International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 5 –NOVEMBER 2014.

Hacking Restrictions in IO Port

S N L SRIHARI YENDURI[*1] and P SAI GANESH[#2]

[*]*Lecturer, Department of CSE, KBN College, Vijayawada, A.P., India*

[#]*Student, Amritha School of Engineering, Bengaluru, India*

[1]srihari.yenduri@gmail.com

Abstract— Major problem faced by many organizations was, data Fabrication, Modification. This problem was mainly caused by the loops in the software. The IO Port in the computer is used to connect all the resources of the computer. The hacking is the process of gain the access to utilize the resources. In this model, I plan to authenticate the user at IO Port. It is a good practice to authenticating the user to access the resources.

In a traditional hacking, un-authorised users can access the resources of the computer, they can inject Trojan horses into our system then they can get control on the computer and uses the resources. In this paper I proposed to observer the data which is transferred from the IO port. We can also maintain the Login user information.

This is the best way to control the un-authorised persons to access our Computer resources.

Index Terms: IO Port addresses, Authentication Models, Security Attacks

I. INTRODUCTION

The definition of hacker has changed radically over the years. With the aid of the mass media, the word has developed a negative connotation rather than the positive one it used to have. Add ethical in front of hacker, and it's even more confusing. I will define these hackers with malicious intent as "crackers." Hackers can be categorized into the following three buckets:

Hacktivists: Those who hack as a form of political activism.

Hobbyist hackers: Those who hack to learn, for fun or to share with other hobbyists.

Research and security hackers: Those concerned with discovering security vulnerabilities and writing the code fixes.

The most dangerous hackers are Hobbyist hackers, they can take control on the others system and make a fun. In this scenario the system slow down and the real persons don not perform their works properly. In this article I would like to introduce a new technique to restrict the persons who are access the resources and applications from outside. Technology has also affected hacking activities. In response to legislation about privacy, business controls and terrorism, companies interested in capitalizing on the opportunities that exist have developed and manufactured sophisticated security hardware and software. The increased sophistication of these products has made the job of the hacker more difficult, and the casual hacker may stupidly get caught when attempting to circumvent a complex security system. This model we can implement as new authentication technique to store the information about the authenticated users

II. SECURITY ATTACKS

The field of network and Internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information. That is a broad statement that covers a host of possibilities.

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources.

This definition introduces three key objectives that are at the heart of computer security:

Confidentiality: This term covers two related concepts:

Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Integrity: This term covers two related concepts:

Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Availability: Assures that systems work promptly and service is not denied to authorize users.

Mainly security attacks can be categorized in to two types:

Active Attacks

Passive Attacks.

Active Attacks: Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

Passive Attacks: Passive attacks are very difficult to detect, because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal-fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of encryption. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

III. Authentication Models

We have several authentication models to authenticate the users of the system. The password protection is the basic one in the authentication models; the high model is OTP in the web authentication.

In this paper, we can use the minimum resources of the system like CPU, and OS are used to authenticate the user to utilize the system resources. The operating system can maintain the IO devices information. We have several IO ports for different devices

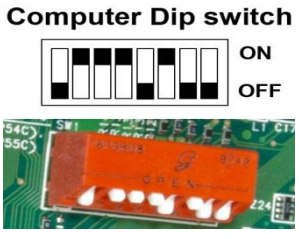
IO Authentication: The best practice to authenticate the resource of the computer is IO authentication. This is a proposed system; this can involve restricting the resources.

External Data Base: We may prepare separate database to store the information about the resources and connecting port information. In this way we can observe the resources whether it was properly utilized by the program or not

IV. IO Port

Alternatively referred to as I/O address, I/O ports, and I/O port address, the input/output port is what allows the software drivers to communicate with hardware devices on your computer. In your computer there are 65,535 ports that are numbered from 0000h to FFFFh.

The I/O port assignment can be made either manually using DIP switches or automatically using PnP. When configuring the I/O port of any device in your computer, it is important that it does not share the same I/O port as another device or you will encounter a hardware conflict.



DIP switches: A dip switch is a set of small switches found on computer hardware that can be turned to the ON or OFF position as shown in the picture below. Like computer jumpers, dip switches are used to configure computer peripherals such as hard drives, modems, sound cards, and motherboards. Today, with most computers using PNP, most hardware no longer requires manual configurations, so dip switches are not as common.

PnP: Short for Plug-and-Play, PnP is an ability of a computer to detect and configure a new piece of hardware automatically, without the requirement of the user to physically configure the hardware device with jumpers or dip switches.

Plug-and-Play was introduced on IBM compatible computers with the release of Microsoft Windows 95, where Apple Macintosh computers have always supported the ability to automatically detect and install hardware. For Plug-and-Play to operate properly on IBM compatible computers the user must have the below features

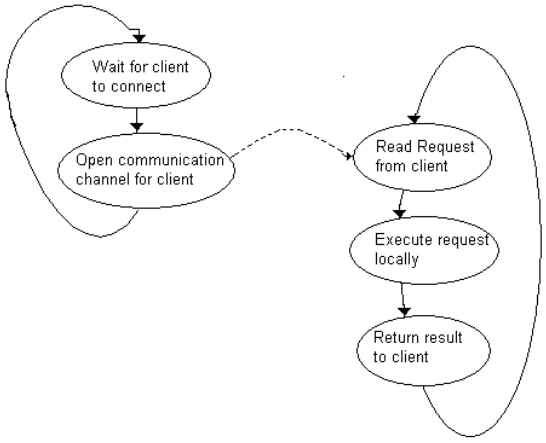
BIOS supporting Plug-and-Play.

Windows 95, 98, 2000, XP or later or another operating systems supporting PnP.

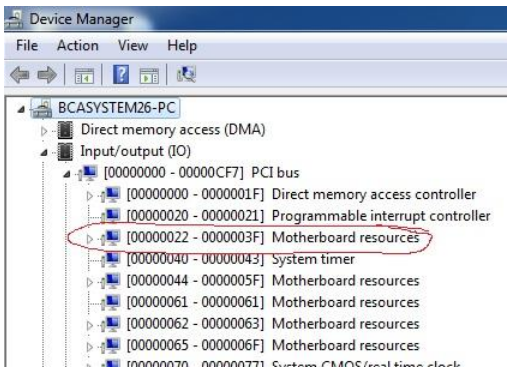
Peripheral with PnP support.

V. IO Authentication model (Proposed System)

In proposed system we can develop an application to store the information about the installed applications and the resources information.



General mechanism of IO communication can be by the CPU, in this way our application can works like interpreter between CPU and IO Ports



For example the Mother Board resources are connected at a specific address, that our application can store the all the port address and information about the resources, and it can maintain the activities of the resources in a log file.

From our application, we can track the resource and utilization. Any un-authorised person can utilize the resources, the application can restrict the access.

Algorithm 1:

Get the Port information form the system.

Observe the resource request from the Operating system resources queue.

Get the information of the resource request.

If the request is an authenticated request, then this request can be assign to CPU.

If the request from the un-authorised process, that process can be blocked and intimate to the user to kill the process.

VI. REFERENCES

[1] www.computerworld.com/article/2563526/security0/is-hacking-ethical-.html
[2] Cryptography and Network Security Principles and Practice.
[3] Operating System Principles, by Abraham Silberschatz, Peter Baer Galvin, Greg Gagne.