Journal of the Nigerian Association of Mathematical Physics
***Volume* 20 (March, 2012), pp 461 – 466**
© J. of NAMP

Towards Securing the Home Computer: a modification of the USB Port

***Evwiekpaefe, A. E., Irhebhude, M. E. and Ekpenyong, F. E.**

Department of Mathematics/Computer Science
Nigerian Defence Academy, Kaduna, Nigeria

Abstract

Hundreds of millions of people use the home computer everyday for different purposes. These systems use the universal serial bus (USB) disk for day to day transfer of data, communication and other applications. The USB as a flexible tool for data transfer raises security concerns relatively to a potential loss of assets. This paper therefore demonstrates how a modification of the USB port can improve the security of the home computer.

Keywords: home computer, operating system, threats, Universal Serial Bus (USB).

1.0 Introduction

Bill Gates once remarked "Microsoft was founded based on my vision of a personal computer on every desk and in every home, all running Microsoft software" [1]. When the International Business Machine (IBM) first introduced their personal computer (PC), in the 1980s, no one would imagine the development of computer technology in the past 30 years. During these years there were tremendous breakthroughs in the computer industry - graphical user interfaces, the internet, web browsers, etc. In the mid 90s, PCs had become easy enough for people to use with the bulk of the credit going to the Microsoft Corporation.

Today, computers are increasingly more affordable and internet connectivity is also becoming commonplace [2]. Moreover, studies have shown that there exist a computer in almost every home in developed countries and the number in developing countries is increasing very fast. The huge number of home computers and the massive internet usage has improved information and communication flow in diverse ways. Indeed the home computer and the internet are surely here to stay and the impact of information technology is rapidly showing up on just any aspect of our lives. Despite these benefits, there are important problems that need to be addressed.

Most people don't have any basic knowledge of how to protect their home computer from the ever increasing threats to computers. Malicious code writers use the internet to launch various attacks on computers around the world. Organized crime uses the internet to steal important information such as credit card numbers. Shady corporations install programs that monitor surfing patterns without the knowledge of the users and these threats are moved from one home computer to another through the universal serial bus (USB).

The USB disk is widely used for storing and transmitting information. Infact, the USB port is among the most prolific hardware computer port in existence, with over 3 million USB devices sold in 2008 [3]. It provides the end-user a simple, universal connection conduit for a multitude of uses, eliminating much of the need for task or peripheral-specific ports of days gone by (parallel ports for printing, PS2 ports for mice and keyboards etc). It is this ubiquitousness, combined with a seemingly infinite number of uses that makes the port a concern to computer security experts. A port that can transfer data, provide power and allow connection of hardware peripherals, but also potentially pose a serious security vulnerability to personal and enterprise computing [3].

*Corresponding author: ***Evwiekpaefe, A. E.*** E-mail: contact_abraham@yahoo.com, Tel.: +2348035600524

A fair amount of research has gone into blocking malicious software (viruses, worms, trogans, spyware, etc). Comparatively less time has been spent researching malicious hardware devices. There are many examples of malicious hardware, to name a few: backdoored routers, surreptitiously installed hosts that that act as pivots on a network, PS/2 key loggers, USB, etc. USB devices are, however, of interest as they often require less user interaction to install on a system than other types of hardware peripheral meaning less attention may be paid to what tasks they are doing under the user's nose [4]. Again, while modern operating systems have ways to help mitigate the threats, little seems to be done by current security systems to thwart malicious USB devices [4]. This is why there is the need to develop a security mechanism to protect the home computers against any threat via USB port.

The purpose of this paper is to demonstrate how an auto modification of the USB port could enhance the security of home computer.

2.0 Background

Home Computer

The home computer is a personal computer specially configured for use in a home rather than an office. Typically, they have only medium -power microprocessors, but are equipped with a full complement of multimedia devices. In addition, manufacturers often bundle recreational and educational software with home computers [5].

Operating System

An Operating System is a collection of programs that handle many of the technical details related to using a computer such as managing computer resources, providing a user interface, and running applications [6].

An operating system performs these services for applications:

- In a multitasking operating system where multiple programs can be running at the same time, the operating system determines which applications should run in what order and how much time should be allowed for each application before giving another application a turn.
- It manages the sharing of internal memory among multiple applications.
- It handles input and output to and from attached hardware devices, such as hard disks, printers, and dial-up ports.
- It sends messages to each application or interactive user (or to a system operator) about the status of operation and any errors that may have occurred.
- It can offload the management of what are called batch jobs (for example, printing) so that the initiating application is freed from this work.
- On computers that can provide parallel processing, an operating system can manage how to divide the program so that it runs on more than one processor at a time.

USB

USB (Universal Serial Bus) is an industry standard developed in the mid-1990s that defines the cables, connectors and protocols used for connection, communication and power supply between computers and electronic devices[7].

USB was designed to standardize the connection of computer peripherals such as keyboards, pointing devices, etc to personal computers, both to communicate and to supply electric power. It has become commonplace on other devices, such as smartphones, PDAs and video game consoles. USB has effectively replaced a variety of earlier interfaces, such as serial and parallel ports, as well as separate power chargers for portable devices [7].

Security

Security is defined as the extent to which consumers believe that his or her home computer is free from unauthorized access, use, alteration, and destruction [8]. This may be due to a higher threat of possible inappropriate behaviors such as security lapses where vital private information can be stolen by hackers [9].

Threats

Threat is a person or thing likely to cause harm or danger. Threats to computer security are: criminals, computer crime and hazards.

3.0 Methodology

Java as our choice language

Java was used as our choice programming language. Java incorporates object-oriented technologies such as class, object, encapsulation, inheritance etc. Classes provide a means of encapsulating the objects used by the program (which ordinarily represents the program`s data) into a well organized, modular format that is easy to reuse and maintain. Through a process called inheritance, new objects can be derived from existing objects by adding new elements to the existing object design.

Java program code was used to automate the USB system. The system modifies the windows operating system registry by enabling and disabling the USB port.

The System Registry

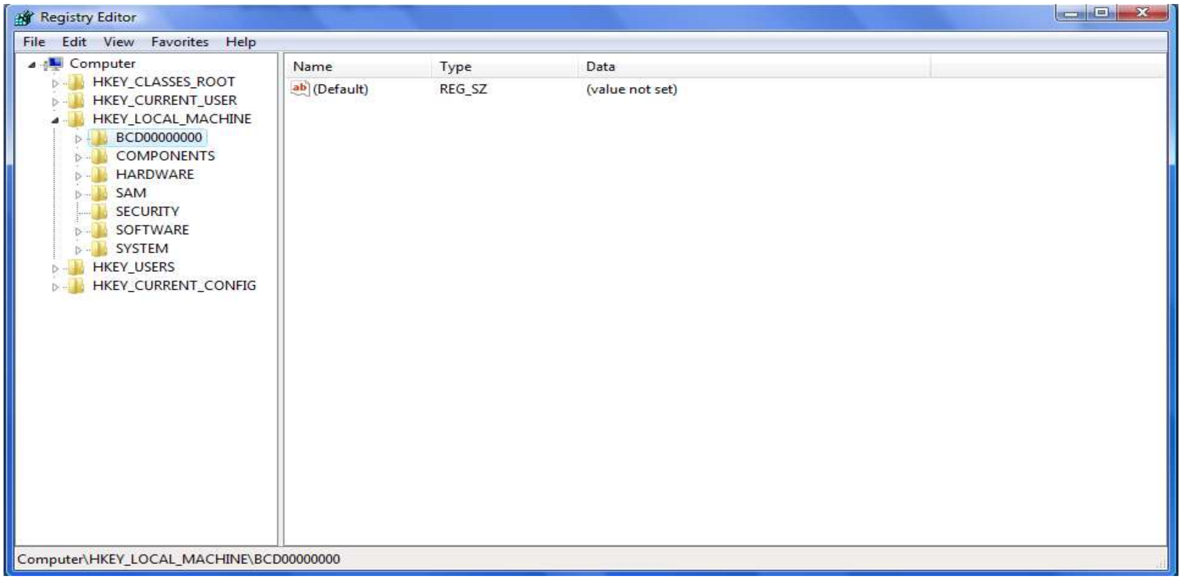
The registry is a database in the Windows operating systems that contains important information about system hardware, installed programs and settings, and profiles of each of the user accounts on your computer. Windows operating system continually refers to the information in the registry.

Registry Editor

Registry Editor is a tool intended for advanced users. It is used to view and change settings in the system registry, which contains information about how your computer runs. Windows refers to this information and updates it when you make changes to your computer, such as installing a new program, creating a user profile, or adding new hardware. Registry Editor lets you view registry folders, files, and the settings for each registry file (See Fig. i).

Ordinarily, you do not need to make changes to the registry. The registry contains complex system information that is vital to your computer, and an incorrect change to your computer's registry could render your computer inoperable. However, a corrupt registry file might require changes. It is strongly recommended that you back up the registry before making any changes and that you only change values in the registry that you understand or have been instructed to change.

To open the registry with elevated privileges, click Start, click All Programs, click Accessories, right-click Command Prompt and then point to Run as administrator. In the command prompt that opens, type regedit.exe.



Name	Type	Data
(Default)	REG_SZ	(value not set)

Computer\HKEY_LOCAL_MACHINE\BCD00000000

Fig i: Registry Editor showing registry folders, files and settings for each registry file.

4.0 Results And Discussion

The system was designed and implemented with Java Programming Language. This system which is an auto modification of the USB, through a password supplied during installation, enables and disables the USB port thus preventing unauthorized use of the USB port. The results are shown in the appendix below.

The system was designed to be portable. Hence it can be installed from a CD ROM, flash Disk or Hard disk and can be transferred from one system to another. The System, Home Computer Security USB Enhancement (HCSUE), is special software meant for 32 bit systems. During the process of installation, the user is prompted to insert a password which cannot be changed thereafter except by uninstalling the program. Java codes were written to enable and disable the USB port with the administrator supplying the installation password with which to enable the port.

After installation two scripts appear on the user desktop and in the programs/USB list. These are:

- UsbEnable
- UsbDisable

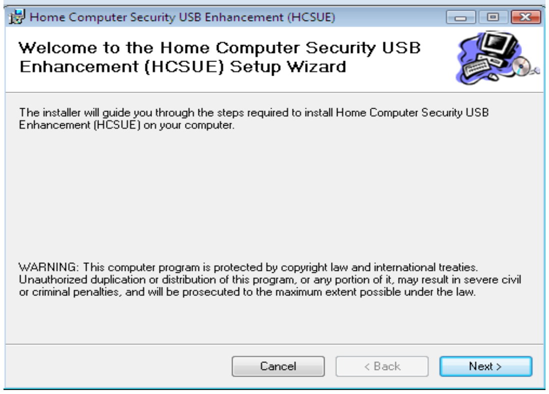
UsbEnable enables USB storage recognition. This is achieved by clicking on the UsbEnable file. UsbDisable disables USB storage recognition. This is achieved immediately after the installation of the software since our system was designed to prevent unauthorized access to the USB port of the home computer.

Results from the software installation show the following. Fig. ii displays the page of the HCSUE. Following this page guides the user through the steps required to install the HCSUE system on a home computer or PC. Fig. iii reminds the user of the license agreement. The HCSUE software cannot be modified or tampered with except with prior knowledge of the authors. In Fig. iv, the installer guides the user to choose a destination folder and an appropriate user specification for the software. The installer is then ready to install the HCSUE on your computer. Clicking on *next* confirms the process of installation in Fig. v while *cancel* terminates the process. To effectively secure the software, password was introduced into the system in Fig. vi. The password secures the system from unauthorized users. Whenever the system USB is disabled an intruder will need the actual password before the UsbEnable can function. This thus undyingly secures your computer and prevents it from an unauthorized user. Fig. vii displays how the password is confirmed. This thus helps the user have mastery of the password. Fig. viii completes the installation while Fig. ix, shows the prompt for password insertion for enabling USB usage or recognition. Fig. x illustrates the instruction for USB insertion.

5.0 Conclusion

Home computer security is an important area in computer security since the number of persons with computers at home is increasing, and the number of interconnected computers is also on the increase. The ease of the USB, especially from the perspective of the average computer user, makes it easy for malicious attacks. This raises security concerns about the home computer and how to adequately protect it from being corrupted in different ways. In this paper we were able to raise the security awareness of the home computer user and also demonstrated how a modification of the USB port can enhance the security of home computer.

Appendix

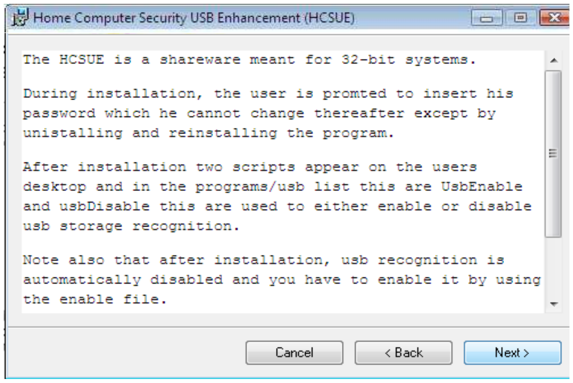


Welcome to the Home Computer Security USB Enhancement (HCSUE) Setup Wizard

The installer will guide you through the steps required to install Home Computer Security USB Enhancement (HCSUE) on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Fig ii: Welcome page



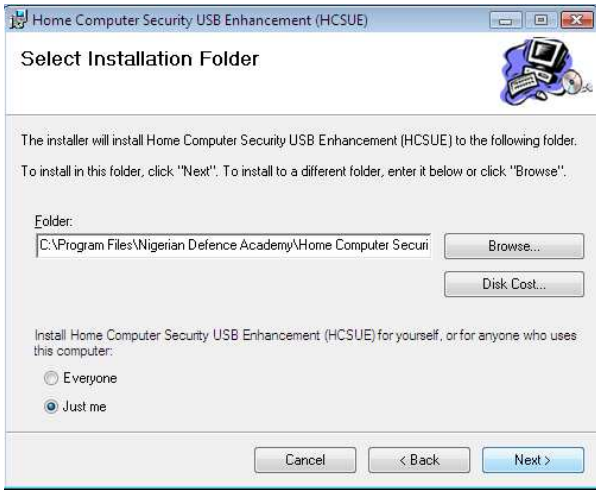
The HCSUE is a shareware meant for 32-bit systems.

During installation, the user is promted to insert his password which he cannot change thereafter except by unistalling and reinstalling the program.

After installation two scripts appear on the users desktop and in the programs/usb list this are UsbEnable and usbDisable this are used to either enable or disable usb storage recognition.

Note also that after installation, usb recognition is automatically disabled and you have to enable it by using the enable file.

Fig. iii: License Agreement



Select Installation Folder

The installer will install Home Computer Security USB Enhancement (HCSUE) to the following folder.

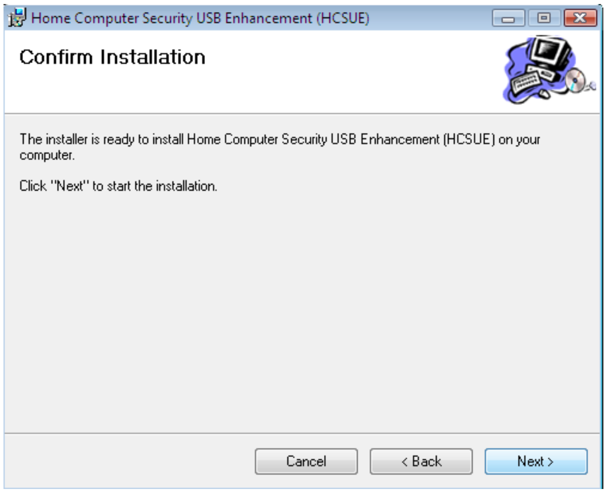
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files\Nigerian Defence Academy\Home Computer Securi

Install Home Computer Security USB Enhancement (HCSUE) for yourself, or for anyone who uses this computer:

○ Everyone
● Just me

Fig iv: Destination folder and users specification

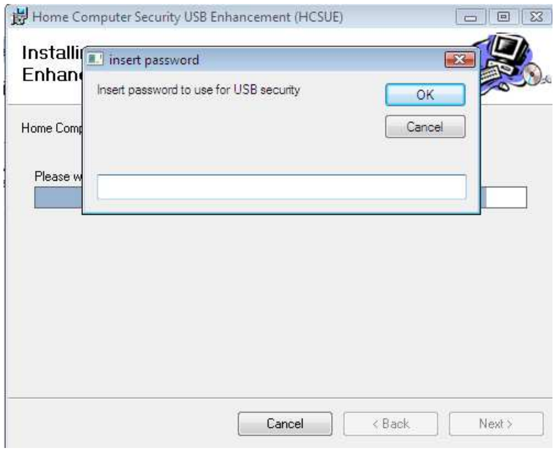


Confirm Installation

The installer is ready to install Home Computer Security USB Enhancement (HCSUE) on your computer.

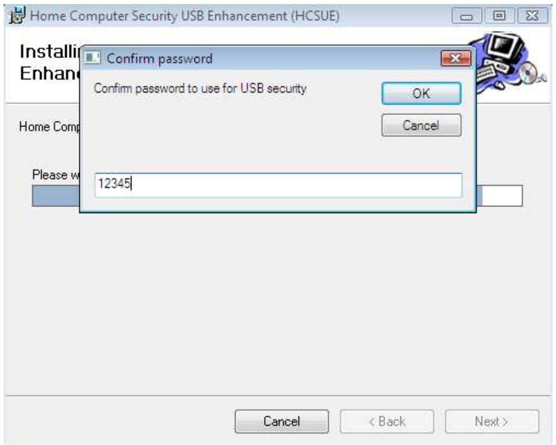
Click "Next" to start the installation.

Fig v: Confirm installation



Insert password to use for USB security

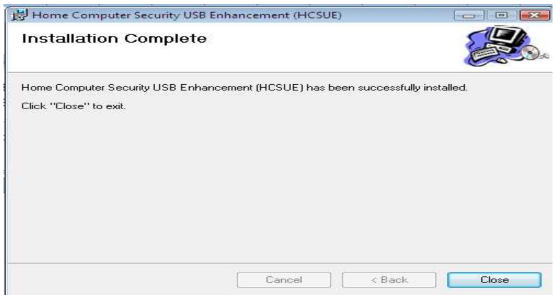
Fig vi: Inserting enabling and disabling password



Confirm password to use for USB security

12345

Fig vii: Confirming enabling and disabling password

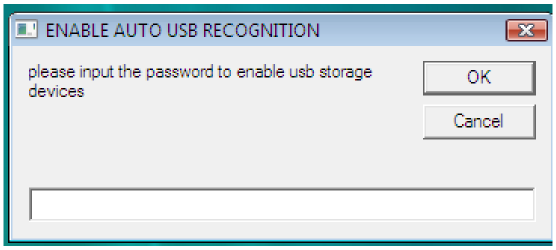


Installation Complete

Home Computer Security USB Enhancement (HCSUE) has been successfully installed.

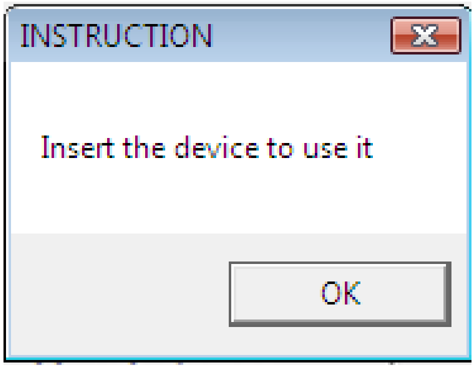
Click "Close" to exit.

Fig viii: Installation complete



please input the password to enable usb storage devices

Fig ix: Prompt for password insertion for enabling USB recognition



INSTRUCTION

Insert the device to use it

Fig x: Message box for correct password insertion

References

[1] Stevenson Keira (2007). "Bill Gates." Bill Gates (2005): 1. MAS Ultra – School Edition. Available @ http://search.ebscohost.com

[2] Longe O.B & Chiemeke S.C (2009). Cyber Crime and Criminality in Nigeria – What Roles are Internet Access Points in Playing? European Journal of Social Sciences. 6(4). 132-139.

[3] Erik Couture (2009). USB – Ubiquitous Security Backdoor. GIAC (GSEC) Gold Certification. SANS Institute.

[4] Adrian Crenshaw (2011). Plug and Play: Malicious USB Devices. Presented at Shmoocon. Available @http://www.irongeek.com/i.php

[5] Webopedia.com. . Available @ http://www. webopedia.com/TERM/H/home_computer.html/. Accessed October, 2011.

[6] Timothy J. O'leary & Linda I. O'leary(2005). Computing Essentials 2005 Complete Edition. Mcgraw Hill, USA.

[7]. Wikipedia.org. Wikipedia, the free encyclopedia. Available @ http://en.wikipedia.org. Accessed September, 2011.

[8]. Olusegun F., Awe OG, Sharma SK, Jeff Z (2006). Factors affecting the adoption of Ecommerce: A study in Nigeria. J. Appl. Sci. 6(10): 2224-2230.

[9]. Suh, B., & Han, I. (2002). Effect of trust on customer acceptance of Internet banking. Electronic Commerce Research and Applications. 1, 247-263.