CHAPTER 5
ANALYSIS OF HARDWARE MEANS OF DATA PROTECTION

5.1 Introduction

In this thesis, there is an extra security proposed by using hardware features. Security hardware tokens are used to prove one's identity electronically where additional higher levels of security are needed. The token is used in addition to or in place of a password to prove that the customer who they claim to be. The token acts like an electronic key to authenticate the user. However, the drawbacks of such an additional hardware token is also there. The first thing is often the higher costs involved in provisioning such a hardware to the users and then comes the added maintenance costs. And on top of this adding additional hardware can often lead to thefts and other failure points. Hence in this chapter of the thesis, focus will be for maintaining a hardware authentication without attaching any hardware to the normal system.

5.2 Currently Used Hardware Methods of Data Protection

5.2.1 USB Based Dongles

In this method of software protection, the publishers generally provide a special h/w which needs to be connected when the s/w is being used. This h/w is widely available as dongles. The dongles can be both serial port based can be USB based dongles. The dongles must be connected always with the computer for the S/W to work.

When the S/W is started it checks for the presence of the dongle and also checks whether the encrypted key is presented in the dongle memory. This kind of
S/W protection is often costly as it involves additional h/w and is used for specialized software which cost millions to deploy. This also involves need of installation of additional drivers to make the hardware dongle work. This will turn out to be cumbersome and also difficult to manage in an enterprise environment if there is a need to install the software on hundreds of computers.

**5.2.2 Steinberg Key**

The usage of dongle for software protection has been used for many decades and it used in expensive s/w like CAD/CAM, expensive and proprietary video/audio processing system and expensive retail software for hospitality and retail industry. A popular example is the dongle is called the Steinberg Key which is used to protect popular Steinberg’s products for audio protection and editing solutions. In the case of this particular key it can be bought separate of the product itself. This dongle apart from the protection part of the software can also be programmed to exactly say which features of the software is actually bought by the user needs to be enabled. For example, when a user buys only 2 modules of a particular software which manages the ERP functionality of an Enterprise, the hardware dongle can be programmed in such a way that when it is connected to the computer along with the software only the intended functionality would be working while the dongle is presented.

Some of the initial versions of dongle based protection was just based on detection which means that if the software detects the presence of the dongle then it will work. However, overtime the dongles started getting small amount of data storage capabilities as well which was enough to store information regarding registration and other vital data which will assist the software protection.
5.2.3 Smart Cards

The recent development in h/w based protection is to use smart card based protection where a card reader is attached to the system and the inserted card is read and provided access to the software.

5.3 Some Other Popular Hardware Related methods

5.3.1 Serial Numbers of CD or Digital Signatures

Various s/w publishers employ different means for protection using software means. Usually, the simplest method is to use Serial numbers which is generated based on an algorithm to tie a user to a particular software. Later on there were some additional methods used by game developers and the most common method is usually used to detect the presence of the original game cd in the cd drive when the game is being played or started. Another method that is commonly used these days is to include special digital signatures into the discs produced at the time they are manufactured. The game or software when run will check for the presence of the cd and also check for the existence of the copy protection digital signature on the disc. However, they do require special hardware to manufacture these discs.
5.3.2 Secured CD/DVD Protection

Let us see some of the methods used for protecting software in CDs or DVDs. One of the most common methods to copy music from Audio CDs and DVDs is to use ripping software to convert the tracks to MP3 music. Later several recording studios to circumvent this introduced monitoring software which will be installed when the DVD/cd is first inserted into the computer. The software will in turn monitor if any ripping software is being run to copy the music and if it finds any will disable the access to the drive or stop the software from doing this.

5.3.3 DVD Region Coding

DVD region coding is another method that is used to region lock software to a particular region so that DVDs that are supposed to sold in that region will be able to play in that particular DVD Player. However later on several DVD players came that circumvented this and hence this method was rendered useless.

5.3.4 Digital Rights Management

DRM services make use of authentication servers in the internet when a music or media is played. However, this will cause bad user experience when the server goes down as the users will not be able to playback the media. And also this method is limited to media consumption and cannot be used for protection of software.

5.4 Alternate Method to existing Hardware Authentication

The term "hardware authentication" is referred to a highly secure computing system that uses a hardware device to grant access to the users. Hardware authentication is used most commonly for computer systems and networks to protect extremely sensitive data. Tokens can contain chips with functions varying from very simple to very complex, including multiple authentication methods. There are many types of tokens like connected tokens, disconnected tokens, smart cards, contactless
tokens, Bluetooth tokens, mobile device tokens etc. This section focuses hardware authentications using the features already available inside the computer.

5.4.1 Hard disk serial number

A hard disk drive (HDD) is an internal physical storage device inside a computer which stores digitally encoded data on fast rotating platters having magnetic surfaces. A "drive" simply refers to a device distinct from its medium, such as a tape drive along with its tape, or a floppy disk drive and its floppy disk. Some of the early HDDs had removable media which could be replaced; however, an HDD today is typically a sealed unit with fixed media. Each manufacturer of hard disk assigns a unique serial number to the disk for their identification purpose. Some of the common hard disk manufacturers are Seagate, Samsung, Hitachi etc. Hard disk serial number should not be confused with the volume serial number. The volume serial number is assigned and changed during formatting of partition.

![Fig 5.2 Screen shots of Hard disk serial number extracting](image)

5.4.2 Ethernet Mac address

All the attached network adapters (NICs) to the computer will have a quasi-unique identifier. This identifier is called Media Access Control address or Ethernet Hardware Address (EHA). Sometimes it is also referred as a hardware address or adapter address. It is a particular number that acts like a name for a particular network adapter. The network cards (or built-in network adapters) in the different computers
will have different names, or MAC addresses. If there are multiple network adapters such as an Ethernet adapter and a wireless adapter in the same computer, then they would have different MAC addresses.

The original IEEE 802 MAC address, comes from the original Xerox Ethernet addressing scheme. This 48-bit address space contains potentially 248 or 281,474,976,710,656 possible MAC addresses. All three numbering systems use the same format and differ only in the length of the identifier. Addresses can either be "universally administered addresses" or "locally administered addresses."

A universally administered address is uniquely assigned to a device by its manufacturer; these are sometimes called "burned-in addresses." The first three octets (in transmission order) identify the organization that issued the identifier and are known as the Organizationally Unique Identifier (OUI). The following three (MAC-48 and EUI-48) or five (EUI-64) octets are assigned by that organization in nearly any manner they please, subject to the constraint of uniqueness. The IEEE expects the MAC-48 space to be exhausted no sooner than the year 2100; EUI-64s are not expected to run out in the foreseeable future. Usually the MAC address can be found from windows command prompt pretty easily. But it can be also found via simple programming.

![Fig 5.3 Screen shots of extraction of ip configuration](image)

Fig 5.3 Screen shots of extraction of ip configuration
5.4.3 Motherboard serial number

Each motherboard will contain a unique serial number. This serial number is a combination of manufacturer name, date of manufacture, bios version and serial number. This identifier will be unique for each computer.

5.4.4 IMEI number

The International Mobile Equipment Identity Number is a unique number that is associated with each and every mobile which cannot be modify. This number is used to identify a mobile to the mobile network. IMEI number is usually a 17 or 15-digit number. IMEI numbers are stored on the phone itself and not the SIM card. Hence swapping the sim card will not change the IMEI number.

5.4.5 Mobile number

A mobile number is an identifier that is allocated to a person and is used to identify that mobile to the other persons on a network. In most cases the mobile number cannot be used as a primary use for identification as a mobile number can be changed from one person to another. However, it can be used as a secondary method of identification along with IMEI number. Swapping the SIM card changes the mobile number.

5.5 Analytical Comparison of various methods

The below table gives the comparison of the existing hardware protection discussed in this chapter techniques. The parameters for which the comparison was done include Ease of use, protection capabilities, how the method will be against hacking etc.
Table 5.1 Comparison of various hardware protection methods

<table>
<thead>
<tr>
<th></th>
<th>Methods using dongles</th>
<th>Method using existing hardware properties</th>
<th>Serial Number/other methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ease of use</strong></td>
<td>Cumbersome to carry around.</td>
<td>Does not need to carry around additional h/w</td>
<td>Easier to use</td>
</tr>
<tr>
<td><strong>Protection capabilities</strong></td>
<td>Uses single method</td>
<td>Multiple properties can be used</td>
<td>Less capable</td>
</tr>
<tr>
<td><strong>Protection against hacking</strong></td>
<td>Single layer only</td>
<td>Multiple layers like h/w, encryption, steganography etc.</td>
<td>Easily hackable</td>
</tr>
<tr>
<td><strong>Extension capabilities</strong></td>
<td>Not extendable</td>
<td>Extensible</td>
<td>No provisions for extensions usually</td>
</tr>
<tr>
<td><strong>Cost effectiveness</strong></td>
<td>Costly for initial setup and also maintain</td>
<td>Comparatively cheap for initial setup and maintain</td>
<td>Cheaper to setup</td>
</tr>
<tr>
<td><strong>Adaptability</strong></td>
<td>Not adaptable</td>
<td>Adaptable across OS and various h/w like PC, mobile etc.</td>
<td>Adaptable depending</td>
</tr>
</tbody>
</table>

From Table 5.1 it is seen that while using an extra piece of hardware is costly and its maintenance is not easy. It is not extendable. Software related hardware protection methods are easy to use but it may lead hacking. Hence it is advisable to use the existing hardware features for better protection and ease of use.

5.6 Summary

In this chapter the various methods used for existing software protection has been studied in detail. Comparison has been made between existing methods like hardware dongles, cd protection methods etc. From the comparison the conclusion is that instead of using traditional dongles it is much better to use hardware features that are already available in the system as they offer much better protection standard and at the same time is quite cost effective too.