Three Tier Securities for Data in Network

Miss. Heena Siraj Khanche
Department of IT,
Navnirman College of Arts,Commerce and Science, Ratnagiri
University of Mumbai.
heenakhanche91@gmail.com

Abstract
The network security is becoming more important as the amount of data being exchanged on the Internet is increasing. Security requirements are necessary in order to secure the network.

In order to secure network, the major challenge is to ensure the proper balance between access and security. There are some of the resources that are to be protected and controlled, such as data in database servers and backend mail server, etc. In this frame work for securing the data in network, it uses multilevel security schemes for securing secret data as well as provision for user authentication and to control eavesdropping. Hence, to reduce the damages caused by data provider replication attacks, we have designed a strong authentication mechanism in the proposed system.

I. INTRODUCTION

As with the increasing use of internet the wide range of electronic services: email and web. Therefore, the network connectivity increases rapidly. Thus, there is a need to provide awareness regarding the confidential data that is being exchanged in a network. Due to which various access control techniques and complex authentication mechanisms are implemented.

The idea to solve security problem is to create various network tiers. The tiered architecture separates the untrusted connections and trusted connections within the network. Generally, the system is developed in with the nodes which are not trust worthy are proceeded to get compromised. But the network with multiple tier can be able todesign sufficient tiers to allow security system to detect an attack. Here, the trusts worthy nodes are secured or prevented from attack.

The Three tier technique implemented in this framework uses and intermediary node or middleware. Therefore, the data from the source node to the destination node is exchanged via intermediate node. These nodes authenticate itself with source node as well as the destination node. The SSL (Secure Socket Layer) security is used by various standardized organizations. Thus, this SSL user session sometimes gets compromised and attackers can get access to user data or can retrieve the keys used for authentication.

Network security measures are needed to protect data during their transmission. All business, government and academic organizations require the strong security scheme in order to secure their confidential data.

An examples where Three Tier security scheme is used is E-banking where the entire system is developed using multiple tiers so as to maintain the 3 requirements:

1. High Availability
2. Security
3. Scalability

Where in this system there is a middleware existing between the customer and bank server and this middleware authenticates itself using keys smart cards. Therefore the keys in the smart card could not get compromised and thus, there is no possibility of attacks. The intermediate node consists of larger storage and computation capability. Data which is exchanged between the customer and bank database is first sent to intermediate node and then based on actual request and authentication the desired data is made available to the customer.

In recent years, wireless network [1] have gained popularity as they provide a promising low-cost solution to a variety of challenges in both military and civilian domains, e.g. traffic monitoring, homeland security, and military surveillance. Comparing to traditional homogeneous wireless network, a three tiered design shows better cost-effectiveness, longevity and scalability.

- Military and intelligence agencies require strong security scheme for efficient data hiding.
- Crime and investigation department uses a complex security schemes to secure their confidential data.
- Law enforcement and counter intelligence agencies are interested in understanding these technologies and their weaknesses, so that they could detect and trace confidential messages.

Generally to ensure security for exchanging data using messages or mails, first is to establish secure transmission in which the sender entering his password or secret key and then either he short text message or entire message can be encrypted and then the result can be used to be stegnographed. The message file could be stego text or image file. And at the receiver side that secret key or password is used to retrieve the secret message that is received encrypted, steganographed.

II. EXISTING TECHNOLOGY

In the existing system, client and Servers are connected to each other directly without any intermediary and they have to authenticate each other in order to exchange the data. This system uses various encryption and cryptographic techniques for authentication. Since no intermediate node is available in the system there is the possibility where the keys can get compromised and hence attackers can easily retrieve the data that causes the great security loss.

Drawbacks of existing system

1. Usually most of existing approaches for security are having utmost 2-tier security.
2. Steganography has been used and many Steganographic tools are available but none of them fulfill the requirements of secure communication and authentication. The few security challenges faced by existing schemes are:

- Provision of authentication.
- The amount of data to be hidden and sent.
- Provision of secure channel.
- The specification of the types of files to be used as cover file and message file.

3. Existing systems Encryption Algorithms are large, complex and time consuming.

III. RELATED WORK

A major concern to network security is replication attacks and other attacks which retrieve the data i.e., vulnerable so that attackers could easily retrieve the data that is being exchanged on internet. According to the survey latest mathematics and operating methods are invented to solve this problem. The key management issues are a competitive research area in wireless networks. The recent scheme proposed a key pre distribution [2] scheme which is used to build the trustbetween the various requesting nodes. The differential distribution and counter keys to requesting nodes and re-keying with no computation and communication capabilityisdescribed. The probabilistic key pre distribution is nothing but the random subsets of keys are retrieving from large key pool.

The requesting nodes are communicated securely with each other by using various cryptographic techniques [4] by using bi-variate key polynomials. It is one of the most initial security services. Some of the constraints of the nodes does not make it possible to utilize pool keys. The efficient techniques provide a direct key established between randomly two adjacent sensor nodeswith the network while data exchange. As compare to the existing security scheme, there are relatively stronger techniques for data security and network connectivity. It also supports dynamic point additionafter the primary deployment of the nodes in the Communication network.

In this new technique of security,the stationary access nodes play an important role to provide authentication within the network, so that access node can obtain access to the data from various providers in the network. Therefore, the message transmission take place between requesting node n provides is through the stationary access node. This technique is based on the scheme i.e., two nodes share at least one key in order to authenticate itself.

IV. THE PROPOSED SCHEME

In the three tier architectural framework network there are three tiers, i.e. three separations are done for the entire network data exchange process namely: access, distribution and core. Access consists of various client connections such as mission critical client which are nothing but the external node which request the data on the network i.e. their task is of data gatherings. Distribution consists of intermediate node these are the middleware connected to client and providers in the network. This middleware acts as proxy server, which consist of larger storage and provide greater security as the large amount of data which is sent from network providers is stored here and when the client node request for a particular data, instead of sending the entire data from providers it filters the data and send only the desired data which is requested from client. Thus, the confidentiality of the data is being maintained and the load on the network gets reduced. So that, the data exchange rate increases. Core of the system consists of various provider nodes these provider nodes provide the data which is made available to multiple clients. Therefore, the same amount of data can be viewed or retrieved by multiple clients at a same time.

In the proposed scheme, the security is maintained by providing authentication between two nodes that is client and server, but this authentication done via intermediate node. The keys used for authentication are placed in two separate polynomial pools which is proposed by Liu and Ning [3]: the Data Requester polynomial pool and the static polynomial pool. The keys used here are in form of polynomials.

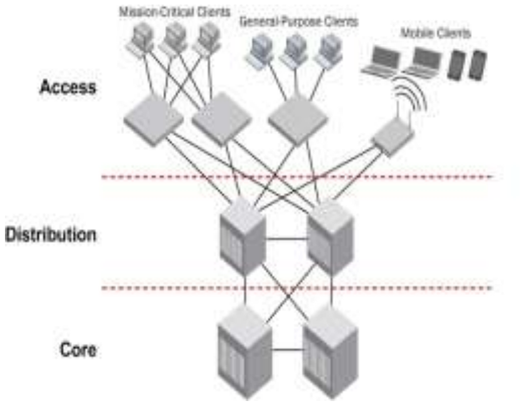


Fig. 1 Three Tier Framework in a Network.

Thus, Polynomials from the Data Requester polynomial pool are used to establish the security between Data Access node and stationary access nodes, which will enable this Data node to access the Data Provider for data collection. Thus, an attacker would compromise at least a one polynomial from the Requester polynomial pool to obtain access to the network for the data gathering. Polynomials generated from the static polynomial pool are used to ascertain the authentication and keys setup between the Data provider and stationary access nodes. Priority wise, each Data Requester randomly picks a subset of polynomials keys from the Requester polynomial pool.

Thus, this becomes one of the efficient techniques by which easy and efficient key generation is possible and it provides higher authentication as that provided by single or two tier framework used for network security.

It improve the network security to Data Requester replication attack as compared to the single polynomial pool based approach, we intend to minimize the probability of a Data Requester polynomial being compromised if Data Provider captured.

V. MODEL FOR AUTHENTICATION

The authentication required to exchange the data between client and internet. Generally, for authentication we use here is polynomial pool generation technique. This is one of the efficient techniques used for authentication. In this technique two separate polynomial pools are used to ensure three tier securities: the data access polynomial pool and the static polynomial pool. For data gathering from the providers through the data providers, the polynomials from data requester polynomial pool are used.

- Keys are generated from polynomial for authentication of access node from data access polynomial pool.
- This access node is connected to intermediate node via network connection and authenticate client with the keys from polynomials.
- The intermediate node consists of both the polynomial pool: data access and static.
- Similarly, the network providers generate keys from static polynomial pool and authenticate it.
- After secure authentication data can easily get transmitted from providers to intermediate node and from intermediate node to client node

In order to gain access to the network for the network access provider data gathering, an attacker has to compromise at least a one polynomial from the pool. For key setup between the requesters nodes and stationary access nodes the polynomials from static polynomial pool are used.The main advantage to use separate pools is to provide complete authentication in the network data exchange.

Key implementation between data requester node and data providers

A. Direct key technique

To establish a direct pair wise key between data requester node 'u' and data provider node'v', a data requester node 'u' needs to find a stationary access node 'a' in its adjacent nodes available, such that, node 'a' can establish pair wise keys with both data provider node 'v' and requester node v. Fig shows a direct secure path establishment between nodes 'u' and 'v', data provider 'v' sends the pair wise key to node 'a' in message encrypted and authenticated with the shared pair wise key ;'a' between 'v' and 'a'.

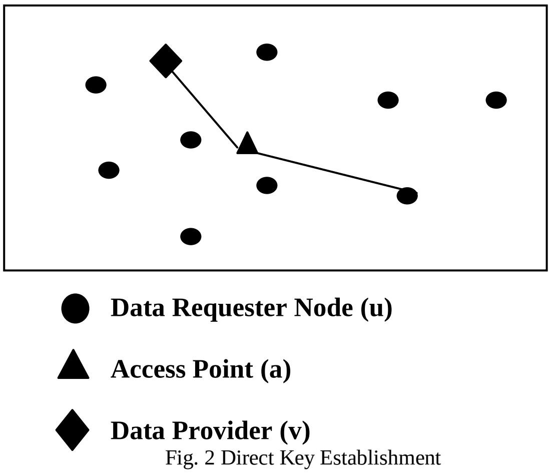


Fig. 2 Direct Key Establishment

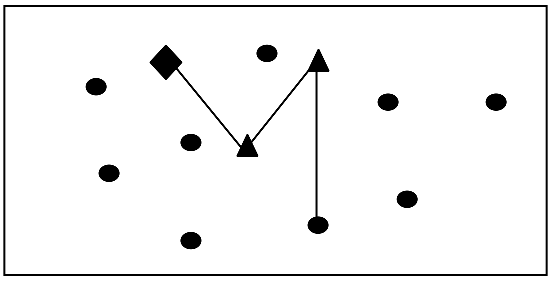
And If node 'a' receives the above encrypted message and it shares a pair wise key with 'u', it sends the pair wise key to node 'u' in a message encrypted and authenticated with pair wise key; 'u' between 'a' and 'u'.

B. Indirect key technique using intermediate node

It illustrates that the provider node and the requester node will have to establish a pair-wise key with the help of other requester nodes using indirect key technique.

To establish a pair-wise key with data provider ‘v’, a sensor node ‘u’ has to retrieve a stationary access node ‘a’ in its adjacent nodes such that node ‘a’ can establish a pair wise key with both nodes ‘u’ and ‘v’

If node ‘a’ establishes a pair wise key with only node ‘v’ but not with ‘u’. As the probability is high that the access node ‘a’ can discover a common requester polynomial with node ‘v’, the data requester node ‘u’ needs to find an intermediate sensor node ‘I’ with the path u ,I , a , v, so that intermediate node ‘I’ can establish a direct pair wise key with node ‘a’.

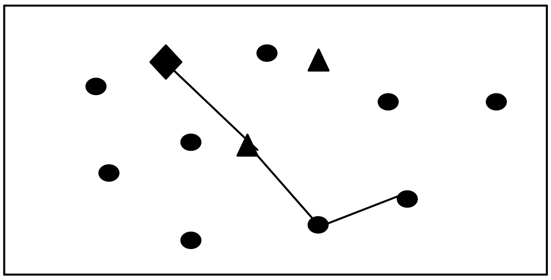


◆ **Data Provider (v)**

Fig. 3 Indirect Key establishment using Stationary Node

C. Indirect key technique using intermediate stationary node

It shows that the providers and the requester node will have to establish a pair-wise key with the help of other requester nodes using indirect key discovery. To establish a pair-wise key with data provider node‘u’, a data requester node ‘v’ has to find a stationary access node a in its adjacent such that node ‘a’ can establish a pair-wise key with both nodes ‘u’ and ‘v’. If node ‘a’ establishes a pair wise key with only node ‘v’ and not with ‘u’.



● **Data Requester Node (u)**

▲ **Access Point (a)**

◆ **Data Provider (v)**

Fig. 4 Indirect Key establishment

As the probability is high that the requester node ‘a’ can discover a common requester polynomial with node ‘v’, requester node ‘u’ needs to find an intermediate sensor node ‘I’ along the path u , I , a , v, such that intermediate node ‘I’ can establish a direct pair wise key with node ‘a’.

VI. CONCLUSION

The three tier security implementation provides efficient and complex security model as compared to single tier or two tier security model. Here in this paper, data on the network is ensured with security, integrity and scalability. Also, the network load is reduced due to which data communication becomes faster.

This paper eliminates the possibilities of various network attacks [5] such as duplication of data, replication of data providers or access node, eavesdropping, accessing of client credentials. Thus, provide a complex secure model and solves the major problem related to network security.

ACKNOWLEDGMENT

I would like to thank from the bottom of my heart, the Head of the department ofMCA, **Prof. Tejas V. Joshi** for encouraging me and I express my profound gratitude to my paper guide **Prof. Waman R. Parulekar** for the valuable help and thorough guidance while the writing paper. I would also like to thank **Prof. Rahul Kotavadekar** for helping me and encouraging me to write this paper.

REFERENCES

[1] .H. Deng, W. Li, and D.P. Agrawal, “Routing Security in Wireless AdHoc Networks,” Proc. IEEE Comm. Magazine, pp. 70-75, 2002.

[2] H. Chan, A. Perrig, and D. Song, “Random Key Pre-Distribution Schemes for Data provider Networks,” Security and Privacy, 2003.

[3] D. Liu, P. Ning, and R.Li. Establishing, “Pairwise Keys in Distributed Data provider Networks,” Proc. 10th ACM Conf. Comm. Security (CCS ’03), pp. 52-61, Oct. 2003.

[4] A. Rasheed and R. Mahapatra,” The Three-Tier Security Technique in Wireless Sensor Networks with Mobile Sinks,” IEEE Transactions On Parallel And Distributed Systems, Vol. 23, No. 5, May 2012.

[5]William Stalli, Cryptography and Network Security Principles and Practices,4thedition,Prentice Hall, 2005.