USB based Dynamic Authentication Alert System for Computers

Chandra J.
Associate Professor,
Department of Computer Science,
Christ University,
Bangalore, Karnataka, India

Shreya Nag
Student,
M.Sc. Computer Science
Department of Computer Science
Christ University,
Bangalore, Karnataka, India

ABSTRACT
In the present work, an innovative mechanism to convert a USB drive into a key has been introduced. A unique key file is written on to the drive which acts as the authentication mechanism to access the user's computer. This device can be used to lock or unlock the system by simply removing or attaching it. The current session is not hampered even though the system is secure and cannot be accessed without the specific USB drive. To further improve security, the key file contents are rewritten after a set time interval, to preserve the security even if the drive is lost. In absence of the USB drive, the user can gain access by entering the master password. A particular system might have more than one USB keys as well, and a key can be used to access multiple systems. This mechanism was then coded into a deliverable software which implemented all the security features including possible intrusion detections and alerts. The advantage of this mechanism is that it is a faster and efficient way to temporarily pause the current session of a system without having to log out. It is most suitable for workplace workstations as well as for desktops, personal computers and laptops. There is, however, scope to improve the current method add incorporate more features.

General Terms
USB authorization, Security locks Windows Operating System, Intrusion Detection of Personal Computer.

Keywords
Windows Security, USB Bases Authentication, Lock, MD5 Hash, Intrusion Detection, Personal Computer, User Verification.

1. INTRODUCTION
USB storage devices have emerged as the primary solution for mass transfer of data from one computer to another. Other than that they can also be used to clone drives, create bootable devices to install Operating Systems etc. Another such usability which has recently surfaced is to use USB flash drives to lock Personal Computers or Laptops in lieu of physical keys.

Access to computers in most households or organizations needs to be restricted to ensure security. Usually such authentication is achieved by a combination of username and password unique to each user.

However, this system has two drawbacks. Anyone having the combination can access the computer leaving it vulnerable. Also, a number of surveys such as Global Password Usage Survey and PC World Piracy Survey report that almost 35% of users never change their passwords [1].

Dynamic authentication goes a long way to eradicate these drawbacks as it updates the login credentials at specific time intervals, making it more secure. Alert mechanism is also implemented along with authentication systems to generated auto alerts for unauthorized access attempts.

2. RELATED WORKS
Many such efforts to use USB devices as authentication tools have emerged in the recent past. Different techniques have been developed to use USB devices as a security device in both standalone and distributed systems.

In a paper by Zhihui Liu et al. [2], he established an identity authentication scheme based on USB Key for Trusted Network Connect to eradicate the limitation in identity authentication. He observed that device authentication is not same as user authentication and thus proposed a unique USB based system which served as user authentication, thus granting access to application servers.

Another effort to make network authentication secure and reliable was suggested by Yu Jin-wei in his paper [3], which proposed a logical system based on USB key and showed the process of network authentication via the same.

In a similar work by Tao Yizheng et al. [4], the weak security of conventional and single authentication is analyzed and the dual-factor authentication system based on PIN authentication and the hardware USB Key digital certificate authentication is designed.

However, all these approaches mainly focused on networked based authentication in a client server model which, albeit effective, are incompatible in a personal computer or common workplace terminal scenario. Significant progress in that area was made by Jiang Yu in his paper on a USB based strong password authentication scheme [5]. He recommended an authentication scheme which advocated the use of a USB-Key to verify the user's password and store the security parameter in the USB itself.

3. METHODOLOGY
Most research towards dynamic authentication mechanisms mainly focuses on network based authentication in a client server model, utilizing one-time password authentication. Also, traditional security systems for PCs has only device authentication or static password authentication, which can be easily copied or decrypted, as pointed out by Zhu Juan-hua et al. in his paper about Personal Computer locking software design based on removable storage device. The author proposed a software design which would utilize the MD5 hashing algorithm and store the pass key in a removable device. It would thus provide a unique key, and only knowing the hash key would not grant access to the protected computer. Also, the two factor authentication of equipment

certification along with the MD5 hashed password would make it immune to brute force attacks.

The proposed work demonstrates the design of a software framework which is an improvement over this current system. The proposed software, when installed allows the user to convert a simple USB flash drive into a unique key by creating a MD5 hash of the MAC address of the system. This USB device can be used to lock or unlock the user's computer without hampering the current Windows session. The user can use the computer normally when the flash drive is plugged in. However when the USB flash drive is removed, the computer will be automatically locked down.

The proposed software framework is depicted by the figure below:

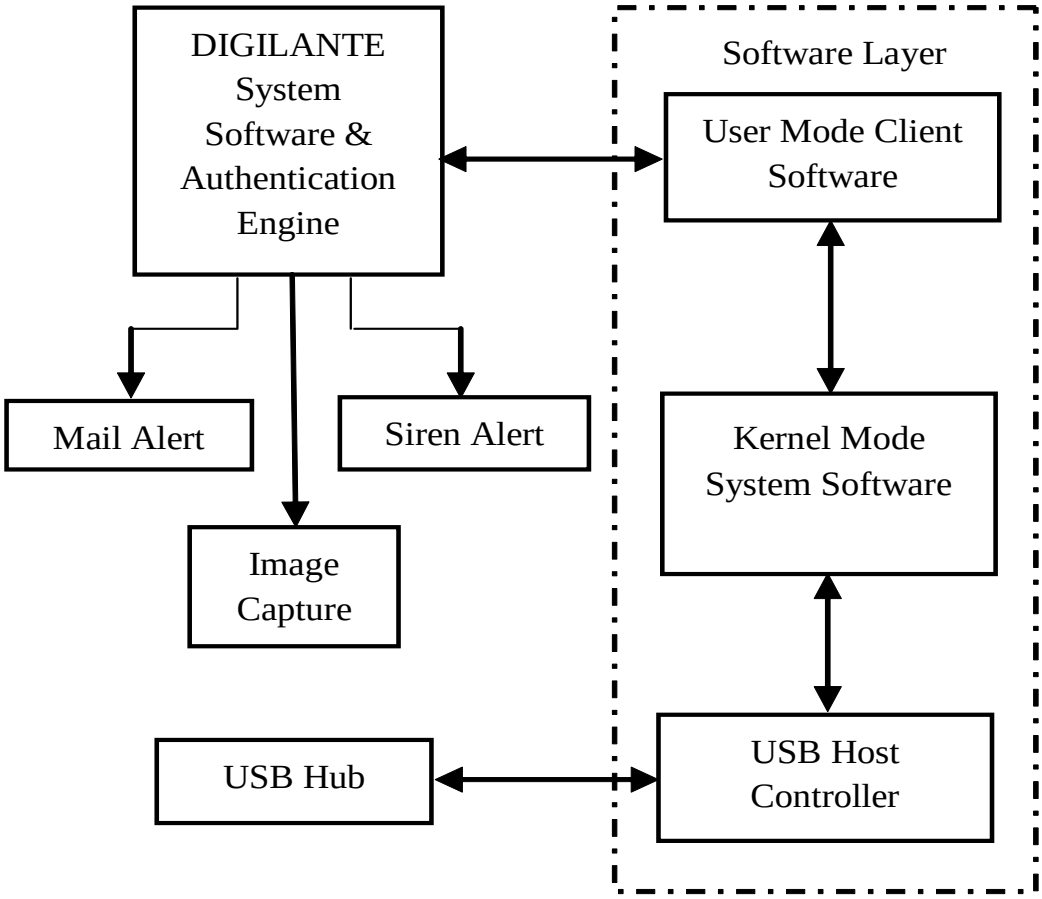

Figure 1 : Proposed Framework for Dynamic Authentication System

The suggested architecture consists of four major modules –

1) USB recognition, unique key generation and authentication
2) Log file handling and event recording
3) Intrusion detection and alert system
4) Key revoking system

The first module takes care of identifying the USB devices attached to a particular system and creating a unique MD5 hash and storing it in the device. It also introduces an enhanced security measure - dynamic MD5 hash password. It can be achieved by rehashing the password in the key file recursively after a set time interval. The MD5 hash would significantly increase the security level. Also, the two factor authentication mechanism of PnP device ID and the key file would be implemented in the key revoking system.

On removing the USB key, the proposed methodology suggests performing the following steps to ensure system lockdown:

1) Hide desktop icons and taskbar
2) Minimize open windows
3) Disable Task Manager
4) Disable keyboard and mouse
5) Turn off monitor

When the USB key is connected, the software would authenticate the drive and, the changes would be rolled back to unlock the system.

The Log files module is designed to maintain the color coded log for all the events such as unique USB key creation, key detection and removal, key revoking etc. There would be provisions to view the log file within the software or to export it in PDF format.

The intrusion detection module implements measures to detect unauthorized access. On account of loss of the USB key, there should be provisions to unlock the computer by using a secret hotkey and supplying the master password. The alert process needs to be timed and in case a wrong password is entered or time runs out, an alarm would be sounded to alert the user. Also, the snapshot of the intruder would be captured from the webcam and sent to the user's pre-configured email address for identification.

The key revoking system allows the user to revoke a key from the list of created ones in case the key is lost or just needs to be changed. The maximum number of keys for a particular

system would be limited and all of them can be removed at one go from this module.

Finally, there would be a separate settings module for the user to change the default time intervals, the features that needs to be activated and the receiver email settings.

The framework suggested would enhance the security provided and also adds a number of advanced features such as dynamic passkey, system lockdown by disabling input devices and an efficient intrusion detection system which would capture a snapshot of the intruder during unauthorized access.

The proposed framework was developed based on this architecture using Visual Studio (VB.NET) incorporating the suggested features and tested in different functional environments.

4. RESULTS AND DISCUSSIONS

When the software is run for the first time, it detects all the attached USB devices and lists them. Maximum number of USB keys for a particular system is however limited to 5.

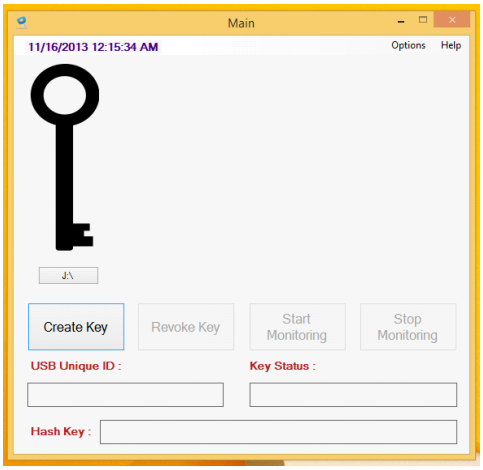

Figure 2 : Digilanté Main User Interface

When a particular device is selected, the MAC address of the system is hashed using the MD5 algorithm and stored in the USB device within a custom file generated by the software.

The hash key, coupled with the PnP ID of the USB device is stored within the software.

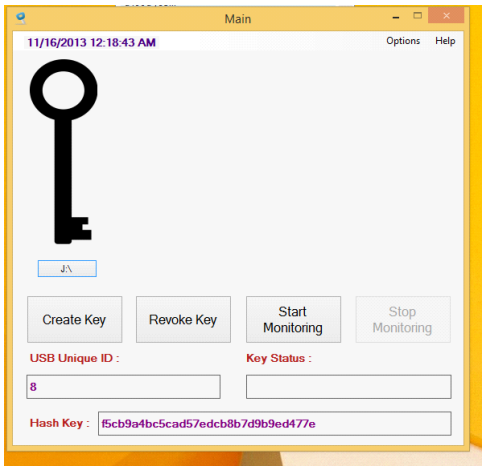

Figure 3 : Key Creation

When the monitoring process is started, the software keeps scanning for attached devices at regular intervals. If it matches with the list of PnP IDs stored within the software, it then checks for the key file. If found, it matches the contents of the file with the hash keys stored within the software. A match signifies a genuine key and thus the system functions properly.

Upon disconnecting the USB key, on the next scan for the USB devices of the software, it detects that the key has been removed. It then executes a module which changes the registry key values corresponding to the mouse, thus disabling it.

Figure 4 : Monitoring Started

It also disables the keyboard and the display by calling system functions and passing appropriate messages corresponding to these commands. The system is thus rendered unusable by removing the secure USB key while perfectly maintaining the current session. When the USB key is connected again, the changes are rolled back and the session becomes active.

In the event of loss of the USB key, the computer can be unlocked by first interrupting the keyboard disable feature using ”Ctrl+Alt+Del” and then using a secret hotkey to open a timed prompt for the master password, which is set to a default password, which can be changed from the settings module. A correct master password entry unlocks the computer and suggests the user to create a new key.

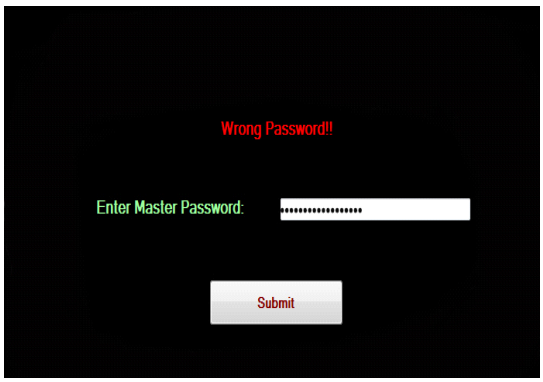

Figure 5 : Master Password Prompt

If any unauthorized person gets hold of the secret hotkey and then fails to supply a master password, or gives a wrong password, an audible alarm is sounded to alert the user of a possible intrusion. It also takes a snapshot of the intruder via webcam and mails it to the user in a specified e-mail address.

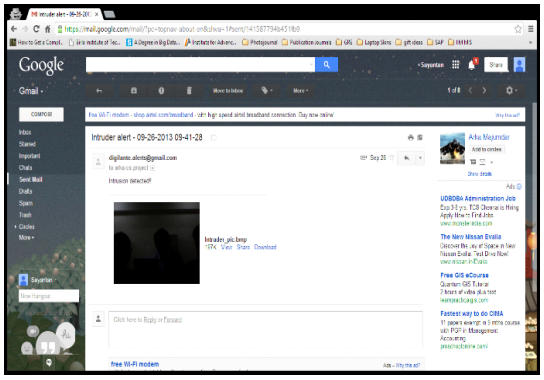

Figure 6 : Intrusion Alert e-mailed by Digilanté

A log is also maintained storing information regarding the activation and deactivation of the USB key as well as such intrusion events for reference.

Any key registered for a particular system can also be revoked from the key revoking module which deletes the record from the software thus making it ineligible.

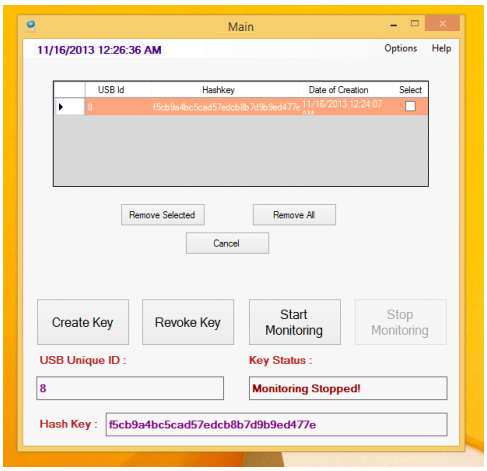

Figure 7 : Digilanté Key Revoking

5. CONCLUSION

Multiple keys for a same system were registered and any of them were able to unlock the computer. On revoking a certain registered USB key, it deleted the corresponding entry in the software thus rendered it unusable even though it had the key file present. A single USB flash drive was also used to serve as a key for multiple systems.

No runtime errors were encountered during the testing phase. The software has been tested on Microsoft Windows 7 and Windows 8 operating systems with Microsoft .NET Framework 4.0 preinstalled.

This software thus successfully implemented an efficient USB based authentication mechanism which allows the user to transform a simple USB device into a unique key. This method of authentication is secure, robust and immune to brute force attacks. The two step authentication of the PnP Device ID of the USB drive, as well as the hash key file ensures that even if the key file is copied to another device, it will not work as a key for the system. Also, provisions are there to encrypt the hash key recursively after regular intervals when it is attached to the system, thus making it dynamic and more secure. The new hash is also updated in the software records.

Additionally, to ensure that the system cannot be used by killing the power and powering on again, the software is made to start automatically after boot. Thus, it will find the USB key missing and again enter the state of lockdown.

6. ACKNOWLEDGMENTS

I am deeply indebted to Mr. Joy Paulose, HOD, Department of Computer Science whose stimulating suggestions and encouragements helped me in successfully completing this work. I would also like to thank all other the faculty members and students of the Department of Computer Science for providing constructive feedback which led to this project being an immense accomplishment.

7. REFERENCES

[1] Zhihui Liu, Gu, L., Yixian Yang and Guoqiang Xing "An identity authentication scheme based on USB Key for Trusted Network Connect", Information Theory and Information Security (ICITIS), pp. 203 – 207, 2010

[2] Yu Jin-wei "The program design for the network security authentication based on the USB Key technology", Electronic and Mechanical Engineering and Information Technology (EMEIT), 2011 International Conference on, On Vol. 5, page(s): 2215 – 2218

[3] Tao Yizheng, Tang Dingyong, Gaoshan, Shenhao "Design and Implementation of USB Key-Based JavaEE Dual-Factor Authentication System", Information Management, Innovation Management and Industrial Engineering, 2009 International Conference on, On Vol. 4, page(s): 443 – 446

[4] Jiang Yu, Chuan-fu Zhang "Design and Analysis of a USB-Key Based Strong Password Authentication Scheme", Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on, On page(s): 1 - 4

[5] Zhu Juan-hua, Wu Ang, Guo Kai "PC lock software design based on removable storage device and dynamic password", Computer Engineering and Technology (ICCET), 2010 2nd International Conference on, On Vol. 3, page(s): V3-326 - V3-329

[6] Leslie Lamport. Password Authentication with Insecure Communication [J]. Communications of the ACM, 1981, 24(11): 770-772

[7] A. Shimizu, "A dynamic password authentication method by one-way function," IEICE Transactions on Fundamentals 1990. On Vol. J73-D-I, No. 7, page(s): 630 – 636

[8] Shreya Nag, Dr. Meenakumari J, Sayantan Chakraborty "Design and Analysis of EyeSeeYou: Computer Surveillance Software", International Journal of Research in Information Technology, On Vol. 1, Issue 6, page(s): 52 - 59

[9] QIN Zhi-guang, "Cryptography algorithm-survey and trends", Journal of Computer Application, On Vol. 24, No. 2, page(s): 1 - 4

[10] Dino Esposito, Microsoft® .NET: Architecting Applications for the Enterprise (Pro-Developer), Microsoft Press, 2008.

[11] Alex Mackey. Introducing .NET 4.0: with Visual Studio 2010, Apress, 2010.