IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 6, Ver. III (Nov – Dec. 2015), PP 71-73
www.iosrjournals.org

Secure System Password (SSP) Application for NT Editor Hacking Tool

T.Sethupathy, P.Veni, S. Selwin Joseph, C. Sathya
[1,2,3]*Final Year/Dept of CSE SNS College of Technology Coimbatore-35*
[4]*Assistant Professor/CSE SNS College of Technology* Coimbatore-35

Abstract: *In windows, the password will be stored in SAM registry by default. This SAM registry hides the windows password when the system is in ON state. The password in SAM registry will be cleared or changed by using NT Editor Tool. So that data can be accessed by any user. Security for the windows will be done by the proposed system as an application. If the user wants to install new OS then the data in the hard disk will be encrypted for prevention of unauthorized access. The application will be start monitoring to avoid password re-modification or clearing the password. Features in this application is, if the user hacks the application password, SSP does not allow the users to access USB, Ethernet and CD/DVD drive. Application will stop the access of the driver ports, until it is re-installed or the password is set right.*
Keywords*: Hacking, NT Editor Tool, SAM Register, Data encryption.*

I. Introduction:

Hacking is the act of manipulating computers to get them to do exactly what you want [1]. A hacker is the person who does the hacking. A hacker is generally defined as someone who is very good with computers and programming [2]. However, in popular culture, a hacker is considered someone who attempts to break into computer systems.

The Security Account Manager (SAM) is a database file[3] inOperating System that stores users' passwords. It can be used to authenticate local and remote users. The Security Account Manager (SAM) is a database[4] present on servers running Windows Server 2003 that stores user accounts and security descriptors for users on the local computer.

Offline NT Password & Registry Editor[5] is a free Linux-based utility, which as the name suggests, works offline. The code creates its own boot environment. Once you burn the ISO image to a CD-ROM, you'll have a tool at your disposal for resetting Windows NT, 2000, XP and Vista account passwords. You won't even have to know any of the current account user names or passwords on the system to make it work.

The Data encryption is the act of changing electronic information into an unreadable state by using algorithms or ciphers. The cryptosystem which is most used throughout the world for protecting information is the Data Encryption [6] Standard (DES) which was announced by the National Bureau of Standard (NBS). The DES must be stronger than the other cryptosystems in its security.

II. System Analysis:

3.1 Existing system:

In windows, the password will be stored in SAM registry by default which is placed in windows program files. This SAM registry hides the password from other user and admin too. This secures the password of windows but only after the operating system turns ON.

But the password in the SAM registry gets clear or can be changed by using NT Editor Tool. This will be called as NT Editor hacking mechanism. This tool will be activated before an operating system turns ON. Using this NT Editor tool the password can be easily modified or cleared. From this the other user can easily enter into the system, access it and retrieve data. To avoid the NT Editor hacking, SSP application has been proposed to secure the windows password.

3.2 Proposed System

Step 1: Security Check-Installation of New OS will encrypt the data found in the hard disk**.**
Step 2:SSP Application starts from installation process. In the installation process, the user has a circle provided by the application to select (Fig 3.2.1) the position for drawing patterns. In this circle the user has to mark (Fig 3.2.2) the points around it to draw patterns. All the points in the circle may or may not be covered for creating patterns. Same pattern has to be given twice (Fig 3.2.3) for confirmation and the verification will be done after the system has been restarted. This security pattern decreases the probability to crack the password by the hacker.

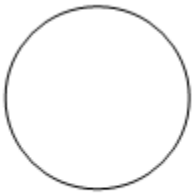


Fig 3.2.1

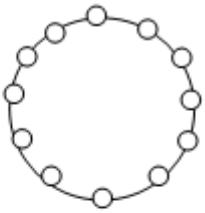


Fig 3.2.2

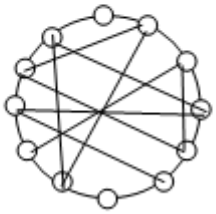


Fig 3.2.3 Security Pattern

3.3 Working Process:

3.3.1 Security Check starts when the user tries to install New OS. This will encrypt the data found in the hard disk**.**

3.3.2 SSP application should be placed before the operating system is being started by the BIOS.

3.3.3 SSP application contains the lock patterns as well as some additional functions for security issues.

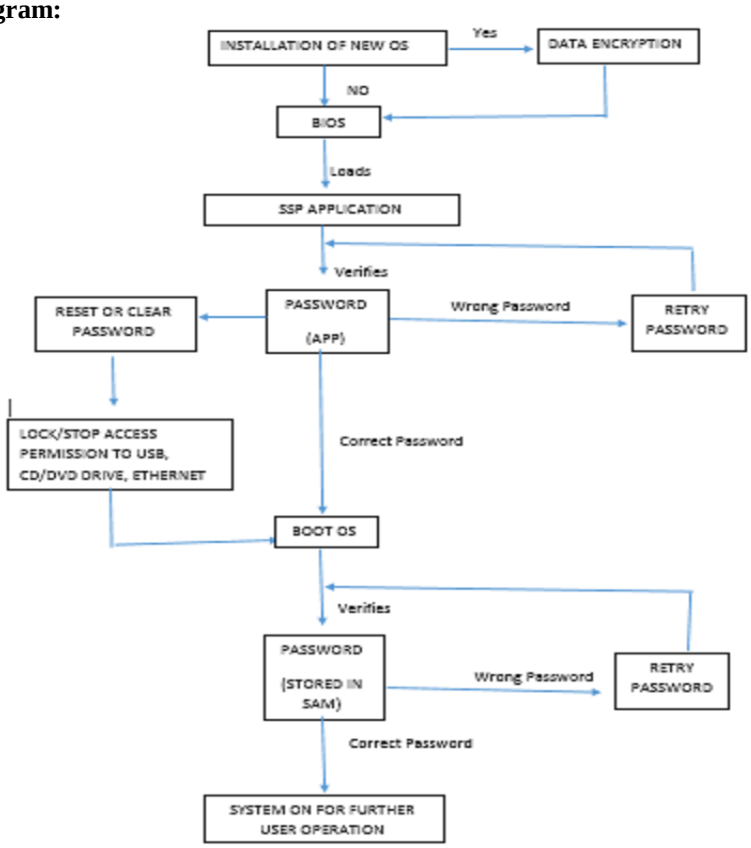
3.3.4 In this application, if the password for this lock is modified or cleared then the applicationwill cancel the access permission for USB and CD or DVD drive.So that the user cannot mount the tool to clear the password which is stored in SAM registry.

3.3.5 Two tier security is provided for data protection and various hacking technologies.

3.4 Work Flow Diagram:

After installation, for each and every time while power on the system or laptop the process goes on like this flow.

3.4.1Process Diagram:



References:

[1]. http://wiki.cas.mcmaster.ca/index.php/Operating_Systems_Security
[2]. http://searchsecurity.techtarget.com/definition/hacker
[3]. https://en.wikipedia.org/wiki/Security_Account_Manager#cite_note-1
[4]. https://technet.microsoft.com/en-us/library/cc756748(v=ws.10).aspx
[5]. http://www.techrepublic.com/blog/windows-and-office/reset-lost-windows-passwords-with-offline-registry-editor/
[6]. http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=563518