International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

Windows Growing Security

Vishal Mali[1], Lakhan Jadhav[2], Namdev Chame[3], Prashant Inje[4]

[1]*Vishal Mali, Dept. Of Computer Engineering, MIT PUNE, Maharashtra, India*
[2]*Lakhan Jadhav, Dept. Of Computer Engineering, MIT PUNE, Maharashtra, India*
[3]*Namdev Chame, Dept. Of Computer Engineering, MIT PUNE, Maharashtra, India*
[4]*Prashant Inje, Dept. Of Computer Engineering, MIT PUNE, Maharashtra, India*

Abstract - *Application Lock is unique type of system which can be developed to secure the applications installed in the computers. Using this system, user can restrict unauthorized access from using systems installed applications. The idea is to lock and unlock the installed applications in the computer system. We are using Windows Registry for implementation of Application Lock for Windows Operating System. By changing the registry values we can deny access to particular application or features like USB, Control Panel, Registry itself can be denied from unauthorized users. For making access control more powerful we are using two levels of authentications i.e. Image Password and Text Password.*

Key Words: **Dual Level Security, USB Lock, Application Lock**

1. INTRODUCTION

In windows operating systems, one who know your computer password, can use any application installed in it. There is few way in operating system to restrict a person form using the applications in your computer, but not sufficient to provide strong security access. The proposed windows growing security system make users system more secure. For e.g. if you want to secure software like ISM, it is a very important software used in Government sectors like TAHSIL, ZP OFFICES and COURTS can be locked by using this proposed systems lock feature, and only authorized user can use this software. Windows Registry provides a convenient way to denied applications in the system. The registry is nothing but a central place to store all settings on the computer machine. While a program doesn't have to store any data in the registry, it is free to if it likes. It is like the configuration files for Linux and Unix, but rather than being stored in folders, it is stored in hives, a folder like structure. The proposed system contains a dual password system such as Image and Text password for security purpose. Using this system user can perform following functions

1. Lock / Unlock system applications.
2. Lock / Unlock user applications
3. Lock / Unlock USB drives
4. Enable / Disable control panel
5. Enable / Disable components in Control panel
6. Getting all the relevant information about operating system, motherboard, processor, etc.
7. Locking the some features that provided by operating system like control panel, task manager.

The ultimate goal of this proposed system is to increase the security level of user sensitive application and restrict unauthorized access to the user's sensitive application. The main feature of this system is having the double level of authentication process for user to determine as the authorized user.

2. PROPOSED SYSTEM

From the current problem section, it is noticed that, existing application lockers for windows operating system are insufficient to provide both the system as well as user application locking facilities also they lack in providing strong access control mechanism. To solve these problems, we propose to implement our Application lock system. It mainly provides facilities for locking or unlocking system as well as user applications. It also provides interactive GUI to deal with system. Additionally by focusing on Windows Registry facilities we are also providing access control for USB Lock, Control Panel, and Windows Registry. For making

authentication stronger dual level security of Text password and Image Password is used. If they make success over text password then only they can go for image password and after that they can access the system.

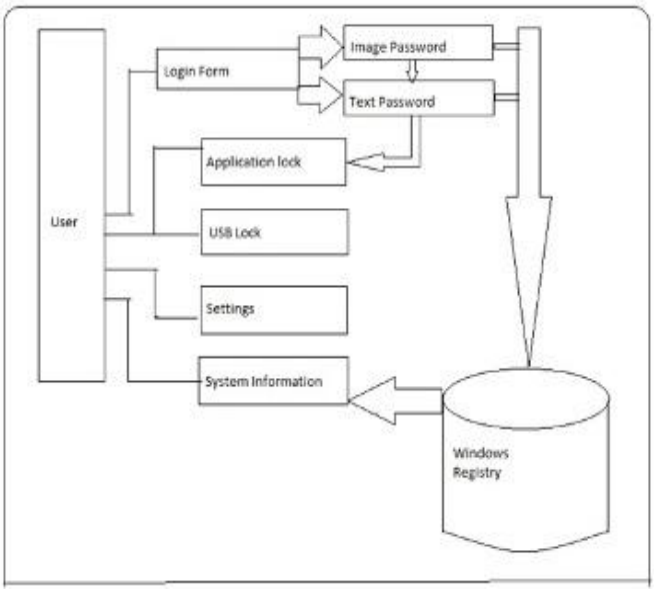

Fig -1: System Architecture

2.1 Windows Registry

Windows registry is a central point of information about all aspect of the computers i.e. it's hardware, operating system, applications and users. Windows 9x/ME, Windows CE, Windows NT/2000/XP/2003 stores configuration information and data in Windows registry. It is a central repository for configuration data that is stored in well arranged manner. System, users, applications in Windows make use of the windows registry to store their configuration information and it is continuously accessed for reference during their operation. The registry is used to replace configuration files which mostly are text-based and used in Windows 3.x and MS-DOS, such as autoexec.bat, .ini files and config.sys files. Due to the huge amount of information stored in Windows registry, the registry can be the source for potential evidential data. We are using Windows registry as a central database to our system.

2.2 Image and Text password

Image password is a first authentication step in this system. A grid of set of images is provided to user and user has choice to select appropriate sequence of images. If user cracks image password then another level of text password authentication is will be there. Text password is a second level of authentication. Image password and text password will get validated against the original passwords stored in windows registry, if they match then only user can have access to the system. If neither of the passwords matches, user is provided with three chances to enter password again, if user fails again then system will simply shutdown.

3. TECHNICAL ASPECTS

Proposed system need to deal with windows registry for providing restriction on user as well as system application. It basically consist five types of HKEY classes, which can perform quality role in proposed system.

a. HKEY_CLASSES_ROOT

This particular class will store all the relevant and important information of user. Hence information stored in registry can be used to face future problems like password recovery, changing user personal information etc.

b. HKEY_CURRENT_USER

This class helps application vendor to provide restriction on system and user software. "Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\policies\Explore\DisallowRun". This is a path in windows registry where developer can create specific key for performing particular kind of operation in windows system.

4. FLOW GRAPHS

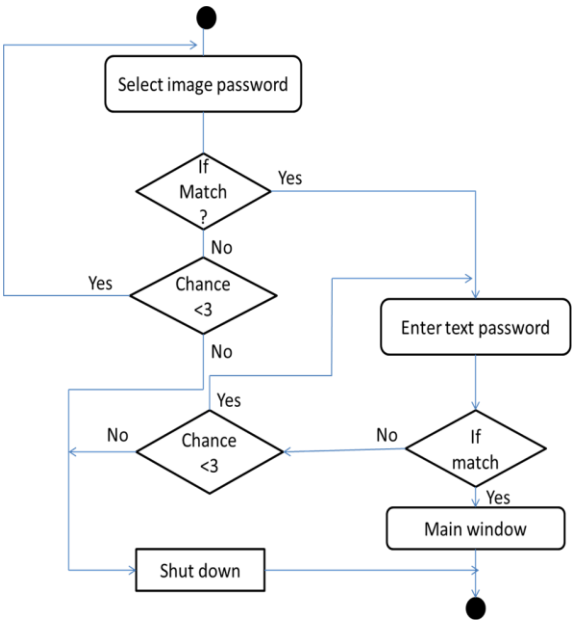

Fig -4: Flow Diagram for authentication process

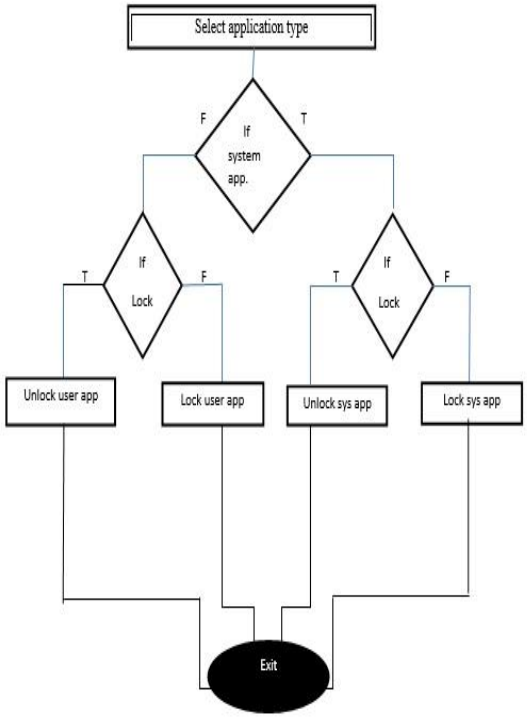

Fig -5: Flow Diagram for authentication lock

5. FUTURE SCOPE

Further enhancements can be done to the application lock like it can be fully compatible with UNIX like operating system but in that scenario windows registry must be replaced with UNIX file system. Also to identify particular user individually authentication mechanisms like face recognition or speech recognition can be used to increase the security level. Along with application lock features like folder lock or file lock can also be implemented. Password recovery system could be made more user-friendly.

6. CONCLUSION

This paper mainly focuses on security issues of windows operating system application in terms of access prevention for an unauthorized user. As windows registry is a one kind of secure place for storing user credentials information and all kind of system software, hardware and user application's of system. As well as use of dual layer security mechanism makes it more robust. Preventing access on some hardware part and system inbuilt routine increase security of windows system.

REFERENCES

[1] Juan-hua, Zhu; Ang, Wu; Kai, Guo, " PC Lock Software Design Based On Removable Storage Device and Dynamic Password" , 2nd International Conference on Computer Engineering and Technology Journal VOL. 3, year 2010.

[2] Rajkumar Janakiraman, Sandeep Kumar, Sheng Zhang, Terence Sim, "Using Continuous Face Verification to Improve Desktop Security", Seventh IEEE Workshop on Applications of Computer Vision, (WACV/MOTION'05).

[3] Brendan Dolan-Gavitt, (May,2008), "Forensic analysis of the Windows registry in memory", MITRE Corporation, 202 Burlington Road, Bedford, MA, USA.

[4] WANG Jing, SUN Chao-yi, FENO Li, ZHOU Ti (ICCASM 2010), "Research on Anomaly Behavior Blocking Method for Desktop Security", presented at computer application and System Modeling (ICCASM), 2010 International confererence on at (VOLUME,4).

[5] Lih WernWong, "Forensic Analysis of the Windows Registry", School of Computer and information science Edith Cowan University.

[6] Haoyang Xie, Keyu Jiang, Xiaohong Yuan, Hongbiao Zeng, (March 2012), "FORENSIC ANALYSIS OF WINDOWS REGISTRY AGAINST INTRUSION", International Journal of Network Security & Its Applications (IJNSA), Vol.4.

[7] Derrick J. Farmer, "A FORENSIC ANALYSIS OF THE WINDOWS REGISTRY", Champlain College Burlington, Vermont.

[8] Tao Feng, Zhimin Gao,Boumber D. Tzu-Hua Liu,DeSalvo, N.Xi Zhao,Weidong Shi, "USR: Enabling Identity Awareness and Usable App Access Control During Hand-free Mobile Interactions", Published in: 6th International Conference on Mobile Computing, Applications and Services on 6-7 Nov. 2014, Publisher: IEEE.