ISSN:2231-0711

Suraj Sawant et al | IJCSET |March 2013 | Vol 3, Issue 3, 116-117

Malicious Hardware

Suraj Sawant[1], Yogesh Vadam[2], Avadhut Bambarkar[3], Harsha Redkar[4]

[1,2,3] *Computer Engineering, RMCET Mumbai University, Ratnagiri, Maharashtra, India,*

[4]*Electronics and Telecommunication Engineering, RMCET Mumbai University, Ratnagiri, Maharashtra, India.*

***Abstract*— Virus attacking has been evolute since 1983, but all viruses were operates as software. Some of them been caught by antivirus, here we are introducing virus through hardware, hence antivirus won't be able to detect virus in hardware. Advanced attacking system, finding ghost drivers in any operating system, crashing down the system will be new applications in this project. In this we are implementing new hardware which contains microcontroller to send commands to operating system and virtual bridge will be responsible for connecting hardware and operating system. This technology of hardware virus is totally new and simultaneously we've found protection system too which will prevent this attack from being used with wrong intentions.**

***Keywords*— malicious hardware, virus attack, microcontroller, commands.**

I. INTRODUCTION

In February 2012 the personal computer virus was 26 years old. In that time computer viruses have caused the loss of untold millions of pounds, wasted decades in productivity, and wrecked companies. Now days we are facing so many computer attacks. The computer system is not much secured because of these attacks.

The Network attacks are done using different networking tools. The attacks are as

- Application layer attack
- Network Layer attack
- Virus attack
- Physical attack

Computer security experts say that this is just the beginning and as per the technology, attacks will be improving itself. The idea behind this is to put the virus in microcontroller with USB interface program and make it run when hardware will attached to system. We are introducing hardware dependent attack in which virus will be contained by hardware (microcontroller). This hardware will be used to attack. The microcontroller of any hardware contains some information along with its program, these programs may help to make virus possible to install in current system. The basic idea behind this project is to find out loopholes in system like information of booting of operating system is stored in one of the system file, if someone could harm that file then system will not be able to take next boot and system may get crash.

Aims and Objectives

The main aim is to make possible the hardware virus i.e. malicious hardware. Because such viruses can be introduced in future as per the computer security expert's results, the CSRI (Cyber Security Research Institute) did survey and found loss of millions of pound because of small virus, our country is not well known about such attacks. The objectives of attacks are:

- The objective is to make this attack possible.
- The antivirus won't be able to detect virus.
- The attack is possible without any administrative privileges.
- Any USB security software cannot prevent the attack.
- For prevention purpose, the external hardware of RTOS[3] is possible which will act as firewall for such kind of hardware attacks.

II. MOTIVATIONS: - VIRUS ATTACKS THROUGH PEN DRIVE

As we know the viruses spreads through flash devices like pen drives. But such viruses can be detected by the antivirus software of system. Sometimes new viruses comes into picture, but when virus patterns get updated by antivirus; those new viruses also get caught. Hence we conclude that if viruses come from hardware like flash devices from its device drivers then antivirus won't be able to detect those viruses. Hence we can just plug the hardware and deploy the virus. Such hardware attack can be come into picture for cyber attacking which will make the Operating System unable to boot next time. This concept can be possible by using Real Time Operating System (RTOS)[3] and many more technologies.

The microcontroller in pen drive is responsible for installing device drivers. Thus microcontroller plays an important role in our hardware attack. We are using the USB interface to connect the hardware to the system. Now days the USB interface is widely used because of plug n play facility.

And hence the USB interface will be future of any hardware specially used for application purpose.

III. IMPLEMENTATION WORK

The implementation work is quite interesting part of this project, because to design such kind of viruses we have to go through the device drivers. In this case we've to go through USB drivers and some USB protocol changes need to be done for this attack. This USB protocol can change the face of every USB drivers, because of its destructive property they can be manipulated by every programmer who is able to understand and design the drivers. For prototype purpose the first attack is applied to the Windows XP platform because of its vulnerabilities. There are several languages for designing device drivers like ASM, Embedded C, Java, C, C++ etc.

Since the core part of hardware is microcontroller, embedded technology will be required programming language.

As we have Real Time Operating System (RTOS)[3] concept for implementing hardware compatible language, we can deploy required tasks with semaphore[3] for resource acquiring purpose. The COM port in the system changes every time according to different USB port on the machine. The embedded c program will be responsible for sending commands to system.

According to our project, we are going to crash the operating system i.e. operating system won't be able to take next boot. Windows XP has several vulnerabilities which are open to access and enables the user to make harmful changes to that system. One of the vulnerability is system files like ntldr, ntdetect.com, sys files etc. The file called ntldr is one of the important file for having next booting information of system itself. So to deploy the virus we've to change the attributes of file first and then deleting the file. It is possible to change the attributes of any file in Windows XP. So we can change the attributes by using command prompt. The project prototype requires hardware containing microcontroller hence we use the hardware shown in Fig. 1.

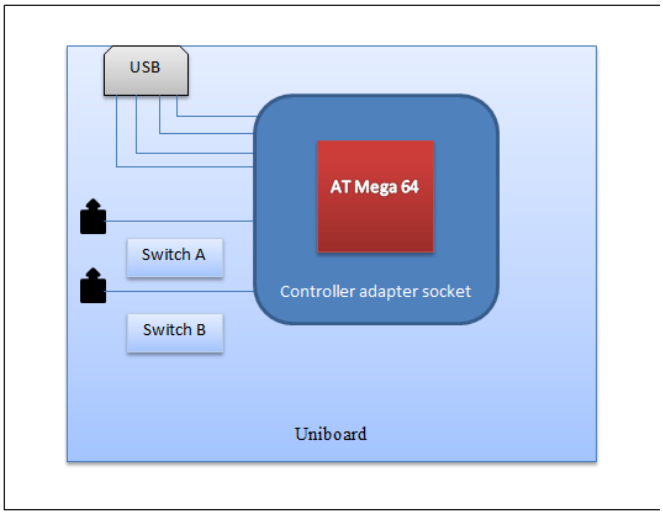

Fig. 1 Uniboard with AT Mega 64 microcontroller

The original hardware can be integrated by removing unnecessary components of the Uniboard like serial port, LED strips, CMOS battery, joystick, L293d IC etc. We can resize it as small as USB dongle or flash drive.

Since our hardware will be smaller, it will be easier to attack without any long procedure. The microcontroller is shown in Fig. 2

Fig. 2 AT Mega64 microcontroller

The destructive property of this hardware will produce so many prevention techniques in cyber attacking system. And such hardware attacks can be prevented.

IV. Conclusion

Our proposed concept is to introduce a new hardware attack in cyber attacking world, This may be an evolution of new attacking system as well as the prevention methods comes into picture for such attacks. Our concept is to crash the operating system as well as in Linux platform we can find out the ghost drives which are hidden, finding vulnerabilities in operating system.

Our future work on project is to find hardware protection in computer system. Because such attacks can be prevented by using hardware only. Hence USB device driver protocol can be change in the future.

V. References

[1] Jan Axelson. *Universal Serial Bus Complete Reference*. Third Edition.
[2] Neil Matthew and Richard Stones. *Beginning Linux Programming*, Fourth Edition
[3] Dogan Ibrahim, *advanced PIC microcontroller projects in C*.
[4] Edward N. Dekker, Joseph M. Newcomer *Developing Windows NT Device Drivers: A Programmer's Handbook*. Digital printed Edition
[5] Penny Orwick, Guy Smith. *Developing Drivers with the Windows Driver Foundation*
[6] http://msdn.microsoft.com/en-us/library/windows/hardware/hh706187(v=vs.85).aspx
[7] http://msdn.microsoft.com/en-us/library/windows/hardware/hh706183(v=vs.85).aspx