International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 7, September - 2012

Secure Storage of Encryption Keys

Vijay Kumar Damera[#1], Dr. Suresh Pabboju[*2], P. Shyam Sunder[@3]

[#]*Dept. of IT, MGIT, Hyderabad, A.P, INDIA*
[*] *Dept. of IT, CBIT, Hyderabad, A.P, INDIA*
[@]*Department of CSE, MGIT, Hyderabad, A.P, INDIA*

***Abstract*— The purpose of this paper work is to make a survey of presently existing devices available in the market to store encryption keys, how the hacker intrudes into the device, what are the attacks behind theft of the keys, how can we store encryption keys securely?. Under the category of storage devices, USBs (Universal Serial Bus), PDAs (Personal Digital Assistant) and Smart Cards were examined. Under the category of attacks on devices, attacks from hackers, attacks from malicious code (Trojan Horses, viruses, worms), attacks from PDAs, attacks from Smart Cards, dictionary attacks and brute force attacks were studied. Based on these requirements we have discussed and analyzed a proposed system to store the encryption keys securely to avoid these attacks.**

***Keywords*— Cryptography, Storage of encryption keys in devices, Attacks on devices, Proposed secure system.**

I. INTRODUCTION

This paper has been written for the specific purpose of finding a way to store encryption keys in a secure manner. Encryption keys are used to protect valuable information. If the secrecy, integrity or availability of the keys are damaged, then the secrecy, integrity or availability of the valuable information may be damaged. In this paper we are going to investigate different storage devices. We will also discuss how a device could be constructed to be able to store encryption keys securely.

II. WHY SHOULD THE ENCRYPTION KEYS BE STORED SECURELY

The growth of Internet has been accompanied by new methods for illegal intrusion into computer systems. When computer systems are connected online, they are vulnerable to computer security attacks. If the user stores encryption keys in his computer, there are chances to access the keys from his computer and there is a possibility that an unauthorized user can copy the encryption key or possibly encrypt messages without the owner of the key knowing it. Thus the owner of the key wants to control the usage of the key. Since most computers are too complex to deserve trust, the question arises how can the user store encryption keys securely?. Computers are used to store valuable information. To store the information securely, the computer security objectives i.e. confidentiality, integrity and availability have to be satisfied. Otherwise the intruder can access the information. The computer security deals with the "Prevention and detection of unauthorized actions by users of a computer system" [1].

III. STORAGE OF ENCRYPTION KEYS IN DEVICES

A. Computer Hard Disk

A hard disk is a storage device which can be found in all computers. If the user wants to manipulate or access the data in the hard disk, then the user needs a software(OS) to communicate with the hard disk, as shown in figure 1. The hard disk is connected to the hardware. The hard disk is used to store data such as programs and user files. The users can get access to memory only through the OS [2]. Data on the hard disk can be erased and/or overwritten. The hard disk is a non-volatile storage device which means it doesn't require a constant power supply in order to retain the data stored on it. Users can store encryption keys on the hard disk. The hard disk listens to commands like read/write from the OS and this is how keys are stored on the hard disk.

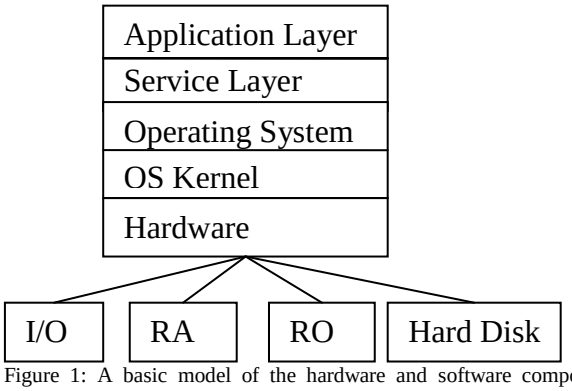

Figure 1: A basic model of the hardware and software components of a computer

B. USB (Universal Serial Bus)

The USB is designed to act as an interface for low- and medium-speed peripherals to get connected to a PC (up to 127 peripherals), with a top transfer rate of 12 Mbit/sec. It is much faster than serial and parallel ports [3]. The major advantage of USB is the plug and play option which doesn't require the system to be rebooted or reconfigured when a new device is connected. Technical issues like bus termination and the assignment of device identifiers are taken care of by the hardware and software architecture and a pipe is the association between the specific endpoint on the device and the appropriate endpoint on the software in the host.

USB memory devices are the most commonly seen devices nowadays. These devices are small in physical size and have a high capacity of storing data. Most of the devices come with capacities ranging from 128 MB to more than 1 GB of data storage. The USBs are solid state memory devices as shown in the Figure 2 that plug into a USB1.2 or 2.0 slot on a computer or a notebook [4]**.** Portability, speed, and storage capacity are the important things that made this device a popular one.

C. PDAs (Personal Digital Assistant)

A personal digital assistant (PDA) is a handheld device that combines computing, telephone/fax, Internet and networking features[5]. A typical PDA can function as a cellular phone, fax sender, web browser and personal organizer. Most PDAs began as pen-based, using a stylus rather than a keyboard for input. This means that they also incorporated handwriting recognition features. "Some PDA's can also react to voice input by using voice recognition technologies" [6].

PDA Data encryption and protection:

To protect data stored in a PDA from unauthorized access, some of the PDAs are secured by using a password, and the data can be encrypted with encryption algorithms. The PDA encryption generally takes four forms.

- Encryption of private records.
- Encryption of the entire memo pad
- Organization and encryption of the user's passwords or other confidential bits of information.
- Encryption of databases.

Most of the information below is from [7]. To protect the data on the device the encryption systems below have been developed. "The Palm OS supports private records, which involves a special flag which can be set for individual entries in the address book, calendar, Memo Pad, and Tasks/To-Do" .

D. Attacks on PDAs

The threats for PDAs, that users need to be concerned with typically fall into one of these three categories:

1. Identity Theft
2. Viruses and data corruption
3. Vulnerabilities of PDAs

One of the biggest security risk to PDAs is that these devices are handled in such a way that they are easily forgotten and someone can easily steal them. For that reason securing the data on the device in standalone mode is probably the best type of precaution users can take. The second risk is because of viruses. Because of these problems encryption solutions exist for PDAs to maintain security for both the data and links used to communicate with remote systems and networks. By using an encryption product to secure either the link to the desktop hot-sync system or for wireless surfing, you basically need to wrap up your PDA traffic in a VPN. To protect the PDA from wireless vulnerabilities you should install a VPN client on your PDA [8].

E. Attacks on smart cards

Smart cards provide security benefits. This can be incorporated in cryptographic protocols that can protect the data from unauthorized users. However, the protection strength is being overestimated by most of the users [9]. Unfortunately there are some tampering techniques to break the smart cards. Those attacks are divided into four major attacks [10].

1. Microprobing
2. Software attacks
3. Eavesdropping
4. Fault generation

Microprobing can be used to access the chip surface directly. We can observe, manipulate, and interfere with the integrated circuit. Software attacks use the normal communication interface of the processor and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation. Eavesdropping techniques monitor, with high time resolution, the analog characteristics of all supply and interface connections and any other electromagnetic radiation produced by the processor during normal operation. Fault generation techniques use abnormal environmental conditions to generate malfunctions in the processor that provide additional access.

IV. PROPOSED SECURE SYSTEM

Today, the Internet has become the fastest growing part of the global network. However, it is the network part that draws more attention to the security related issues because of its possible design flaws and vulnerabilities to attacks.

When an external device is connected to the computer there is always a risk for illegal or unauthorized access to personal information and secret keys which are stored in the external storage. The hacker generates a malicious program over the Internet which can copy or block the keys form the external device or hard disk. For example, consider an e-mail virus program which gives the control access to the hacker who has generated that virus. Similarly, if the same virus program can be extended to access the data from the external storage and give the total control to the hacker, then the hacker can either copy the key or use the key.

A. *Hardware and software components of a proposed secure system*

A USB connector provides an interface to the host computer. A USB Mass control device is a USB host controller which contains a RISC microprocessor and a small amount of on-chip ROM and RAM. Inside of the flash memory there is a reference monitor. This reference monitor is used to mediate all access to the USB mass control devices and USB flash memory chip. The purpose of reference monitor is to verify the authorized requests.

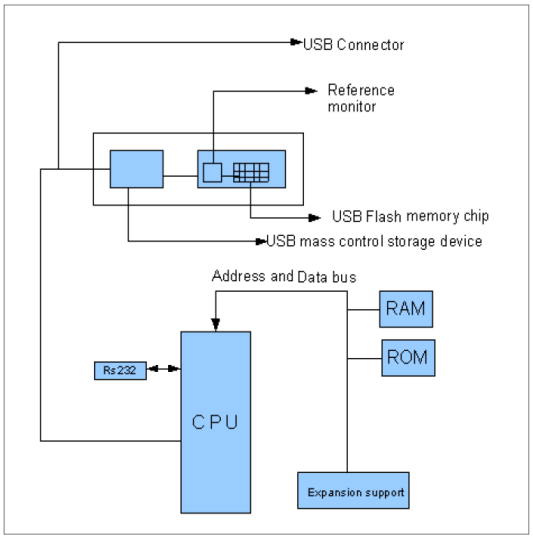

Figure 2 Computer Block diagram Connecting with USB

The Windows Host Program communicates with the device driver to send commands and data to the external USB device. The host program communicates with the device driver through file IO. The flow of this program as shown in Figure 3. The host first calls a Windows API function to get the path to the driver. This call relies on the GUID to find the correct one. This path, when opened, corresponds to USB Endpoint 0, the command endpoint. To send a command, the host program sends an IO Control message (IOCTL) to the driver, telling it what to do. This is used mainly to send vendor specific commands. All the routines used for finding and opening the IO pipe to the driver are collected in one file, USB.cpp

To send and receive data on the bulk endpoints, two other files have to be opened. These have the same path as the driver, but have "\PIPE*nn*" appended where nn is the pipe number. This device has only two pipes, PIPE00 and PIPE01. PIPE00 is the output bulk pipe, and PIPE01 is the input bulk pipe. Communication over these pipes uses standard file IO.

B. *Software components of the proposed secure system*

<Note>
<Protecting the device from malicious code>
<Scanner which is used to detect the Viruses Trojan horses and worms >
It can use multiple times to detect, the malicious code
\. result: = "yes"
<_if malicious code test based on the
signature ="\.result == "yes" >
<then>
Scanner detect the virus
<else>
Go to the function unknown user
</else >
</if >
</Scanner which is used to detect the Viruses Trojan horses and worms >
<UNKNOWN USER>
It counts the risk level
<_if risk is high >
<then>
RISK IS HIGH PLEASE CHECK THE SYSTEM ONCE
<else>
GO TO THE FUNCTION AUTHENTICATION
</else >
</if >
</UNKNOWN USER>
</protecting the device from malicious code>
\.Checking: = "correct"
<Authentication>
<_if password="\.Checking: == "correct" >
<then>
U CAN ACCESS THE PERSONAL FOLDER
<else>
PLEASE RE ENTER U R PASSWORD
</else>
</_if>
</Authentication>
</Note>

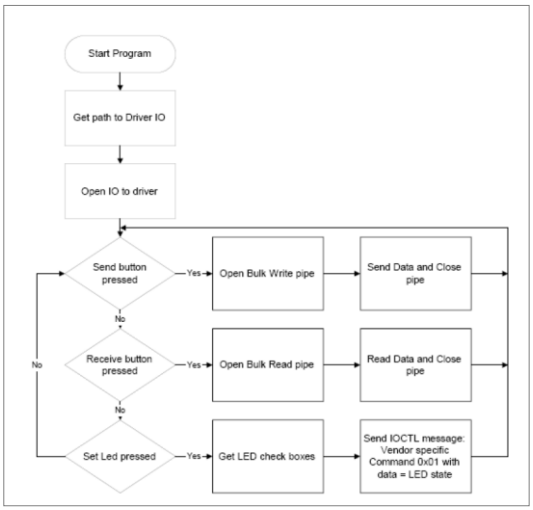

Figure 3 Windows flow chart diagram

C. *Security system for normal users*

When an external device is connected to the system, the system will recognize it and the device will be displayed as an external device in the explorer as shown in the Figure 4 on the windows operating system. This can be run on any platform like UNIX and Macintosh. The user connects the external device to the computer. After connecting the external device, the IO commands will be performed and the information transferred from the external device to the computer in a secure way as explained below how we are protecting the personal information and secret keys in the external device. The external device will have two folders namely, control protector (cp), and the personal information. Control protector is a third party tool for providing administrator control over the device. When the user accesses this device, the control protector folder will do the operation to control our secure information from the hackers (see appendix C&D). The external device will have two folders namely, controlprotector (cp), and the personal information. When we are trying to access the external device

the controlprotector folder will check the programs running on the host computer. If a malicious program is running in the host computer, then the controlprotector will indicate the risk level to the programs, which are running in the OS kernel of the host computer. If the controlprotector finds the risk in the host computer, then the user should be aware of the risk and try to stop the running programs or format the operating system(OS). Encryption keys and personal information are secure from the hackers. If the controlprotector didn't find a risk in the host computer, then the user can access the sensitive data.

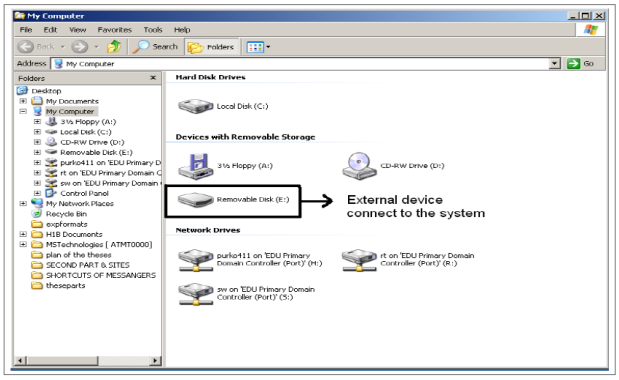

Figure 4 Representing the external device

Suppose the user wants to transfer money or documents to another user. Then, the user must follow the following steps to protect his/her personal information.

- Click on the external device. It shows the two folders as shown in Figure 5.
- The user must click on the controlprotector (CP) for the device to connect with the operating system
- After that the user has to run the program by giving appropriate instructions in the controlprotector (CP) folder to access the personal information.
- If the user doesn't run CP folder, the storage device cannot open our personal folder in the external device.
- Then it will connect to the OS through that the controlprotector will be active and give the protection to the external device.
- After that the USB mass storage device will ask the password for authentication. As shown in Figure 7.
- If the password is correct then the user can access the sensitive data from the proposed device with the help of the software.

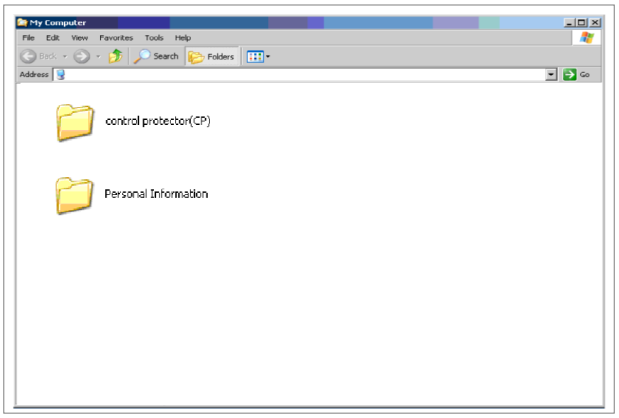

Figure 5 Showing two folders to the user

Figure 6 Showing control protector window

Figure 7 Password window

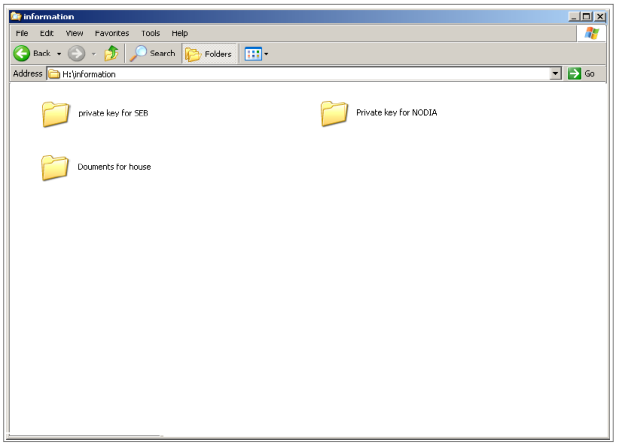

Figure 8 Showing contents of the main folder

The most advantageous concept in this type of device is that, if we lost our external device or the external device is stolen, there is no risk for the user as it is secured by the password. The development cost for this sort of external device's are less when compared with higher authority application. No enemy program can intrude into the external device because the scanners and executable scanner intelligently analyzes the system for known and unknown viruses.

CONCLUSION

Securing the storage of encryption keys will eventually reduce the attacks from intruders, viruses and other forms. This paper has focused on different concepts of cryptography related encryption keys and secure storage of encryption keys. Different kinds of storage devices and common attacks on them are studied which helped us in proposing a secure system for storage of encryption keys. Finally securing encryption keys is a challenging task. By using some third party tools in the storage device which provides administrator control, we can achieve such secure storage.

REFERENCES

[1] Dieter Gollmann, Computer Security, John wiley & sons ltd 1999.
[2] William stallings, "Operating system" 2002.
[3] How USB works? http://www.tech-pro.net/intro_usb.html
[4] Kingpin, "Attacks on and Countermeasures for USB Hardware Token Devices" Reykjavik University 2000.
[5] Prifitt, Brian, "customize your palm or hand spring" 2004.
[6] PDA Security with Windows CE http://insight.zdnet.co.uk/business/management/0,39020490,2134022,00.htm
[7] PDA Security with Windows CE with PDA encryption option. http://insight.zdnet.co.uk/hardware/mobile/0,39020442,2119359,00.htm
[8] David Melnick, Mark Dinman and Alexander, "PDA security" MuratorMcGraw-Hill Professional 1 edition Jul 25 2003.
[9] W. Rankl, W. Effing "Smart Card Handbook" John W illey, 2000
[10] Oliver Kömmerling, Markus Günther1999, Design Principles for Tamper-Resistant Smart card Processors
[11] Phil Zimmermann "Introduction to Cryptography" Network Associates 1999.
[12] William Stallings "Cryptography and Network security: Principles and Practice" Prentice Hall 2005.
[13] Alfred J. Menezes, Paul C. van Oorschot and Scott A.Vanstone , Hand book of Applied Cryptography .
[14] Adams C and Lloyd S "Under Standing PKI: concepts, Standards and Development Considerations" ACM Press New York, NY, USA 2003.
[15] Rune Torgersen, General Purpose USB Device, South Dakota School of Mines and Technology 2000.
[16] W. Rankl, W. Effing "Smart Card Handbook" John W illey, 2000.
[17] Hendry , "Smart Card Security and Applications, Second Edition" , Artech House, Inc. Norwood, MA, USA 2001 .
[18] Eugene lokett, Sung kyu park, gaungcheng jiang, MikeRiddle,"Security Aspects of smart card".
[19] Prifitt, Brian
[20] Debra Littlejohn Shinder ,"customize your palm or hand spring" 2004.
[21] Thomas Shinder, "The Best Damn Windows Server 2003 Book Period", 2003.
[22] Andrew Michael colarik, "The Home Executive's Guide TO Computer Security" 2005.
[23] Tipton, Harold F, Krause and Micki, Information security management hand book Auerbach; 4th edition 2003.
[24] Oliver Kömmerling, Markus Günther, Design Principles for Tamper-Resistant Smart cardProcessors 1999.