International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 05 | May - 2021 ISSN: 2582-3930

Password Based Authentication for Insider attack detection and prevention using Elgamal Encryption

Shriniketh D[1], Dr. Umarani C [2]

[1]Student , [2]Assistant Professor

Jain University, Bangalore, India

Abstract - ***The recent developments in web services has brought high attention towards providing security for various real time applications, which servers internet users. To access applications and get authenticated for using various applications users provide their username and password for authentication purposes, which may have some personal information revealing privacy of users may also provided. The privacy information shared by users on applications is stored on the server and may be exploited through security attacks on server. Thus the information shared should be kept secure otherwise can be exploited for illegitimate activities. Providing security to the system from security attacks are more important. Identifying and preventing insiders attacks are more challenging than external attacks, due to the fact that identifying such attacks are difficult and the users acts are legitimate and they use valid privileges for accessing applications. There are existing works studied by researchers on insider attack detection through various techniques and there is still a strong model to be proposed. In the proposed system, a novel security framework using cryptographic algorithm, Elgamal is used to identify and prevent insider attackers. The experimental results and analysis shown that the proposed protocol provides not only security to application and also prevents other types of attacks. The implementation of cryptographic keys and communication cost is less in the proposed work. The proposed protocol satisfies application authentication by providing two way authentication protocol through Elgamal encryption.***

***Key Words*: Insider attacks, Web Services, Elgamal Encryption, Cryptography, legitimate node, Secure authentication, Two way authentication**

1.INTRODUCTION

Information communication engineering is the growing area of demand in many real world applications, providing security to these applications are even more crucial at present. Security measures must defend against insider attackers, which can cause severe security breach for user information stored in the server. Access privileges and authentications plays crucial role in information security. Authentication is important to access an application and it verifies user identity and password provided by user to access the application, which checks the user's as legitimate or not and then authorizes users to access an application. Authentication is divided into few major categories namely, login credentials, which is provided to access application with user ID and password, smartcards i.e. electronic card using which users can get authenticated, verification keys and access cards, and biometric fingerprint matching, voice recognition, face recognitions. User authentication via login credentials are more comfortable, reliable, and inexpensive to implement such modules and give more strength to application security. These are types of authentications provided to users to identify and authorizing them.

Information security achieves security through password credentials for identifying user with random bits generated password. Under web services, password bits required are less than or equal 29bits and this is the measure of password strength. Users need to exploit their password to get authenticated for accessing and applications. However, brute force attacks is one the strong attack , in which attackers guess the passwords randomly and try to authenticate themselves. Thus credentials should be more secure and defend against possible attack types.

There are many security attacks based on source it comes from or behaviour of attack on applications. Source of attacks external attacks and insider attacks. Behaviour are two major classifications namely active attacks and passive attacks. External attack are the come which comes outside of network, these are kind of physical attacks externally by the attackers. Insider attack the one which is attempted within the network or application, these attackers are normally one who prior knows about network and user's credentials like previous employees of organization.

Active attacks are the attacks which cause serious damage to the functioning of networks. Whereas passive attack are one, intercepted data or packets dropping and modification attacks. Many type of active attacks are spoofing, Sybil attacks, masquerading, Denial of service (DoS), sinkhole, wormhole attack etc. Passive attacks are traffic analysis, which analyze all incoming packets, but only analyses and do not drop or modify data. The most severe once is insider attacks this is implemented with less efforts by the attackers as the network is completely known to them. Overview of insider attack prevention is shown in the below figure.

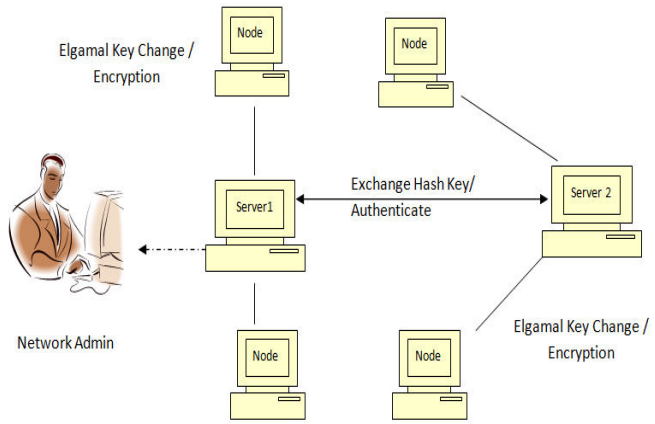

Figure: 1 Overview of insider attack protection

CRYPTOSYSTEM

ElGamal algorithm is a public-key cryptography algorithm. This is a asymmetric key algorithm used for communication between two entities or users. This is based on discrete logarithm function, where difficult to find the key by attackers. Give a Secret key SK and publick key PK, the system has to compute based on discrete logarithm to get the secret key. This algorithm helps in exchanging privacy information between two users through a secure channel. The digital signature created through the algorithm is difficult to identify by the attackers. This signature is valid only when the session between users exists. For the next authentication, a new session is created for the secure channel communication. There are many advantages using ElGamal cryptosystem, most important is we get a unique ciphertext whenever the same text is encrypted. The key size is shorter compared to other traditional algorithms.

In the following chapters some of the research related to network monitoring are discussed. In chapter 3, the details on implementation of proposed methodology is discussed. In chapter 4, Results and discussed are given. Finally, chapter 5, discussed work Conclusion and further enhancements are discussed.

2. RELATED WORK

Insider attack detection and prevention is a crucial role for every industries and businesses, there are many researchers studied on insider attack detection. In this chapter, some of the researches handled in insider attack detection is studied in detail.

Insider attack detection in DMZ a special network model was designed in [1], this work has deployed with network intrusion detection monitoring, but NIDS only cannot find insider attacks, thus a more secure model of identifying system calls was proposed. The PDF obfuscation method was proposed to check the performance of IDS monitoring and deep packet inspection can be identified.

Insider threat in cloud was studied in [2] specifically for mobile edge cloud computing, higher the number of monitoring agents are deployed, higher the possibility of detecting insider attackers in network. Combined knowledge of monitoring agents of collected access privileges are used. When an insider request to learn a data, the request may not be granted at the host level itself, thus it can mitigate the insider attackers at host level itself.

The paper [3] analyzed insider threat detection based on data granularity. System analyzes individual data, as well as insider and malicious data. There are few works proposed based on machine learning detection of insider threats, these are indentified by the patterns learned by algorithm. The work considered CERT dataset for implementing a supervised machine learning model. Experimental results shown that random forest algorithm achieved highest accuracy on insider threat prediction.

Insider threat detection with multi feature is studied in [4] which used graph based correlation on CERT dataset. User activity log including email, login frequency and history of browsing were analyzed for content based and behavior based feature data to train the classification machine learning algorithm. When the user behavior varies with historical data, then the possible insider attacker is detected.

The work [5] discussed symptomatic risk on insider threat framework for an organization in real time using a quantitative analysis, two insiders were found. Insider profile is identified through integrated container. This container used to find the threat scoring function. When the employees are assigned a questionnaire using which risk assessment is done with proficiency to malicious activities.

Detecting insiders attack in network application through an ensemble learning method was proposed as negative selection algorithm. This technique is one the machine learning model which used classifier to identify insider threat, the data sources were collected from various source thus as heterogeneous in nature. However, the author used to analyze through patterns, real time detection is not much feasible to analyze the network security.

Insider attack detection in IoT (Internet of Things) enable application is studied in [9]. Deep learning algorithm is used to analyze the attackers and based on learning they are classified. Jaccard based Distance calculations technique and cosine similarity were arrived to identify threshold under data pre-processing steps. Results were given good accuracy on attacker detection.

Insider threat detection by reputation identification and clustering algorithm were proposed in [10]. This model used node's reputation values to build the system, agent node were deployed for monitoring purposes, attacker activity is identified when there is a low reputation values. Genetic algorithm for feature selection is applied then clustering used to classify attackers. However, this method on detection may fail and more complicated identifying when all agents get compromised by insider threats.

Insider threat detection in wireless sensor networks were studied in [11] using trust management and monitoring model. Node

reputation is shared by the neighbor nodes is considered for arriving trust value and then assigned to nodes. There were two types of trust values are calculated one is direct and other is indirect trust values. However, this technique may not indentify insider attacks when any one of neighbor node who is give trust value is compromised and assign a wrong reputation value.

From the above study, some of the points were inferred are, most of existing studies researched had few complexity on insider threat detection, some work exploited security algorithms for authentication through login credentials. Some of the studies discussed were using machine learning algorithm and deep learning algorithms, however, machine learning and deep learning can only identify patterns, detecting insider threat under real world scenarios is highly difficult. The proposed protocol identifies insider threat and prevents the other possible attacks also through a novel ElGamal Encryption and elliptic curve cryptography algorithms. The proposed protocol creates a secure communication channel, which indentify insider attacker, also prevent them getting any services from service provider by two way authentication process.

3. PROPOSED WORK

This section briefs proposed security protocol for identifying and preventing insider attacks. Three entities are used for the implementation are password management server (PMS), service providers (SP) and Clients PC. PMS is responsible for generating authentication keys for secure channel and it is provided by two way authentication. Every client PC register to the PMS with unique authentication keys and in the second level of authentication, session key is generated and shared, which is turn indentifies insider attacks if any. Service providers gives corresponding service reply to service request from client PC.

The following figure represents the proposed architecture of insider attack detection and prevention, three entities and its functions are represented. Attackers attempt within the network can be identified by computational Diffie Hellman problem.

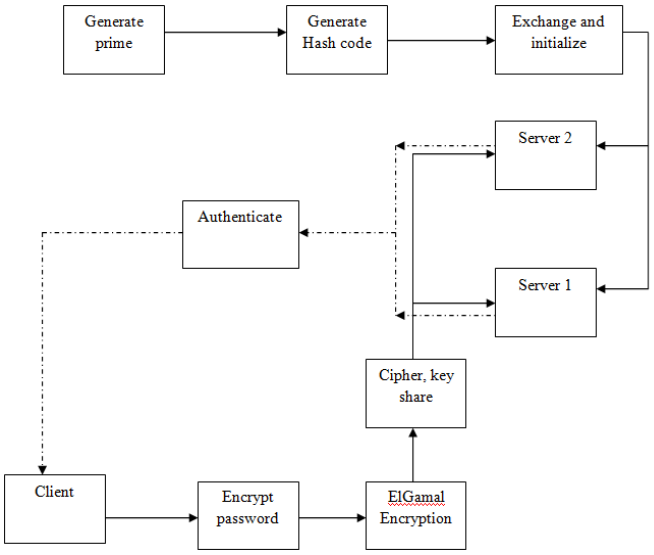

Figure 2: Work Flow

Proposed protocol implementation need following five modules and the modules description and functionalities are discussed in this chapter

- Service provider Instantiation
- Client PC registration
- Authentication module
- Query Request
- Attacker identification

The above modules and its implementation are discussed in the below chapter with their importance and output of each modules are discussed.

SERVICE PROVIDER INSTANTIATION

Network instantiation is considered as the first module of implementation, the service providers Server A and Server B is considered with unique IP address and port number. Service providers are registered with PMS and unique keys are assigned for them. Using Diffie Hellman key exchange, these two servers exchanges a secret key and get authenticated themselves on instantiation time. On network initialization, the next entity Client PC/Users are established and assigned unique key by PMS module. After initialization, users shares their login credential such as username and password to service providers to avail the service requests. Clients crede3ntial data are encrypted through ElGamal encryption algorithm by PMS module and sent to service providers, they can decrypt and check the credential before giving them services.

CLIENT PC REGISTRATION

Client PC are registered with password management server and get their unique username and password as login credentials to application. Once the client PC gets logged into to application, the session key will be shared by the password management server as a second round of authentication. Session key will be shared to the service provider for requesting services for every transactions. ElGamal encryption algorithm encrypts the client password shared in the server system. For access the application and get the services, every client PC has to register with two servers Server A and Server B. The cryptanalysis on every message transmission is done between the client and PMS. The following figure represents Server A and Server B monitoring client PC activities.

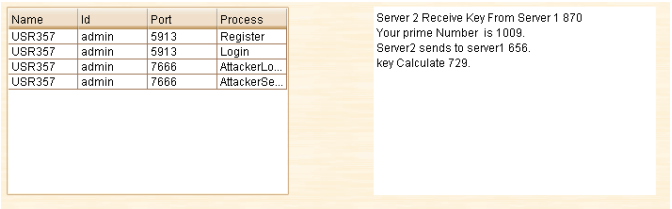

Figure: 3 Client Registration

AUTHENTICATION AND KEY EXCHANGE

Two Service providers Server A and Server B gets credentials shared by the clients for password authentication through registration process. Once the credential are valid, the active clients are shared a session key for second round of authentication.

Client PC choose a random integer value 'R' and 'Q' using Diffie Hellman key algorithm, these keys are transferred through secure channel to request a services from service providers.

Message ={C, Req, R}

where R is the password, to the two servers SA and SB.

Server SA and SB computes key upon receiving a service requests from client PC then exchange key and requests among service providers. Server SA and SB both transmits an integer values to user/client. When the key is authenticated, client is considered as valid client authenticate service providers for establishing secure session through the proposed protocol.

The following figure explains Session key generated by PMS server and broadcast to client for authentication.

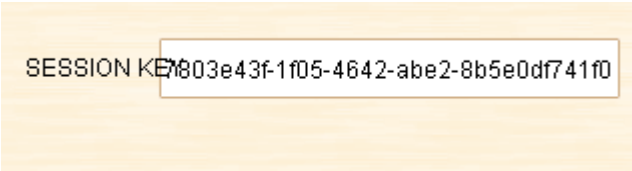

Figure: 4 Session key generation for client

QUERY REQUEST

Client PC uses a secure communication channel created by the proposed protocol between client PC and service provider. They used the channel to make their service request and get service reply from providers. Client PC requests a query 'Q' through secure communication channel and it sent to service providers SA or SB, which will reply query results 'R'.

Figure: 4 Query response from service provider

The following screen represents communication through secure channel using session key provided by elliptic curve cryptography. The results are retrieved from database and replied through secure channel of proposed protocol.

ATTACKER IDENTIFICATION

Attacker is designed in such a way that, they use the existing legitimate users login credential for login application. The attacker node also uses session key of existing users session, which is a insider attack. This is a kind of passive attack, used existing users identity to login the application and the services from service provider. Whereas the session key is verified by service provided if found as existing one, then identified as attacker and requests are denied.

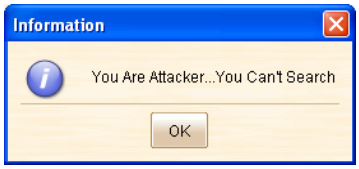

Figure: 5 Attacker detection module

The above screen mentioned attacker detection module through authentication credential failure from client PC and service provider through secure channel.

4. RESULTS AND DISCUSSIONS

This chapter briefs implementation of proposed protocol, which establishes a secure communication channel between user and service providers. The implementation Java version JDK 1.8 for design and logics. Database server used is MySQL 5.5. Graphical user interface is designed with Java Swing. There are three entities developed are Service providers as Server A and B, Client PC and Password management server, whereas PMS is an invisible module, which only used for generating user credentials and session key through secure cryptography algorithms.

Every nodes deployed in network is assigned with unique IP address and port number and the network is considered as wireless networks. Clients PC designed as Windows application assigned unique ID and password for login. Socket connection is established between client and servers to access network. A smart attacker is also designed with same pattern as Client design and try to get access of existing users credential and misuse it. Though the attacker is able to interrupt the secure channel and try get any services from provider, cannot get any valid data as they are identified and blocked by the proposed protocol.

Proposed protocol is public, which means client and attacker can execute and mimic themselves as legitimate node. The following figure represents protocol established a secure key through ElGamal Algorithm and exchanged in communication channel for authentication between service providers.

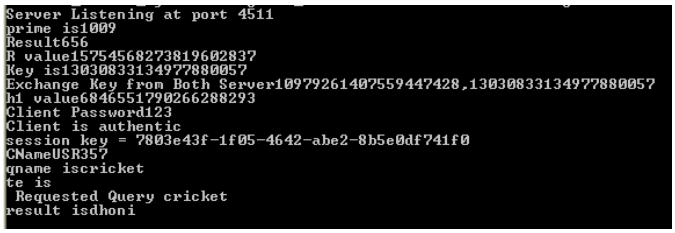

Figure 6: Client and Service provider authentication

The following screen shows ElGamal Algorithm generated key for node with prime number and secure key is exchanged between two providers A and B for authentication.

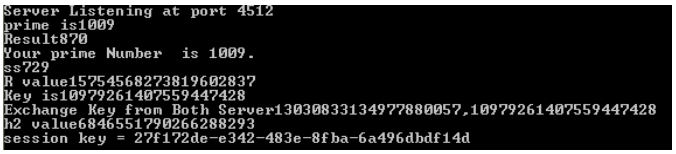

Figure: 7 Service provider authentication

Session key establishment and sharing over the secure communication channel by ElGamal Algorithm and authentication is done in time interval for every few seconds throughout the connection time for client with service providers are shown in the below screen.

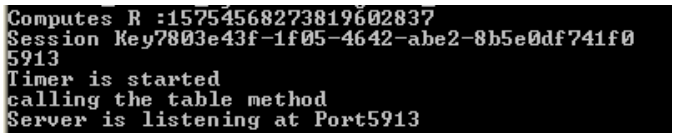

Figure: 8 Time wise authentication of session key

Attacker is designed as same as client module, insider attacker enters node Identity existing user and password. Communication channel is established as initial and attacker when used session key of legitimate user, service provider validates the session key and blocked as attacker node.

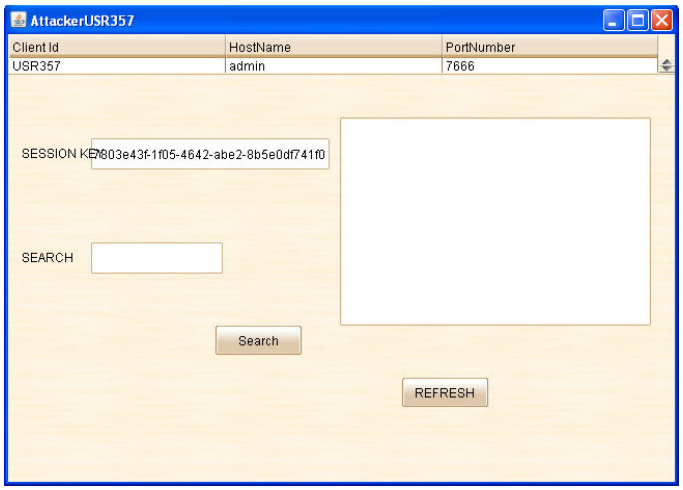

Figure: 9 Application design of Insider Attacker module

5. CONCLUSIONS

The current demand for secure communication to access many applications has paved way for enormous research in this area. The performance of security algorithms proposed so henceforth were lagging with major drawback that it may not detect or prevent the insider attacks, which may damage serious threat to networks. There were many cryptographic techniques experimentally proved were failed to identify insider attacks. In this proposed work, a secure communication channel is created using cryptographic protocol Elgamal technique identifies and prevents insider attacks. Time taken for renewal phase is less compared to all existing systems and the periodic validation of credential keys makes the network more secure than existing one. The proposed protocol not only defend against insider attacks but also many other security attacks. The computation cost for creating key credentials are less in the proposed protocol.

FUTURE DIRECTIONS

The future enhancement may be extending with various cryptography comparison, namely Elliptic curve cryptography (ECC). As an extension to current work, location of client PC can also be monitored to improve the security for location based services.

REFERENCES

[1] R. Gegan, B. Perry, D. Ghosal and M. Bishop, "Insider Attack Detection for Science DMZs Using System Performance Data," 2020 IEEE Conference on Communications and Network Security (CNS), 2020, pp. 1-9, doi: 10.1109/CNS48642.2020.9162260.

[2] Q. Althebyan, "A Mobile Edge Mitigation Model for Insider Threats: A Knowledgebase Approach," 2019 International Arab Conference on Information Technology (ACIT), 2019, pp. 188-192, doi: 10.1109/ACIT47987.2019.8990987.

[3] D. C. Le and A. Nur Zincir-Heywood, "Machine learning based Insider Threat Modelling and Detection," 2019 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), 2019, pp. 1-6.

[4] J. Jiang et al., "Warder: Online Insider Threat Detection System Using Multi-Feature Modeling and Graph-Based Correlation," MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM), 2019, pp. 1-6, doi: 10.1109/MILCOM47813.2019.9020931.

[5] J. Ikany and H. Jazri, "A Symptomatic Framework to Predict the Risk of Insider Threats," 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD), 2019, pp. 1-5, doi: 10.1109/ICABCD.2019.8851020.

[6] L. Flynn, C. Huth, R. Trzeciak and P. Buttles, "Best practices against insider threats for all nations," 2012 Third Worldwide Cybersecurity Summit (WCS), New Delhi, India, 2012, pp. 1-8, doi: 10.1109/WCS.2012.6780874.

[7] Safa, Nader & Maple, Carsten & Watson, Tim & Solms, Rossouw. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications. 10.1016/j.jisa.2017.11.001.

[8] O. Igbe and T. Saadawi, "Insider Threat Detection using an Artificial Immune system Algorithm," 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 2018, pp. 297-302, doi: 10.1109/UEMCON.2018.8796583.

[9] A. Y. Khan, R. Latif, S. Latif, S. Tahir, G. Batool and T. Saba, "Malicious Insider Attack Detection in IoTs Using Data Analytics," in IEEE Access, vol. 8, pp. 11743-11753, 2020, doi: 10.1109/ACCESS.2019.2959047.

[10] Z. Bankovic, J. M. Moya, J. C. Vallejo, D. Fraga and P. Malagon, "Holistic Solution for Confining Insider Attacks in Wireless Sensor Networks Using Reputation Systems Coupled with Clustering Techniques," 2011IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Changsha, China, 2011, pp. 61-72, doi: 10.1109/TrustCom.2011.12.

[11] R. R. Sahoo, S. Sarkar and S. Ray, "Defense Against On-Off Attack in Trust Establishment Scheme for Wireless

Sensor Network," 2019 2nd International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, 2019, pp. 153-160, doi: 10.1109/ICSPC46172.2019.8976869.

[12] Q. Yaseen, A. Alabdulrazzaq and F. Albalas, "A Framework for Insider Collusion Threat Prediction and Mitigation in Relational Databases," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019, pp. 0721-0727, doi: 10.1109/CCWC.2019.8666582.

[13] L. Liu, O. De Vel, C. Chen, J. Zhang and Y. Xiang, "Anomaly-Based Insider Threat Detection Using Deep Autoencoders," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), 2018, pp. 39-48, doi: 10.1109/ICDMW.2018.00014.