INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

THREE LEVEL AUTHENTICATION SCHEME FOR PREVENTION OF INTERNAL INFORMATION LEAKAGE

MR. VIPIN R. KHAWALE

ME (CE) Final Year, PRMCEAM, Badnera.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract: This chapter introduces the 3-level authentication technique to prevent internal information leakage in network system. When system authenticates users, it requires user's ID&P/W firstly. Then, it requires a secondary authentication component to check whether he/she is legitimate user. By doing so, it can implement a more robust authentication system. So, there is no risk because it never exposes or copies. This is also providing the access privilege to the system. The generation of 3-level authentication passwords generated by own random password generation algorithm. Every password in 3-level authentication password is different for every Id only the second password is same for Id's in same project employees.

Keywords: Authentication, Information Leakage, Access Privilege.

PAPER-QR CODE

Corresponding Author: MR. VIPIN R. KHAWALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Vipin R. Khawale, IJPRET, 2016; Volume 4 (9): 1125-1130

INTRODUCTION

2012 cyber security watch survey [1] said that 51% of respondents answered damage caused by insider attacks more damaging than outsider attacks. Top-10 guide for protecting sensitive data from malicious insiders [2] also said that database security is one of the most important areas for critical data protection from insiders because it saves the attractive data insiders want. Insiders are capable of saving data in USB memory stick and their portable disk, and they can illegally use the data for people who need it. Most security techniques are focused on detects information leakage from outside, not necessarily by insiders. When user tries to access database, system checks user's identity. It is an authentication. Authentication techniques prevent forgery and unauthorized access as well as identity check. In the first, the common authentication approach is the use of passwords. But, as password has been used for a long time, it is possible to copy by hacker [3]. In that order, smart card appears to resolve security problem of password in a secondary authentication techniques. This also proved to be vulnerable to attack impersonation attack [4]. Nowadays, we are using human factors as reliable authentication components. Human factors include iris, face, fingerprint, etc. Authentication by biometric information is automated method of verifying or identifying the identity of user physical characteristics [5].

II. RELATED WORKS

The aspects of internal information leakage:

Insiders can access database with legitimate

Access authorization. When insider's misuse their authorization to leak internal information from database, it is not easy to detect his/her behavioral anomalies. Internal information leakage caused by insiders is considered the most critical risk to organization. The reason of information leakage by insiders is that they have a legitimate access authorization to database and can bypass logical & physical security systems. And they know well ID&P/W to log-in at database, security systems and the main location of sensitive data. Recently, in Korea, three of the country's major credit card firms are stolen personal information of tens of millions of their customers. The thief was authorized by the firms to access the database. He accessed the card firm's network system and simply copied the data to a USB stick when he worked as a dispatch duty in 3 card firms. The following table shows the examples of data leakage by insiders in Republic of Korea [6].

It is difficult to predict internal information leakage by insider because it happened by insider with legitimate access authorization. Also, information leakage by insider can't be detected accurately because it is not easy to perceive it. The path of information leakage by insiders is variable as following figure:

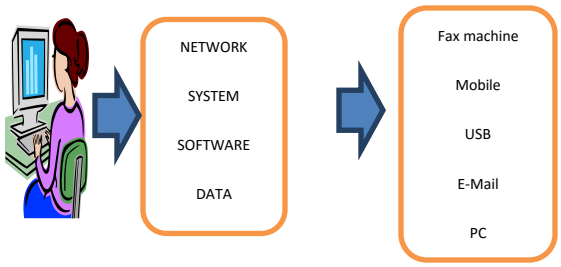

Fig 1.1 the Path of Information Leakage by Insider

TABLE 1. THE LEAKAGE CASES OF INTERNAL INFORMATION

Date	Financial Company	Criminal	Leakage Information	Path
Apr. 2013	Citibank	Local Employee	Personal Information Of 34,000 user	Printed Paper
Feb. 2012	Standard Chartered Bank	Subcontractor employee	Personal Information Of 1,00,000 user	Access database
Feb 2012	Meritz Fire & Marine Insurance	Employee	Personal Information Of 1,64,000 user	E-mail and USB
Jun. 2011	NH NongHyup Securities	Hacker	Personal Information Of 15,000 user	Program Error
May 2011	Leading Investment Securities	Hacker	Personal Information Of 12,000 user	Homepage Hacking

This table shows us the internal information Leakage cases happened in financial companies by hackers by dates.

3-LEVEL AUTHNTIVATION MECHNISM

Three Level authentication process

The concept of proposed 3- level authentication mechanism monitors insider's generated passwords when Id's

Tries to operate a critical data in database and compares measured insider's passwords in Real time with stored the normal boundary of passwords in password management database. If measure value passwords are out of normal boundary, system checks status of insider's operation. If the change of passwords related to insider's abnormal behavior, it alerts to security manager, and deny requested operation.

Our proposed system composes of user monitors, passwords analysis module, authentication module, and passwords management database:

User Monitor: monitors behavior relater to data leakage such as critical data copy, uploading, and prints, etc. Critical data are determined by the security policy, and monitoring is done by hooking the main system call.

Password Analysis Module: Detect suspicious behavior as comparing and analyzing the collected value of insider's conductivity with his/her normal value stored in a database when received passwords from Id's. It performs the 3 function such as sensor monitor, analysis, and D/B manager. A sensor monitors periodically calls insider's the value of conductivity by Id's and generates the normal value of passwords conductivity after collected insider's conductivity for some months. An analysis function compares the value of conductivity received from sensor monitor with insider's normal values in database, and if the value of

Collected conductivity is out of normal boundary, it determines the probability of data leakage. D/B manager manages and decides the normal values of insider's conductivity, using data stored in database as the initial value. If there is no data stored in password management D/B, it measures the value of insider's conductivity to set normal value.

Authentication Module: Determines whether insider requested operation will allow or not. The change of insider's passwords conductivity is used as an indicator for identifying the potential data leakage. If it receives that the measured value is different from the normal value of conductivity from passwords analysis module, it reject the operation requested by an insider. And then, it report to security manager.

Passwords Management Database: Stores the normal value of insider's passwords conductivity and normal boundary of insider's conductivity changes regulated leakage possibility.

Password Generation Algorithm:

In this password generation algorithm there are three random passwords are generated. These are SA (Organization/ Institute Password), TA (Project/ Team Password) and PA (Privileged Access). The steps for how to generate these three passwords at random are as Follow:

First of all at the time of generation of three random passwords Admin Takes 10 char random user text this is generated by system automatically. Then

Generation of SA:

SA= Starting 3 char of (MD5 of (Random user text))

Generation of TA:

TA= Starting 3 char of (MD5 of (Project Name)) + Last 1 char of (MD5 of (Project Name))

Note: This Password is same for all Ids' in same project.

Generation of PA:

PA= Starting 3 char of (MD5 of (SA+TA+ Access right)).

IV. CONCLUSION

In this paper, we proposed 3-level authentication mechanism using passwords generation algorithm. Insider enters his/her ID&P/W when he/she access to company network system. Next step, insider sends his/her passwords information for accessing server stored critical data to authentication server. Last step, when insider tries to operate on critical data, third authentication mechanism detects abnormal behavior of insider. In other words, we applied insider's unique authentication mechanism which detects whether he/she tries to leak internal critical information illegally.

Our proposed authentication mechanism monitors insider's passwords conductivity when he/she tries to operate critical data in database, and compares measured insider's passwords conductivity in real time with stored the acceptable boundary of passwords conductivity in password management database. If measured value of passwords conductivity is

Out of acceptable boundary, system checks the status of insider's operation and alerts to security manager, and then denies requested operation.

In future, we will consider adding other biometrics signals to third authentication elements for improving FAR (False Accept Rate) and FRR (False Reject Rate).

REFERENCES:

1. "Top-10 Guide for Protecting Sensitive data From Malacius insiders", Imperva White paper, iMPERVA, 2009.
2. Carnegie Mellon University, "2012 Cyber Security Watch Survey", Sof. Engg. Ins., 2013.
3. James Wayman,et. al, "An Introduction to Biometric Authentication Systems", Springer Biometric System, pp.1-20, 2005.
4. Jung ho Eom, "The Quantitative Evaluation of a Level of Insider Activity using SFI Analysis Techniques", Journal of Security Engineering, Vol.10. No.2, pp.113-122, 2013.
5. Reetu Awasthi and R.A.Ingolikar, "A Study of Biometrics Security System", International Journal of Innovative Research & Development, Vol.2, Issue 4, pp.737-760, 2013.
6. F. Fatemi Moghaddam, Secure Cloud Computing with Client-Based Control System: Protection of Stored Cloud-Based Data by Increasing End-User's Role, Chapter 1: Cloud Computing, 1st Edition. Saarbrücken: Lambert Academic Publishing (LAP), 2013, pp. 9-2.
7. A.J. Choudhury, P. Kumar, M. Sain, L. Hyotaek, and H. Jae-Lee, "A Strong User Authentication Framework for Cloud Computing," in Proc. IEEE Asia-Pacific Services Computing Conference (APSCC), Jeju Island, South Korea, 2011, pp.110-115.
8. I-En Liao, Cheng-Chi Lee, and Min-Shiang Hwang, "A Password Authentication Scheme over Insecure Networks," Journal of Computer System, vol. 72, no. 4, pp. 727-740, 2006.
9. M. Scott, "Cryptanalysis of an Id-Based Password Authentication Scheme using Smart Cards and Fingerprints," ACM SIGOPS Operating Systems Review, vol. 38, no. 2, pp. 73-75, April 2004.
10. B. Wang, J.H. Li, and Z.P. Tong, "Cryptanalysis of an Enhanced Timestamp-Based Password Authentication Scheme," Elsevier Journal of Computers & Security, vol. 22, no. 7, pp. 643-645, October 2003.