems. Cryptographic algorithms can be divided into symmetric key algorithms and public key algorithms. Symmetric key algorithms mangle the bits in a series of rounds parameterized by the key to turn the plaintext into cipher text. The main public key algorithm is RSA, public key algorithms. Commonly messages to be signed are hashed using algorithms such as MD-5 and SHA-1 and then hashes are signed rather than original messages. Including some that use a trusted third party, Diffie-Hellman, Keberos and Public-Key cryptography. Digital data transmission raises many issues in which technology interacts strongly with public policy. Some of the areas include privacy, freedom of speech and copy right. Thus we have seen the basic reasons and requirements to provide data transmission security and its importance. The data transmission security can be achieved by using combination of RSA, AES, and SHA-1 algorithms. This eliminates the threats to the data transmission security. Voice data, image and text data from Host A to Host B is sent securely.

Keywords: *security, cryptography, protocols, algorithms.*

1. Introduction

The requirements of the information security within an organization have undergone two major changes in the last several decades. Before the widespread use of data processing equipment, the security of information felt valuable to an organization was provided primarily by introduction of the computer, the need for the automated tools for protecting files and other information stored in the computer became evident. This is especially the case for shared system, such as time-sharing system, and the need is even more acute for a system that can be accessed over public telephone network, data network, or the Internet. The generic name for the collection of tools designed to protect the data and to thwart hackers is computer security. The second major change that affected security is the introduction of the distributed systems and the use of networks and communication facilities for carrying data between terminal user and computer and between computers and computer. Network security measures are needed to protect data during their transmission. Our focus is on the Data transmission security, which consists of measures to prevent, detect security violations that involve in the transmission of data. Before analyzing a project lets get briefly introduced to object oriented analysis. Starting from a statement of the problem, the analyst builds a model of the real world situation showing its important properties. The analyst must work with the requestor to understand the problem because problem statements are rarely complete or correct. The analysis model is a concise, precise abstraction of what the desired system must do, not how it will be done. The objects in the model should be application domain concepts and not computer implementation concepts such as data structures. Record shows that most of the attacks are not perpetrated by outsiders but by insiders with a grudge.

1.2 Previous Work: After invent of notion of symmetric and asymmetric cryptographic algorithms there has been a tremendous amount of work in the field of secure data transmission through various networks. Some of them are stated below **IBM Secret-Key Management Protocol:** In the late 1970's IBM developed a complete key management system for communications and file security on a computer network, using only symmetric cryptography. By automating the generation, distribution, installation, storage, changing and distribution of keys, the protocol went a long way to ensure the security of the underlying ciphers. This protocol provides three things:

*Corresponding author **Premchand Ambhore** is a Research Scholar; **B B Meshramr** is working as Professor and **Archana Wankhade** as Assiatant Professor

secure communications between a server and server terminals, secure file storage at the server and secure communications among servers. At both the server and the terminal, all encryption and decryption takes place within the cryptographic facility available on each machine. **MITRENET:** One of the earliest implementations of public key cryptography was the experimental system MEMO (MITRE Encrypted Mail Office).MEMO was a secure electronic mail system for users in the MITRENET network, using public key cryptography for key exchange and DES for file and message encryption **ISDN:** Bell-Northern Research developed a prototype secure Integrated Services Digital Network(ISDN) telephone terminal. The resulting product was the Product Data Security Overlay. **Kerberos:** Kerberos is the third party authentication protocol designed for TCP/IP networks. A Kerberos service sitting on the network acts as a trusted arbitrator. Kerberos provides secure network authentication, allowing a person to access different machines on the network. Kerberos is based on symmetric cryptography. **Kryptoknight:** Kryptoknight is an authentication and key distribution system designed by IBM. It is a secret key protocol and uses either DES or a modified version of hash function MD5. It supports four security services: user authentication, two party authentication, key distribution, authentication of data origin and content. **Smart Cards:** A smart card is a plastic card, the size and shape of a credit card, with an embedded computer chip. A smart card contains a small computer, RAM and ROM. Smart cards can have different cryptographic protocols and algorithms programmed into them. They might be configured as an electronic purse, and be able to spend and receive digital cash. They may be able to perform zero knowledge authentication protocols.

*1.3. Statement of the Problem***:** The problems associated with the communication between the two Computers that has been taking place over last few decades

Normal Flow: User A is able to communicate with the user B without any interruption in the flow of the data that has been transmitted by the user A to user B or by the user B to user A. **Interruption:** User A transmits the message to B, the message contains some instructions that B should immediately follow. User C, who is not supposed to read the file, is able to monitor and interrupt the communication so that he can capture the copy of the message.

Interception: User A transmits a message to a computer B, the message instructs computer B to update an authorization file to include the identities of a number of new users who are to be given access to a computer. User C intercepts the message to B as shown in the diagram. Only difference between this type of the threat is that user B will receive the message.

Modification: User C, rather than intercepting the message constructs its own message with the desired entries and then transmits the message to b as if it had come from user A. Computer B accepts the message as coming from A and update the authorization file accordingly.

Fabrication: User C, who is not part of the developed network can, constructs his own message and can, transmits the message to computer B, as if it has been sent by the user A.

2. Literature Survey

To excel in any new domain, one needs a strong foundation. For this simple reason, the project work was started with literature survey to get a feel of the new field being worked on. The survey focused on data transmission security in particular and various security transformation algorithms in general. Data transmission security is becoming evident these days. For developing the security system one needs to understand the previous system as employed for secure data transmission. Hence previous system was also studied. The issues and challenges faced by data transmission were looked upon. What could be possible solution for them was also studied. After getting idea of the domain we started the literature survey of the basic tool of data transmission security namely Cryptography, Digital signatures and Hash functions. The following sections present the study done on the above mentioned topics.

2.1 Cryptography: The science of secrecy - is the process of keeping the message secure to hide its content so that valuable or sensitive information can be protected from unauthorized use. Its purpose is to ensure security and privacy by keeping the information hidden from anyone for whom it is not intended. Encryption and decryption are the key features of cryptography. Historically four groups of people have used and contributed to the art of cryptography. The military, the diplomatic corps, lovers and diarists. Of these, the military have had the most important role and have shaped the nature of the field. The messages to be encrypted, known as the plain text, are transformed by a function that is parameterized by a key. The output of the encryption process, known as the cipher text or cryptogram is then transmitted .We assume that the enemy, or intruder, hears and accurately copies down the complete cipher text. However unlike the intended recipient he does not know what the key is and so cannot decrypt the cipher text easily. The art of breaking ciphers is called Cryptanalysis. The art of devising ciphers (cryptography) and breaking them (cryptanalysis) is collectively known as Cryptology. The fundamental rule is that one must assume that the cryptanalyst knows the general method of encryption used. In other words, the cryptanalyst knows how the encryption method works .There are various cryptographic protocols to ensure that a message is really from the sender and not an impostor, this is called Authentication. A digital signature binds a document to the possessor of a particular key, while a digital timestamp binds a document to its creation at a particular time**.** Integrity is also an important aspect of cryptography .It ensures that the message has not been modified during transmission or storage.

2.2. Encryption & Decryption: Encryption is a secure and trusted method for keeping your sensitive information private. It is a process by bits of data is mathematically scrambled with a password-key. Encryption transforms the data so that it is unreadable until it is decrypted.

Encryption is a Greek word meaning to hide. It is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption. it is the transformation of encrypted data back into some intelligible form. Encryption and decryption require the use of some secret information, usually referred to as a password-key. Encryption works by mathematically scrambling your data files using an algorithm.

Plaintext → **Encryption** → Cipher Text → **Decryption** → Plaintext

Plaintext is denoted by M, for message. It can be stream of bits, a text file, and a bitmap, a digital video image… whatever. As far as computer concerned M is simply binary data. Cipher text is denoted by C, it is also binary data: sometimes the same size as of M or may be larger. The encryption function E operates on M to produce C. In
E (M) = C b
In the reverse process the decryption function D operates on C to produce M:
D (C) = M
Since the whole point of encrypting and decrypting a message is to recover the original Plaintext, the following identity must hold true:
D (E (M)) = M
Depending on the way the key is used to encrypt the data the encypherment can be divided into three categories: Symmetric key cryptography, In this type of cryptography the message is encrypted and decrypted by the same key, or shared key which both the parties involved in the communication.

Public key cryptography, In this type of cryptography the requester encrypts the message using first key while addressee decrypts the cipher using the second key.
The first key is called Public Key while the second key is called Private key. This keys in pairs so that what one key encrypts the other can decrypt.

Digital signature: In this, message is encrypted with private key and decrypted with public key; this is used in digital signatures which serve the purpose of authentication.

2.3 Algorithms & Keys

A cryptographic algorithm, also called a cipher, is the mathematical function used for encryption and decryption. If the security of the algorithm is based on keeping the algorithm works a secret, it is called as restricted algorithm, which is used for low security applications. Modern cryptography solves this problem with a key, denoted by K. This key might be any of the large number of values. The range of possible values of the key is called key space. Both the encryption & decryption operations use this key. Thus we have
E_k (M) = C
D_k (C) = M
Thus
D_k (E_k (M)) = M
Some algorithms use different encryption (K1) and decryption key (K2). In this case:
E_{k1} (M) = C
D_{k2} (C) = M
Thus
D_{k2} (E_{k1} (M)) = M
All of the security in these algorithms is based in the key ; none is based in the details of the algorithm. This is called as Kirchhoff's principle.

3. Implementation

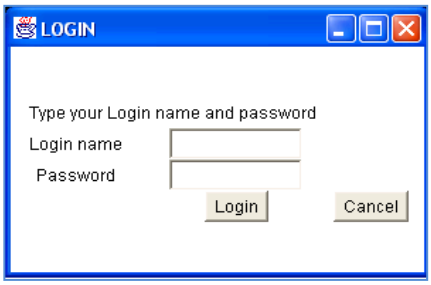
3.1 Modules: The modules used in the project are
RSA: The RSA class is used to implement the public-key cipher. It is used to provide the digital signature. The sender signs the document using his private key while the receiver verifies the signature using the sender's public key.
SHA: The SHA class is used to calculate the 160-bit hash value and append it to the message. The signed message is processed, the hash value for the signed message is calculated and is appended to the signed message. At the receiving host the hash value is separated from the signed message. The hash value is calculated again for the separated signed message. This hash value is compared with the hash value sent. If they match then the process of decryption proceeds forward. AES: The AES class is used to implement the symmetric-key cipher. The sender signs the message and appends the calculated hash value. Then the message with rthe hash value is encrypted using the symmetric-key. At the receiver the received message is decrypted using the symmetric-key. Sender: The sender class is used to input the symmetric, public and private key of the user. The different types of message like text, voice and image to be sent are prepared. Then the message is encrypted using the objects of RSA, AES and SHA classes. The encrypted message is then sent in datagram packets using the UDP protocol. Receive: The receive class is used to receive and decrypt the messages. The message is received in the form of fragmented UDP packets. The packets are reassembled to form the complete message. The message is decrypted using the objects of AES, SHA and RSA classes. Login: The login class is used to take the login name and password of the client who wishes to communicate. The login name and password are verified. If the password is found correct then the communication proceeds by creating objects of the Send and Receive classes.

3.2 Input-Output Screen Design

The screen shots are used to provide the user interface to the program. The screen shots used in the project are

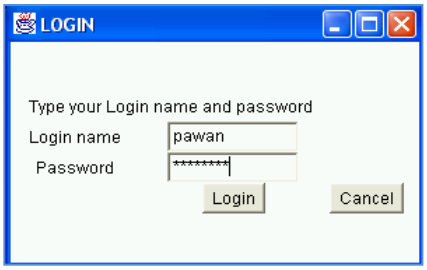
3.2.1 Login screen

The screen-1 shows screenshot of the Data Transmission System For Multimedia Database when it is launched. The screen displays an intuitive interface. The text boxes in front of "Login name" and "Password" are used for inputting the client name and his password. The buttons in the screenshot are self-explanatory.



Screen – 1 Initial Login screen

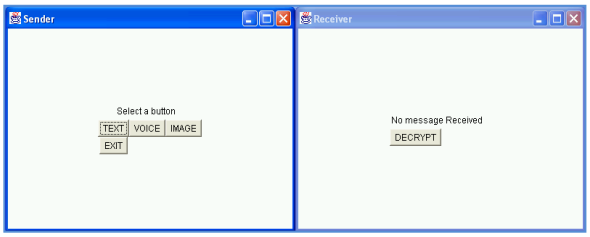
"Login" is used to read the client-name and password and search in the available client-names and passwords for a match.
"Cancel" is used to exit from the system.



Screen – 2 Final login screen

The screen-2 shows the input given by the user for Login

3.2.2 Sender & Receiver Screen



Screen – 5 System idle

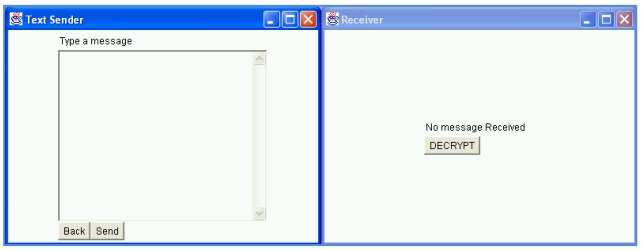
The screen-5 shows the screenshot after entering the keys and pressing the "Next" button. As we can see there are two windows open,
Sender: For encrypting and sending the message. It contains four buttons

TEXT: To form and transmit the text message.
VOICE: To record and transmit the voice message.
IMAGE: To form and transmit an image.
EXIT: To exit from the "Sender" system.

Receiver: For decrypting and receiving the message. It contains only one button and a message. It shows the state of "Receiver". Depending upon the type of message received a proper message is displayed. To read the message "DECRYPT " button has to be pressed.

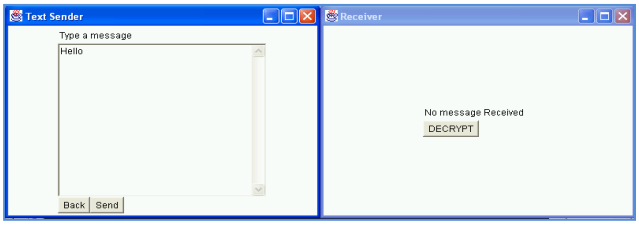
3.2.3 Text Message Screen

This screen-6 shows the screenshot for sending a text message. It is displayed after the "TEXT" button is pressed. There are two buttons



Screen – 6 Entering text message

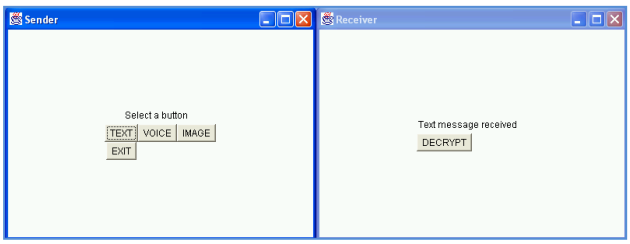
Back: To go back to the main "Sender" window.
Send: To send the encrypted message.



Screen – 7 Text message entered to encrypt

The screen-7 shows the message typed by the user in the text box available. To send the text message typed user has to press the "Send" button. After the SEND button is pressed the following output is generated at the command prompt.

Encrypting the message using RSA...
2893 1113 1795 1795 2237
Message signed using RSA.
Hash Value...
981214339 2039929060 -1763421218 -1778665578 1315017456
size:64
Encrypting File using aes...
189 173 49 204 33 137 89 199 104 204 229 60 233 230 158 124
189 173 120 39 53 137 154 171 104 204 198 208 233 230 29 62
189 1 73 125 65 33 42 154 74 104 204 198 195 122 230 124 62
172 157 27 120 12 225 149 205 249 19 242 123 211 202 135 245
Message encrypted using AES.
size of sent file 64 bytes
file sent successfully

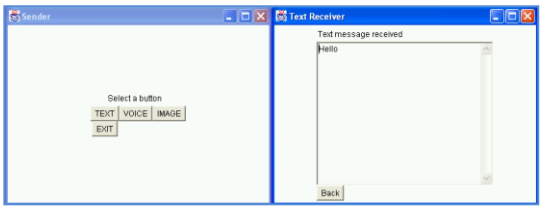


Screen – 8 Encrypted Text-Message received

The screen-8 shows the screen displayed after the text message is received. The text message can be read by

pressing the "DECRYPT" button. After the DECRYPT button is pressed the following output is generated at the command prompt.

Decrypting File using aes...
0 0 11 77 0 0 4 89 0 0 7 3 0 0 7 3
0 0 8 189 128 0 0 0 0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0 0 0 0 160 58 124 36 131
121 150 216 228 150 228 83 222 149 251 183 150 78 97 146 240
Message decrypted using AES.
Hash value sent with message is...
981214339 2039929060 -1763421218 -1778665578 1315017456
New Calculated Hash Value...
981214339 2039929060 -1763421218 -1778665578 1315017456
Data Integrity Verified
Decrypting the message using RSA...
104 101 108 108 111
Message decrypted using RSA



Screen – 9 Decrypted the text message

The screen-9 shows the screenshot after the "DECRYPT" button is pressed. To get back to the "Receiver "window user has to press the "Back" button.

Conclusion & future research directions

The journey through this project work has been a tremendous learning experience. It gave an exposure to a new domain "Data transmission security". It introduced us to fantastic development platform of security. The entire project can be summarized as follows. Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity. Cryptographic systems are based on Kirchhoff's principle of having a publicly known algorithm and a private or secret key. Many cryptographic algorithms use complex transformations involving substitutions and permutations to transform the plain text into cipher text. However, if quantum cryptography can be made practical, the use of one pads may provide truly unbreakable cryptosystems.

Future Scope

Our system is using AES with 128 bits key for actual encryption of the data, this provides the security which is even not provided by 3-DES which is a more widely used algorithm in industries. Highest securities can be achieved using AES with 256 bits key. RSA with 64-bits keys is used to reduce complexity but currently RSA with 512-bits keys are more common & RSA with 1024 bits keys is likely to replace it. SHA-1 has withstood for many years and is likely to stand for coming few years. New versions of SHA-1 are under development for hashes of 256, 384 and 512 bits respectively .Future of cryptography will all focus on strengthening the above mentioned algorithms and thereby developing a solid system.

References

William Stalling Cryptography and Network Security Principles and Practices Third Edition Pearson Education
Bruce Schneier (1996) Applied Cryptography Second Edition John Wiley's
Tanenbaum (2002) Computer Networks Fourth Edition PHI
James Rambaugh Object Modeling and Design
Naughton, Schildt The complete reference Java 2,3rd ed. Tata McGraw-Hill Publishing company ltd.
www.parallab.uib.no,
www.aip.de ,
www.fags.org/faqs/cryptography-faq/,
www.cbbrowne.com/info,
www.cs.georgetown.edu/~denning
www.gnu.org/sw/guide.ref/
www.rsasecurity.com
www.cro.net:8040
www.pajhome.org.uk
slis-two.lis.fsu.edu/~security