IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 1, No. 2
April 2015

2nd National Conference on "Recent Advances in Science Engineering & Technologies" RASET 2015

Organized by
Department of EEE, Jay Shriram College of Technology, Tirupur, Tamil Nadu, India.

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Special Issue, Vol. 1, No. 2, April 2015
2nd National Conference on "Recent Advances in Science,
Engineering&Technologies" RASET-2015

Research Paper

FILE SECURITY SYSYTEM FOR AVOIDING INSIDERS ATTACK

B Balakrishnan[1]*, S Haribaskar[1], P Stalin[1], V Gokul[1] and K S Mohan[1]

Corresponding Author: **B Balakrishnan ✉ pbskrish@gmail.com*

The emerging computing technologies had significantly change the way we access and store millions of information .The increased rate of data accessed and stored have put forth several data security challenges .The existing data protection mechanisms we are using today is good at preventing unauthorized data access but it fails to prevent attacks perpetrated by an insider to the server. A data theft attack is one of the security challenge now a days .Our approach is to protect the secret data with high security. The existing mechanism like encryption is not able to prevent the real data. So instead of encryption,a different approach to secure or protect insider data theft attack using decoy technology .This technology check data access and identify abnormal data access pattern. When the illegal users try to access is supposed and then confirmed using challenge question(security key),if an attacker enter a wrong key for the file ,then session will be log out and new password will be send to actual user .IP address and Picture of the victim will be captured and send to the actual user and the actual user also know which file the hacker attempt to open at which time and date .If user enter the correct key for question will get the right information.

INTRODUCTION

Much research in computer security has focused on the means of preventing unauthorized and illegitimate access to systems and information. Unfortunately, the most damaging malicious activity is the result of internal misuse within an organization, perhaps since far less attention has been focused inward. Despite classic internal operating system security mechanisms and the body of work on formal specification of security and access control policies, we still have an extensive insider attack problem. Indeed in many cases, formal security policies are incomplete and implicit or they are purposely ignored in order to get business goals accomplished. There seems to be little technology available to address the insider threat problem. Insider attack has overtaken viruses and worm attacks as the most reported security incident according to a report from the US Computer Security Institute. The annual Computer Crime and Security Survey for 2007 surveyed 494 security personnel members from US corporations and government agencies, finding that insider incidents were cited by 59

[1] Department of Information Technology, SNS College of Technology-Coimbatore, Tamilnadu, India.

percent of respondents, while only 52 percent said they had encountered a conventional virus in the previous year. The state-of-the-art seems to be still driven by forensics analysis after an attack, rather than technologies that prevent, detect, and deter insider attack. We define insider threats by differentiating between Masqueraders (attackers who impersonate another inside user) and Traitors (an inside attacker using their own legitimate credentials). One possible solution for masquerade detection involves anomaly detection . In this approach, users actions are profiled to form a baseline of normal behavior. Subsequent monitoring for abnormal behaviors that exhibit large deviations from this baseline signal a potential insider attack. The common strategy to prevent inside attacks involves policy based access control techniques to limit the scope of systems and information an insider is authorized to use, and hence ,limit the damage the organization may incur when an insider goes away. Prevention techniques may not always succeed, and thus, monitoring and detection techniques are needed when prevention fails. In this paper, we are focused on different techniques aimed at detecting masqueraders and traitors.

INTRODUCTION ABOUT SECURITY

Security is a principal consideration when planning, designing, implementing , and managing a network infrastructure. This is especially true for wireless LANs, which present a unique set of challenges to IT and security professionals. In addition to the typical problems that new network and device technologies engender, including incompatibilities and ongoing support issues, non-secure wireless LANs can expose an organization's network traffic and resources to unauthorized outsiders. Such individuals may capture data and exploit network-based resources, including Internet access, fax servers, and disk storage. More importantly, wireless access to a network can represent the entry point for various types of attacks, which can crash an entire network, render services unavailable, and potentially subject the organization to legal liabilities.

DECOY TECHNOLOGY: INTRODUCTION

Decoy Information technology works on the algorithm Key Hashed Message Authentication Code (HMAC). If the hacker gets the success to hack the username and password he tries to access the files but before that he has to cross one more barrier of security question which has been randomly set by the user. Even if the hacker tries and enters anything he gets the access to the account but the data displayed will be in the encrypted format. Here the terminology is that a key will be generated every time during entering the security question. This key will be matched every time the key generated during previous login will be matched with the key generated during next login. If the security question entered is correct then same key will be generated and will have access to the data but if the security question falls to be wrong then the key will not be same . This will prevent the unauthorized user to hack the data.

PROBLEM STATEMENT

The emerging computing technologies had significantly change the way we access and store millions of information .The increased rate of data accessed and stored have put forth several data security challenges The existing data protection mechanisms we are using today is good at preventing unauthorized data access but it fails to prevent attacks perpetrated by an insider to the server. The data security approach proposed here is for securing data in the server using a special mechanism called *"Offensive decoy technology"* .This technology uses decoy information (duplicate information set) to prevent the unauthorized access of original dataOnce an attack is noticed the attacker is provided with large amount of decoy information so the user's real data is secured from attackers access.

EXISTING SYSTEM

Existing data protection mechanisms such as encryption have failed in preventing data theft attacks, especially those perpetrated by an insider to the server. Much research in File security system has focused on ways of preventing unauthorized and illegitimate access to data by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise. There are encryption techniques to transmit the data securely over the network but they cannot stop the data access if user name and password are stolen. Security should be provided to users data even user names and passwords are stolen. To overcome this problem, there is a need of multi-level security. Even though there are Mobile verification technique and E-mail verification technique to validate the data access, those techniques are simply leaving the attackers. So, they are coming again with a new technique to attack. To reduce the attacks or to kill the resources of attacker, some more security protocols need to be implemented.

DISADVANTAGE OF EXISTING SYSTEM

- Previous research in File security System has focused on ways of preventing unauthorized and illegitimate access to data.
- Accomplished by developing sophisticated access control and encryption mechanisms. However these mechanisms have not been able to prevent data compromise.
- Various Mechanisms fail from time to time for a variety of reasons, including insider attacks, faulty implementations, and buggy code.
- User profiling is a well known Technique that can be applied here to model how, when, and how much a user accesses their information in the Cloud. But keeping data of huge number of users past information, practically does not work

PROPOSED SYSTEM

This proposed system is a completely different approach to securing the data using decoy information technology. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.In the system we develop whenever insider observed to be performing data theft, only then decoy file is created and is passed on to the requesting insider, whenever user trying to upload a file on the cloud user provide security key. The same security key appear when any user want to download or do any operation perform on the particular file . Incase insider tries to download the same file once again the usage of time stamp based key gives him a new decoy file as compared to the previous which will confuse him. This protects against the misuse of the users real data. The decoys, then serves two purposes:

(1) validating whether data access is authorized when abnormal information access is detected,

(2) confusing the attacker with bogus information.

A. Advantage of proposed system

- The basic idea is that we can limit the damage of stolen data and we can achieve this through a 'preventive' disinformation attack.
- We propose a completely different approach Picture of the victim will be captured and it is send to the alternate mail id.to securing the data using decoy information technology.
- We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data.
- Size of the files are not visible.
- Session will be expired when the attacker click the fake data.
- New password will be generated and it is send to the alternate mail id.
- IP address will be tracked.
- Picture of the victim will be captured and it is send to the alternate mail id.

PROJECT DESCRIPTION

Overview of the Project

The existing data protection mechanisms we are using today is good at preventing unauthorized data access but it fails to prevent attacks perpetrated by an insider to the server. A data theft attack is one of the security challenge now a days .Our approach is to protect the secret data with high security. The existing mechanism like encryption is not able to prevent the real data. So instead of encryption ,a different approach to secure or protect insider data theft attack using decoy technology .This technology check data access and identify abnormal data access pattern. When the illegal users try to access is supposed and then confirmed using challenge question(security key),if an attacker enter a wrong key for the file ,then session will be log out and new password will be send to actual user .IP address and Picture of the victim will be captured and send to the actual user and the actual user also know which file the hacker attempt to open at which time and date .If user enter the correct key for question will get right information

B. List of modules

- User Interface
- User Behaviour
- Chat Option
- Decoy documents
- Alerting System

MODULE DESCRIPTION

User Interface

User Registration Module provides functionality to register viewers of the learning site in order to get access to personalized content that the site using this module provides to its users. Module can be also used to register users for custom modules that support personalization and user specific handling. For example module can be used to get awareness from the users and updating the resources of learning based on the awareness. Updating the resources means adding some additional information based on the user request if it is a valuable one

User Behaviour

This system monitor data access in the server and detect abnormal data access patterns User profiling is a well known Technique that can be applied here to model how, when, and how much a user accesses their information in the server. Such 'normal user' behavior can be continuously checked to determine whether abnormal access to a user's information is occurring. This method of behavior-based security is commonly used in fraud detection applications. Such profiles would naturally include volumetric information, how many documents are typically read and how often. We monitor for abnormal search behaviors that exhibit deviations from the user baseline the correlation of search behavior anomaly detection with trap-based decoy files should provide stronger evidence of malfeasance, and therefore improve a detector's accuracy.

Chat Option

Transmission of text data between the two users is made possible when a connection is established between them. This option has been designed to make chat between two users. This option sends the regular text data when certain keywords are entered

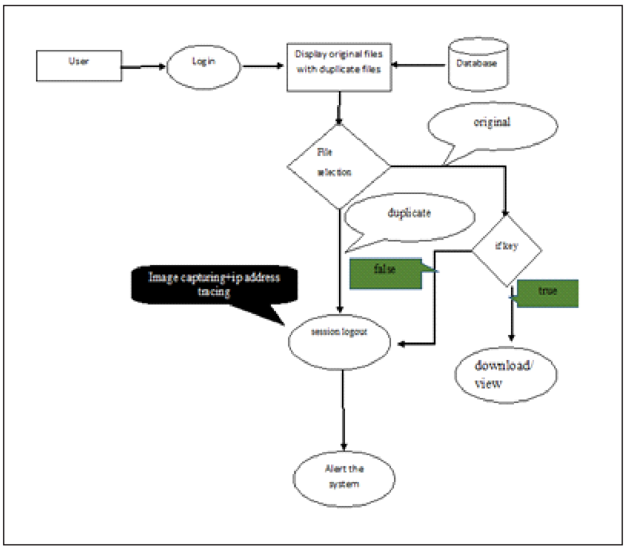
Decoy Documents

Proposed system has a different approach for securing data in the server using offensive decoy technology. We monitor data access in the cloud and detect abnormal data access patterns. we launch a disinformation attack by returning large amounts of decoy information to the attacker. This protects against the misuse of the user's real data. We use this technology to launch disinformation attacks against malicious insiders, preventing them from distinguishing the real sensitive customer data from fake worthless data the decoys, then, serve two purposes:(1) Validating whether data access is authorized when abnormal information access is detected(2) Confusing the attacker with bogus information

Alerting System

In this module, it reports about the attack to the actual users by sending the new password to the registered mail id. If any attack detection found, the system itself generate the new password for the hacked username and send that new password to the registered mail id. The old password gets deleted and expired, the hackers cant use the same password for entering into the system.

DATA FLOW DIAGRAM



CONCLUSION

This proposed novel approach to securing personal and business data in the Server. We propose monitoring data access patterns by profiling user behavior to determine if and when a malicious insider illegitimately accesses someone's documents in a service. Decoy documents stored in the Server alongside the user's real data also serve as sensors to detect illegitimate access. Once unauthorized data access or exposure is suspected, then session will be log out and new password will be send to actual user .IP address and Picture of the victim will be captured and send to the actual user and the actual user also know which file the hacker attempt to open at which time and date .If user enter the correct key for question will get right information

FUTURE WORK

The enhancement of the project is to give more security when even the outsiders enter inside the system. The extra security is provided by using the muti checking technique to solve the above problem and provide extra security. Honey pot technology can be used to track the attacker when he tried access the secret information

REFERENCES

1. Ben-Salem M., and Stolfo, Angelos D. Keromytis, "*Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud,"* IEEE symposium on security and privacy workshop (SPW) 2012. [2] "*Protect Sensitive Data in Public Cloud from an Theft Attack and detect Abnormal Client Behavior"* May2014
2. 1.Dnyanesh s. patil, 2.suyashs.patil, 3deepak p. pote, 4. nilesh v. koli Proceedings of 4th IRF International Conference, "*SECURED CLOUD COMPUTING WITH DECOY DOCUMENTS" at* Pune, 16th March-2014
3. Salvatore J. Stolfo, Malek Ben Salem, Angelos D.Keromytis, "Fog Computing Mitigating Inside Data TheftAttacks In The cloud",IEEE Base Paper, 2013
4. Etikala Aruna, Dr.Ch GVN Prasad, A. Malla Reddy Issue 9,*Securing the cloud using Decoy Information Technology to preventing them from distinguishing the Real Sensitive data from fake Worthless data*, September 2013
5. *Minimizing Internal Data Theft in Cloud Through Disinformation Attacks* P.Jyothi1, R.Anuradha2, Dr.Y.Vijayalata3 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 9, September 2013
6. V.Sriharsha Student , Dept.of CSE SNIST, Ghatkesar, India V.Prabhaker Dept.of CSE. SNIST, Ghatkesar, India N.Krishna Chythanya SVSIT, Warangal, India "Dynamic *Decoy File Usage to Protect from malicious insider for data on public cloud"* International Journal of Advanced Engineering and Global Technology Vol-1, Issue-3, October 2013
7. The Telegraph. 'Boozing Brits' losework devices when drinking. (2013)
8. CERT Insider Threat Team. Unintentional insider threats: Afoundational study. (2013).
9. Madhusri.K,Navneet. " *Fog Computing: Detecting Malicious Attacks in a cloud* international Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013
10. D. M. Cappelli, A. P. Moore, and R. F. Trzeciak, *The CERT Guide toInsider Threats: How to Prevent, Detect, and Respond to InformationTechnology Crimes*, 1st ed. Addison-Wesley Professional, 2012.
11. SC Magazine. Danger within: Insider threat. (2012)

12. R Richardson, "CSI computer crime & security survey,"(last viewed March 2011),

13. BBC News. (2011) Former Olympus boss Woodford blows whistle oncompany.

14. FBI. (2010) Fannie Mae corporate intruder sentenced to over threeyears in prison for attempting to wipe out Fannie Mae financialdata.

15. Cloud Security Alliance, "Top Threat *to Cloud Computing V1.0," March 2010*

16. M. Arrington, "*In our inbox: Hundreds of confidential twitter documents,*" July 2009.

17. IDC. (2009) Insider risk management

18. C P Pfleeger, *Reflections on the Insider Threat*. Springer, 2008.

IJERST

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991
01
9 772319 599001