International Journal of Trend in Research and Development, Volume 3(2), ISSN: 2394-9333
www.ijtrd.com

Quantum Key Distribution

[1]S.Divya Bharathi and [2]R.Ranjani,
[1]Student, [2]Assistant Professor, Information Technology Department,
Sri Krishna Arts and Science College, Coimbatore, TamilNadu, India

Abstract: *The key generation problem in the two-way relay channel, in which there is no direct channel between the key generating distributions. We propose an effective key generation scheme that achieves a substantially keys than direct channel. Unlike existing schemes, there is no need for the key generating terminals to obtain. Secure key distribution schemes establish communication between a group manager and group members through an unreliable broadcast channel. The improved efficiency for key management process is realized by periodically refreshing all public private key as well as the multicast keys in all the nodes using one newly generated function. The article classifies and compares the most significant key distribution schemes, key distribution algorithms, at the predistributed secret data management, and self-healing mechanisms. It consists of polynomial-based algorithms, exponential arithmetic based algorithms and hash-based techniques. Proposed classification is based on the applied cryptographic primitives.*

Keywords: *Self-Healing Mechanism Polynomial- Based Algorithm, Exponential Arithmetic Based Algorithm, Hash-Based Techniques.*

I. INTRODUCTION

A. Overview

In the field of networking, the area of network security process consists of the provisions and policies adopted by the network administrator to prevent the unauthorized access, modification, or denial of the computer network and network-accessible resources [2]

B. Network Security

The term network security and information security are used interchangeably. The security is generally used as providing protection to the boundaries of an organization. Information, however, explicitly focuses on protecting data resources from hacking by people within an organization by use of data loss prevention (DLP) techniques. It is to compartmentalize networks with internal boundaries [1]

C. Denial-of-Service

DoS (Denial-of-Service) attacks are most difficult to address. These are very easy to launch, difficult to trace and it isn't easy to avoid the requests of the attacker, also refusing legitimate requests for service**.** The DoS attack is ease: it sends requests to the administrator that it can be handled. There are toolkits available in the underground machines that make a simple test of running a program and saying it which host to blast with requests. The attacker's simply makes a connection of program on some service port, forging the packet's header information that highlights where the packet hacked from, and then dropping the connection. If the host answers 20 requests and the attacker is sending 50 requests, obviously the host will be unable to service all of the hacker's requests; much less any sending requests [4]

D. Unauthorized Access

``Unauthorized access'' is one of the technique that refer to a different sorts of attacks. The goal of these attacks is to access the resource that the machine should not provide the hacker. For example, a host might be a web server, and should provide anyone with logged web pages. However, the requested host should not provide command shell access without conforming the person making such a request that get the message, such as a local administrator [5]

E. Executing Commands

It's obviously unwanted for an untrusted person to be able to execute commands on machines. There are two classifications of the severity of this problem: normal user login and administrator access. A user can do multiple things on a system (such as reading the files, send them a mail etc.) An attacker should not hack any file of the logged user. This is the process how the attacker hacks the file. On the other hand, an attacker also wishes to make changes to the user (instead changing the system IP address, starting a start-up script in correct page to cause the machine to log out all the time it's started or similar sometimes). In this case, the attacker will gain administrator privileges on the host [6]

F. Destructive Behavior

There are two major categories of break-ins and attacks. They are:

Data Diddler

The data diddler is one of the worst sorts, since the fact of a break-in might not be immediately obvious. And also he's toying with the password and changing the dates in the projects and plans. Might be the hacker changes the users account password to auto-deposit of particular paychecks. It is rare where you'll work one day, and know that something is wrong.

Data Destruction

Some of the illegal attacks are simply twisted jerks who like to delete things. In these situations, the result on your computing capability – and continuously your business – is nothing less than if a fire or other loss caused your equipment to be completely destroyed.

G. Objective

The main objective of our project is to improve the network security. As the network usage increases day by day, the number of threats posed by intruders and hackers increases. To overcome these threats and data loss and provide a safe network that overcomes these threats we have to produce an advanced safety technique. So this project proposes a mechanism is to advertise the routing path information for IP prefixes. Improve the security that flexible communication infrastructures which provide a diverse set of securities. Improves in verification and signature generation.

II. EXISTING SYSTEM

Insecure mechanism in the existing network. No schemes are suitable for large scale WSN in real-world applications. Existing solutions present the tradeoff between the scheme performance and security level. It Identifies basic building blocks of the security scheme and describes briefly all essential types of existing solutions. It also contains a thorough security and efficient analysis of every solution, and figures out issues not identified. Performance is low. Security will be the problem while transferring the data from one system to another in the network due to the pattern recognition system. The hackers are extracting the secret key in between the data transfer in the network. The technique using in the approach is pattern recognition technique.

III. SYSTEM TESTING

A. Testing Objectives

Testing is a set of activities which is already planned and executed. For this reason the software testing, a set of steps that can be placed some specific test case techniques and testing methods should be defined for software processes. Testing puts more effort than any other software engineering activity. If it is conducted accidentally, time is wasted, unessential attempt is extended, and even worse, errors sneak through undiscovered. It is seemed to be reasonable to establish a systematic strategic for testing software. Testing is done for each and every module. After testing every module, the modules are integrated and testing of the final system is done with the test data and it is specially designed to show that the system will operate successfully in all its aspects conditions. Thus the testing is a confirmation that all is correct and an opportunity to show the user that the system works.

B. Testing Strategies

A number of software testing strategies have been proposed in the literature. They provide the software developer with a template for testing and all have the following generic characteristics: Testing begins at the component level and works toward the integration of the entire computer-based system. Different testing techniques are appropriate at some points of time. The developer of the software conducts testing and for large projects, independent test group.Testing and debugging are different activities, but debugging must be accommodated in any testing strategy. The final step involves Validation testing, which determines whether the software function as the user expected. The end-user mostly than the system developer conducts this test most software developers as a process called to uncover that only the end user seems able to find. The compilation of the entire project is based on full satisfaction of the users. In the project, validation testing is made in different forms. In question entry form, the correct answer will be accepted in the answer box.

C. Type of Testing

Unconventional Testing

Unconventional testing is a method of examining that is done by Software Quality Assurance team. It is a prevention technique which is executing from the beginning to the ending of the project development. In this process Software Testing Analysis team identifies the project development and it insures that the developing project is satisfying the requirement of the client or not.

Conventional Testing

Conventional Testing is the process of to find the bugs and fit the project. Testing indicates that in this process that the developed project is according to client's requisite or not. This process is a technique where testing team finds bugs and informing to the developing team for correction On developed project built.

Table 1: Test Case

Test	Requirement or Purpose	Action / Input	Expected Result	Actual Result	P/F
1	Browse the file you want to send	To click the browse button	Getting file contains window	Same as expected	Pass
2	For reset all text fields	To click the reset button	To clear all text fields	Same as expected	Pass
3	For sending the file to receiver	To click the send button	Receiver getting the files	Same as expected	Pass
4	For close the window	To click the exit button	Window closed	Same as expected	Pass
5	All the network connected system getting sending file	To choose public button	All the system getting file	Same as expected	Pass
6	Only specified system getting sending file	To choose private button	Only ip addresss mentioned system getting message	Same as expected	Pass
7	Files attached with virus file	To choose any virus file	File not received at receiver side	Same as expected	Pass

IV. PROPOSED SYSTEM

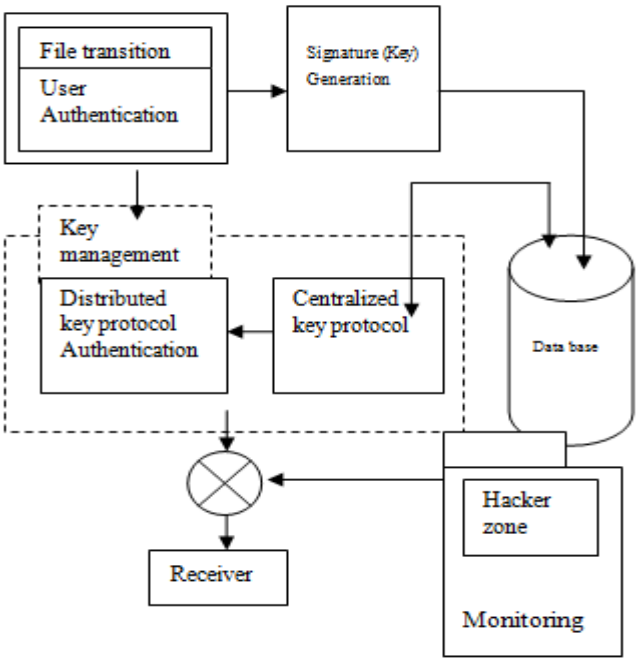
This system is categorized into three separate aspects, namely: Quantum key distribution process, predistributed data management and also self-healing mechanism, which are used to classify and compare schemes. There are three-dimensional classifications used based on each aspect of the scheme individually, which allows for more flexibility. The Self-healing group key distribution systems can be used in multicast networks with the centralized management system, which are established through an unreliable broadcasting channel, such as machine-to-machine systems, embedded and sensor networks, wireless and cellular networks. Communications security is accomplished by message encryption and authenticating it by using the shared symmetric secret group keys. A group key distribution method should satisfy the following requirements:

- Authorization: The system should inhibit adversaries or unauthorized user nodes, which are not in G, from knowing the group keys.
- Key freshness: Key distribution system has to furnish fresh keys.

Advantages of the Proposed System

1. Individualized encryption
2. Robust network connectivity
3. Efficiency is increased.
4. Hacker cannot easily detect the server.
5. The proposed system is harder to shutdown, monitored, hijacked and shutdown.

V. SYSTEM DESIGN SPECIFICATION



A. System Architecture

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be the considered to be the most critical in achieving a successful system and in giving the user, confidence that the new scheme will function and be effective. The implementation stage implements a careful planning, investigation of the existing system and it's restraint on implementation, designing of methods to achieve the changeover and evaluation of some changeover methods. Each program is tested individually and at the time of developing by using the data and it has been verified that the program is linked together in the way that specifies in the programs, the computer scheme and more over the environment is tested to the satisfaction of the user. The system that has been developed is admitted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. An operating system is included so that the user can understand the different functions clearly and quickly.

VI. MODULE DESCRIPTION

The following are the modules of the project along with the way they are implemented and that is planned according to the proposed system, while overcoming existing system and also providing the support for the future enhancement scheme. There are five modules used in our project which is listed below. Each module has some specific use in the project and its description is given below followed by the list of modules.

A. Sender/File Transmission

In this module, the login process itself has lots of security. Usually the users account name and password is sufficient to do the validation and login process, but there are some more actions are given to make more security during the login process. When the user is registered with the database, a set of keys will be generated for authentication. These authenticated keys will provide more security while sending the data from one system to another. The file search method is used to select the file to be sent. New User Creation process entitled to collect the details to maintain the file transfer or Key Management. The keys that are been generated in the database acts as a onetime password while the data is transferred.

B. Signature (Key) Generation

Sender holds the key values which have been generated by the key generation scheme. The keys are in two categories public and private that gives more security to the data transmission. The private key that allow sending the selected data to the particular location or system. The public key that allow sending to all the users who are all currently available in the network and the file transmission can be able, to process through Routers and reached the destination(receiver).

C. Signature (Key) Management

We present two new symmetric key that approaches for the secure mechanism: Pre-key distribution approach, centralized key distribution approach.

1. Pre-Key distribution

The users are given some substantial number of keys to avoid frequent key update. Periodic rekeying method, the keys are changed at the beginning of each process which is sufficiently long. Where the individual router is responsible for each key distribution, to secure the current updates. In the key distribution protocols the center node maintains a set of "k" keys.

2. Centralized Key Distribution

Where a central authority is responsible for key distribution. In this approach, the cost of signature generation for each router is only one signature, i.e., the route attestation that is added by this speaker. The charge of signature generation is lowering this approach, the cost of signature generation is very low, that each router needs to add its own signature to the update.

D. Hackers Zone

The node which is present in the different network or individual system accessing the data in the false name of a node which is present in the router network is called as hackers. The randomly generated key is not allocated to the hacker system.

E. Monitoring Access

Monitoring Access module takes care of the data sending through the network using the key. It accesses the database in order to check on the validation for proper and improper user. It also monitors the hackers if anybody accessing the data, which does not belong to the network.

Receiver:

Some of the node is acting as a sender and all the remaining nodes are the receivers. If a node sends a message that includes a signature from each of the keys it has and the receiver will verify the signatures based on the common keys that it has and then it can conclude that the message is authentic.

VII. RESULTS AND DISCUSSION

Implementation is the most crucial stage in achieving a successful system and giving the user the confident that the new system is feasible and effective. It may be implementation of a modified application to replace an existing system. This type of conversation is almost easy to handle, provide there are no major changes in the system. Each program is tested separately at the time of development using the data and has verified that this program linked together in the way that is specified in the programs specification, the computer system and its settings is tested for the satisfaction of the user. The system that has been developed is acknowledged and proved to be satisfactory for the user. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. Where the first step is the executable form of the application that is to be created and loaded in the common server machine that is to be easily accessible to the entire user and the server is to be connected to the network. The final step is to analyze the entire system which provides components and the operating procedures of the system. Implementation is one of the steps for the project when the theoretical design is turned out into a working system. And thus it is considered to be the most critical stage in achieving a successful new system and in giving the user the confidence that the new scheme will work and it will be effective. The implementation stage involves thorough planning, investigation of the existing system and constraints it by executing, designing of methods to achieve the changeover and evaluating the changeover methods. Implementation is the method of converting a new system design into operation. It is the phase that it focuses on user training, site preparation and conversion of file for establishing the candidate system. The important factor that is to be considered here is that the conversion should not disrupt the functioning of the organization. This process is said to be a correction technique where testing team identifies the bugs and reporting to the development team for further correction on developed project built.

CONCLUSION AND FUTUREWORK

There are three generating key contributions in this paper. First, we show that the right trade-off between efficiency and security for information could be achieved by adding the little bit of trust on routers. We present a capable threat model where for any path of length k, at least one router is trustworthy. Second, we introduce two new symmetric key approaches to securing information: the centralized key distribution approach and the distributed key distribution approach. Third, we estimate the efficiency of the two approaches with previous approaches to securing data. The estimation results show that the approaches are significantly much more efficient than previous approaches. Also, we have discussed the deployment issues and essential concerns like key management and interoperability to illustrate the feasibility of our protocols. There is a constant development in this area, and particularly post September11 a lot of discussion has been around protecting critical infrastructure such as the Internet. Router is a critical component of this. We have been lucky up to now that there have been no significant security related incidents related to Network, but the possible impact of an attack is so significant we should not be complacent. The internet community is coming up with a lot of new proposals regarding network security all the time; we discuss a few here that may be significant in the future. Secure distribution is a proposed version of key freshness that includes strong authentication and encryption using public key infrastructure. Read the work by the BBN Technologies, Internetwork Research Department for a detailed explanation of the proposal. This has been around for a few years in discussion stages and a number of prototype network have been successfully trailed. However a technological chicken and egg problem has so far stopped it from being deployed in the real world. The main issues are that there are several parties that implicate all the needs to agree. The Internet Engineering Task Force (IETF), the

registration organizations and the ISPS. The ISPs will need to invest in new technology and spend money to implement this. As these will not provide new services to the clients they cannot directly charge their clients for this work. This makes them unwilling to invest in these changes. The registration organizations need to agree to set up a digital signature Public Key Infrastructure (PKI) again without ISP buy in they are reluctant to invest the time and effort. The hardware manufacturers have not bought into the new process and have been reluctant to include support for SBGP in their platforms. The dilemma is that there is a high cost to secure BGP and avoid any major incident, but unless an incident occurs the parties involved are reluctant to spend that money.

Ptomaine

When you advertise a route to a peer you have little or no control over how this is distributed or how other ASs will use it in route decision making. Ptomaine proposes a new external community mechanism that allows a route advertisement to include filters so that we can control how this is passed upstream to other ASs. As we know prefix filtering is one of the main security techniques and anything that allows this to be extended this will improve the security of BGP. It would be possible for example, to not only create egress filters to stop us advertising other IP addresses than our own, we add this filter to the route advertisement so that upstream ASs so they don't propagate invalid routes for our address space.

References

[1] H. Zhou, L. Huie, and L. Lai, "Key generation in two-way relay wireless channels," in *Proc. 17th Annu. Conf. Inf. Sci. Syst.*, Baltimore, MD, USA, Mar. 2013, pp. 1–6.

[2] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in UWB channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364–375, Sep. 2007.

[3] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[4] L. Lai, Y. Liang, and H. V. Poor, "A unified framework for key agreement over wireless fading channels," *IEEE Trans. Inf. Forensics Security*, vol. 7, no. 2, pp. 480–490, Apr. 2012.

[5] T.-H. Chou, A. M. Sayeed, and S. C. Draper, "Impact of channel sparsity and correlated eavesdropping on Secret key generation from multipath channel randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2518–2522.

[6] A.Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Process.*, Las Vegas, NV, USA, Apr. 2008, pp. 3031–3016.