Implementation of Routing Protocol for Network and Data Security using Onion Routing with Salt Method

Sweta Tiwari[1], Deepak Arora[2], Vineet Singh[3]

[1]Student, Dept. of Computer Science
ASET, Amity University
Lucknow, India
Swetatiwari21@gmail.com

[2]Faculty, Dept. of Computer Science
ASET,Amity University
Lucknow,India
Deepakarorainbox@gmail.com

[3]Faculty, Dept. of Computer Science
ASET,Amity University
Lucknow,India
Vineet.singh85@gmail.com

Abstract: Electronic communication is becoming an important issue now’s day. Hiding the details of communication, content, nodes from the adversaries like an eavesdropper, hacker etc is usually not considering before. Encryption is becoming the most important part of all the communication channels. Onion routing is an anonymous connection that can provide support anonymous mail as well as other applications. The nodes include in the network cannot be always trusted, since a valid node may be captured by enemies and becomes malicious. Onion routing with salt is the secure network topology that help to protect the data and the network after the enemy captures the node path. Onion routing with salt make the network more secure and data more protected.To create this and provide main aim of onion routing its uses public key encryption with salting method to put multiple layer of encryption around the original data thus making an onion like structure and each layer between source to destination peel off each layer of encryption.

Index Terms: Onion, Salt, Encryption, Security TOR

I. Introduction

Onion routing was initiated by Sun Solaris with implementation for web browsing, remote login process and sanitizing the user information from the browser while transmitting information through data packets. Onion routing promises to protect the integrity and confidentiality of data from the theft, eve dropping over the network and internet, onion routing proceed a devised a technique to limit the knowledge of information as possible while high level of anonymity is achievable. Onion routing have ability to work against the traffic analysis attack mainly because of there is no direct communication between sender and receiver. As it initiates a communication with an application specific router called onion routing proxy that was enough to manage TCP and Sock request of the client.

Routing onion is a data structure designed by wrapping a plain text message with the successive layer of encryption such that each layer can be unwrapped by an one intermediary and no other can decrypt it. Onion routing is implemented with the help of encryption in the application layer of network in the communication stack like the layer of an onion. Tor help in encryption of original data including the IP address and send to the destination through a virtual circuit comprising successive, randomly selected. Each relay decrypts the layer of encryption to obtain only the successive relay in order to transmit the data. The final relay decrypts the innermost layer of encryption and sends the original data to its final destination without revealing and hiding the information of sender

TOR is the descendant of the onion routing project work by the project had many concept in it. TOR is a collection of onion routers which may have different functionality and roles in the network and during the network communication they perform their roles. Each router send an information in a secure way to next hop in the TOR network connection whereby if any single nodes is compromised then this been will be not affected anonymity as well as data communication send to and from the sender and receiver is work properly.

TOR main aim is to hide the communication between the initiator and the target host fir which the initiator needs to communicate with the nodes [3]. The Tor network is an network in which each onion router runs as a normal and perform their usual duties without having any special type of privileges. A TLS connection is maintain for every other onion router. Each user can fetch their directories and establish circuit across the network and handle difficulties in handling connection from user application. Each router in the Tor maintain a long term identity key and short term identity key that is use to sign as TLS certification

Salt is not only a single hash function, it is all about using more than one hash function among more the one hash function. Salt is the process of selecting a unique hash function from many hash function that are also known to server. Salt is also be added to make it more difficult from an attacker to break in a system by using password hash matching strategies because adding salt to a password hash prevent an attacker from testing known dictionary words across the entire system. Salt can also be added to make it more difficult for an attacker to break into a system by using password hash-matching strategies because adding salt to a password hash prevents an attacker from testing known dictionary words across the entire system.

Hash = (salt + password)

Verifier = salt + hash (salt + password)

Diffie Hellman Exchange - It is protocol that help to maintain data integrity by exchanging a secret key between two users. Two users may be one is server and one client.

II. Problem Statement

This portion of paper discuss the problem involves in onion. The first problem is Longstanding Connection that means If the longstanding connection between two nodes of onion router in the network is broken down so it will may result in many destruction of messages one for each anonymous connection that was suppose thorough that longstanding connection . Second problem is Expensive i.e. Onion message packets are in the sequences of cells that must be processed together. This onion processing involves a public key operation which is relatively very expensive in all other cryptographic. The third problem is Data Latency its means that delay in data. Data latency is also the main problem in the onion routing protocol. Message has been transmitted to may circuit and latency may be happen sometimes.

Eve dropping is the forth problem that means an attacker can start monitoring the system when an onion router incoming queues and outgoing queues are empty so that attacker can determine the order in which marker arrives at a onion router Traffic Cost is also include in the problem. Traffic analysis to be cost of brute force attack on the cryptographic algorithms un reasonable [4]. Compromised nodes can cooperate to uncover the rout information to the outsider that was the main problem .Accessing a remote onion router does not really provide a protected anonymous environment because connection between the machine and onion router is not protected.

.

III. Related work

A paper is published by Uma Somani, Kanika Lakhani and Manish Mundra in Cloud discussion of that we have problem like security of data, files system, host security etc[1].They have proposed a concept of digital signature with RSA algorithm, to encrypt the data while transferring it over the network. This technique solves the dual problem of authentication and security. The strength of their work is the framework proposed to address security and privacy issue.

Anonymous Connection and onion routing by paul and david specify of onion routing system, vulnerability analysis based on specific and performance result.

G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom proposed to generate RSA Public keys and Private Keys for public and private access to overcome the problem of data security. Certificate Binary file is used inside control node configuration file to make sure cloud data flow securely. The control node sends data through Secure Socket Layer after certificate activation. Finally AES algorithm is used for encryption .This unique combination makes this solution best to prevent different types of attacks.

Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments by Wei Liu, Member proposed that the route request packets are authenticated by a group signature, to defend against potential active attacks without unveiling the node identities. The key encrypted onion routing with a route secret verification message is designed to prevent intermediate nodes from inferring a real destination.

Onion Routing for Resistance to Traffic Analysis by Paul Syverson proposed that using encryption on a packet-switched network can hide the content of messages, much like placing the messages inside a physical envelope. However, by itself encryption does not hide who is talking to whom, and how often. Onion Routing is a general purpose infrastructure for private communication over a widely shared network such as the internet or the SIPRNET.

IV. Proposed work

All this process is implemented to provide security in avoiding data modification at the end of server side. For the same purpose two different servers are made and maintained one for storage server for storing user data file and second is for rehashing user password.

When a user want to transmit a file to the server of the onion networks firstly key are exchange using our first process diffie Hellman key exchange process at the time of login [2]. Finally user's data file is encrypted using cryptographic algorithm with salt and only then it is going to be transmitted on network.

Steps 1:

Picks nodes from a list of nodes-the chosen nodes are ordered to provide a path that forming a circuit through which the message may be transmitted.

Step 2

Using asymmetries key cryptography with salt, entry node uses public key to sends the encrypted message creating a cell calls create cell.

1-An create cell have-

2-The originator's half a diffie Hellman handshake

3-A circuit id

Diffie Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel.

This shared could be a password or a big number or an array of randomly chosen bits.

Step 3:

1-The entry node which just received the handshake, replies to the originators with:

2-The entry nodes' half of the handshake

3-A hash of the shared secret

Step 4:

The originator and the entry node use their shared secret for encrypting everything

Step 5:

1-The originator send s the entry node relay-extend cell for the next nodes using public key with

2-The originator's half of the differ Hellman handshake, a circuit id, a request

Step 6:

-The relay nodes then replies to the handshake

Step 7:
-Similarly the chain is extended further.

V. Implemenation

All this process is implemented to provide security in avoiding data modification at the end of server side. For the same purpose two different servers are made and maintained one for storage server for storing user data file and second is for rehashing user password.

I: Implementing the encryption algorithms with salt.
II: Connection Establishment.
III: Data transfer

The first step starts with implementation onion routing encryption algorithms adding salt in it. There are many different algorithms are used for connection establishment and data transferring. RSA algorithm is used for establishing connection. It is the standard public key cryptography algorithm and cipher text are not easily decrypted, because the process of decryption is not an inverse process of encryption.. Random prime numbers are generated for encryption and decryption. Using system time onion key is generated. While sending the onion keys are generated that made difficult to predict the keys.

TCP socket connection is used for connection. For anonymous communication and private is to be performing first. So the path that is to be followed by the sender and receiver and the address of the proxies through they pass during connection.

The first layer of onion decrypted at its intermediated proxy and appropriate details such keys, IP address and the function for decrypting the data that will be build into routing table.

As connection is established over the network and data start passing through it in encrypted form of the onion[5]. finally the data is sent to receiver send by the sender by encrypting at each level of intermediate proxies and finally it decrypted at the initiating proxy and serves as plain text the sender.

A. *Execution Steps*:

1. Start Connection
2. Data Encryption with salt
3. Key Exchange – Diffie Hellman
4. Network communication using ToR
5. Files Transferred to router
6. Connection End.

.

VI. Conclusion

Data security become the most important part in the network building.We shloud need to create such netwrk that provide security in avoiding data mdification and eve dropping in the network.Onion routing with salt make the network more secure and data more protected.To create and provide main aim of onion routing its uses public key encryption with salting method to put multiple layer of encryption around the original data thus making an onion like structure and each layer between source to destination peel off each layer of encryption. As the data reached t the destination it is fully secured as only next router can get address of previous node. So node will ever know the full path of onion.

References

[1] Uma Somani, Kanika Lakhani, Manish Mundra “Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

[2] G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom proposed to generate RSA Public keys and Private Keys for public and private access, 2009.

[3] Wei Liu: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments” , IEEE Transaction on vehicular technology,Vol.63,no.9,November 2014.

[4] Onion Routing for Resistance to Traffic Analysis by Paul Syverson, 2003, IEEE

[5] K. Kaviya” Network Security Implementation by Onion Routing” 2009 International Conference on Information and Multimedia Technology.

[6] Michael Backes,”Provably Secure and Practical Onion Routing”, 2012 IEEE 25th Computer Security Foundations Symposium