International Journal Of Computer Architecture And Mobility (0097-0161)
Volume 1-Issue 1, November 2012

FIREWALL AS A PORTABLE EMBEDDED SYSTEM

MONICA PANDEY
monicapandey2792@gmail.com
CDSE, INDORE

RAMITA AJMANI
ramita2809@gmail.com
CDSE, INDORE

PRANSHU PARMAR
pranshu.parmar@gmail.com
CDSE, INDORE

***ABSTRACT*— The firewall is defined as a set of components that restricts an access between a protected network & an unprotected network. Problem with firewall are it does not provide full protection against virus, prevention against previously unknown attack type and protection against insider/connection that do not go through it. A firewall provides a basic, but critical level of security for an embedded device, allowing it to block unwanted packets.**

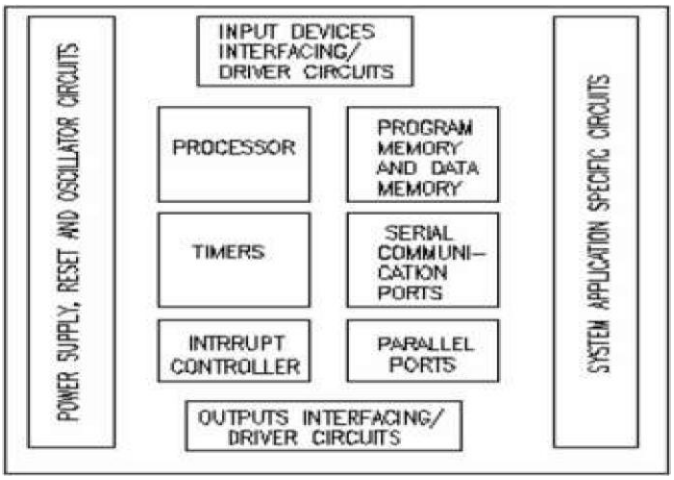
In the proposed paper of "Firewall as a portable embedded system", firewall is designed as a portable & multiple platform supported device. Firewall is implemented with an embedded system to safeguard both Internet & Intranet and it can update itself automatically. In this way, the functions of the firewall is combined with central security policy server into a portable embedded system, which can be realized as a network interface card.

Keywords— **Firewall, Embedded System; NIC; Portable Device; Intelligent Firewall; Packet Filtering**

I. INTRODUCTION

FIREWALL: Firewall is the most familiar method among relevant technologies for internet security. A home PC or enterprise network is not considered to be secure without a firewall. A firewall is a security guard placed at the point of entry between a private network and the outside Internet so that all incoming and outgoing packets have to pass through it. A firewall configuration defines which packets are legitimate and which are illegitimate. An error in a firewall configuration means a wrong definition of being legitimate or illegitimate for some packets, which will either allow unauthorized access from the outside Internet to the private network, or disable some legitimate communication between the private network and the outside Internet. Neither case is desirable. It does not provide protection against insider connection and previously unknown attack type [1]. It also does not provide full protection against viruses.

EMBEDDED SYSTEM: An embedded system is a combination of computer hardware and software, and perhaps additional mechanical or other parts, designed to perform a



specific function. The program instructions written for embedded systems are referred to as firmware, and are stored in read-only memory or Flash memory chips [2]. They run with limited computer hardware resources: little memory, small or non-existent keyboard or screen [3]. And hence they can be optimized to reduce size and cost and increased reliability and performance.

WORKING OF EMBEDDED SYSTEM: Embedded system basically works on two systems i.e. multiprocessor and multi-controller. In processor instructions are fetched by program flow and data path control unit. For ALU, execution unit is responsible.

PORTABLE DEVICE: It is a small hard drive designed to hold any kind of digital data [4]. When travelling, a portable storage device may be used to alternative to backup or purging memory cards if a computer is unavailable for downloading.

II. RELATED WORK

Charles Payne and Tom Markhan have introduced 'Distributed Firewall'. They have given an important new line of network defense. They have designed a distributed firewall which acknowledge that everything behind the firewall may not be trustworthy [5].

Vassilis Prevelakis and Angelos Keromytis have designed an 'Embedded Firewall' through which they have increased the protection of computing platform [6].

Alex X. Liu and Mohamed G. Gouda have introduced 'Diverse Firewall Design' in which they proposed diverse firewall design in two phases (design and comparison phase). They presented series of three algorithms [7].

Pennie Walters have worked on different devices, making them portable. He also told about the risk and how to overcome those problems which comes during using the portable device [8].

III. PROPOSED ARCHITECTURE

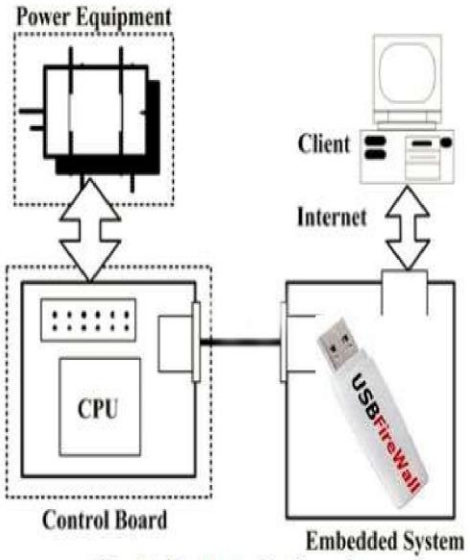


Fig. 1 : Hardware Configuration

IV. PROPOSED TECHNIQUE

Firewall is set up in a single choke point, if the firewall is broken due to power outage or flooding attack, all computers in the Intranet will be disconnected from the Internet.

In the proposed firewall system, the main firewall software is implemented on an embedded hardware so as to improve the efficiency of the conventional firewall. Here firewall system is designed as a portable embedded system which can support several multiple platforms. The system propose that the firewall is implemented on an embedded system. Here, the embedded system is actually a piece of hardware which can be connected to a computer device through the USB port and will directly act as a firewall from it as it would be present in multiple executable formats which can run according to the platform on which they need to work at that instance of time. In the proposed portable embedded firewall system, the memory would be divided into two basic parts and between them one would be the Read Only Memory and another would be a writable memory and both of them would have different essential purposes. [9] The main software logic would be more secure than the present firewall system as it is present in the ROM area of the hardware memory. In the writable memory of the proposed system a part of memory is present which is writable and thus the virus definitions could also be updated and the basic virus definitions would be present in the ROM only. The memory is divided into two parts so as to provide more security and flexibility [10] in terms of memory and efficiency. In the USB Firewall system even if the writable memory is affected then also it can be recovered by the ROM as the main software is not affected in any way. If no viruses or malicious activities are found on the system, the existence of the processor and software could be completely unnoticeable by a user of the system. The virus definitions are updated by the server through the internet so as to keep the system secure and protected.

V. WORKING

When the USB Firewall is connected to the system the voltage is supplied to the embedded system, the multiprocessor starts running. It will execute instructions from the program and data memory according to the program flow and thus it will first detect the type of operating system. If the operating system is supported then the supported software is run accordingly. The firewall system will thoroughly scan the files which are currently present on the system and at the same time it will also perform real time packet filtering. Each and every data which is going out or coming into the system will be filtered and thus the system would remain safe in both the conditions, whether it is internet or intranet. The set of rules or instructions are written in ROM so the internal memory of

USB firewall is always safe. When USB is connected to the system then it will perform the overall scanning. During the scanning of the files if any file or activity is marked as malicious according to the virus definitions in the system itself then that particular activity is blocked and the same is informed to the user. A log file is also created for further references. Also during the packet filtering, if any particular packet is found suspicious or malicious then access to that specific website or client (in case of intranet) is blocked and informed to the user. The USB Firewall is also capable of updating its virus definitions and those updates are stored in writable memory of the portable device. And thus a flexibility in memory and use of system is provided through this. While updating firewall download all the new virus signatures and attack types present on a targeted system. So in this way, firewall is up to date and is able to detect any kind of viruses whether they are previously known or the new one. So proposed firewall will not only detect the packets on network access but also scans the inside system. If due to the absence of updated virus definition a new kind of virus attacks the system, then also the system can be cured. In that case the approach of the portable firewall system would be to clean the client's system and its own writable memory area by the basic virus definitions present in the ROM. USB Firewall is a portable device so it can be removed from the system when system is not accessing the network. It can be placed on any other device with any supported operating system. And again the same working would be repeated for that system. And thus this approach is better than today's present approach.

VI. ALGORITHM

1) Connect the USB Firewall to the system
2) Detect the platform (OS)
    a. If supported,
    b. Then, continue
    c. Else,
    d. Exit
3) Accordingly run the software
4) Background scanning and real time packet filtering is performed
5) Check malicious activity
    a. If found,
    b. Then, block activity and report user
6) Update virus definitions
7) Network status
    a. If ON,
    b. Then process continues
    c. Else,
    d. User can port USB Firewall to another system

VII. RESULT

Features	Firewall	Portable Embedded (USB) Firewall
Portability	No	Yes
Platform Dependency	Yes	No
Memory Partition	No	Yes
Size	Small	Large
Speed	Less	High
Expandable Memory	No	Yes
Self-Updating	No	Yes
Recovery	No	Yes

VIII. CONCLUSION

The new proposed firewall system is in the form of a portable embedded system which is basically a piece of hardware and can interact through any system with a USB port. The device is capable of scanning internal files to find out any suspicious activity or virus any file infected by virus of that system and can also filter all the packets which are going out or coming in to that system so that it could provide security to both the networks i.e. internet and intranet. Its memory is partitioned in such a way that it is capable of updating itself and then also its main firewall software will be restricted to any change thus, providing more security and is more secure than the present system. It also provides

support to multiple platforms. The partitioning of memory into two parts which are Read Only Memory and writable memory provides it more flexibility, security and some more features like virus definition updating and system recovery in case of infection by virus or malicious software activity. And again portability is one of the brightest features of this USB Firewall system which makes it more flexible, reliable and much more usable.

IX. FUTURE WORK

The Portable Embedded Firewall System can be made more advanced by making it completely platform independent. The memory requirement could also be reduced but keeping the same flexibility. This can be achieved by using Firewall Compressor [11]. It can also be designed by providing it artificial intelligence [12] with help of neural networking, capable of making its own decision and can be made to remember the computer systems so that more flexibility, easiness and features could be provided to the system.

X. REFERENCES

[1] *R. Zaleaski; "Firewall Technologies", IEEE Potentials, Vol. 21, Issue 1, 2002, pp 24-29.*

[2] *Jen-Hao Teng, Chin-Yuan Tseng and Yu-Hung Chen; "Integration of networked Embedded System into Power Equipment Remote Control and Monitoring", I-Shou University, Kaohsiung, Taiwan*

[3] *S. Zhang, C. Zhu, J.K.O. Sin, and P.K.T. Mok; "A novel ultrathin elevated channel low-temperature poly-Si TFT" IEEE Electron Device Lett., vol. 20, pp. 569–571, Nov. 1999.*

[4] *Steve Evans; "Portable devices,technology and entertainment"*

[5] *Charles Payne, Tom Markham; "Architecture and Applications for a Distributed Embedded Firewall", Secure Computing Corporation*

[6] *Vassilis Prevelakis and Angelos Keromytis; "Designing an Embedded Firewall/VPN Gateway", Department of Mathematics and Computer Science, Drexel University, U.S.A.*

[7] *Alex X. Liu and Mohamed G. Gouda; "Diverse Firewall Design", Department of Computer Sciences, The University of Texas at Austin, Texas, U.S.A.*

[8] *Pennie Walters," The Risks of Using Portable Devices", "Protecting Portable Devices: Data Security," Security Tip ST04-020*

[9] *Kasom Koth-arsa[1], Surasak Sanguanpong[2], Pirawat Watanpongse[2], Surachai Chitpinityon[3] and Chalermpol Chatampan; "Experiences in Deploying Machines Registration and Integrated Linux Firewall with Traffic Shaper for Large Campus Network", [1]Engineering Computer Center, Faculty of Engineering*

[10] *WU Jin-hua, CHEN Xiao-su, ZHAO Yi-zhu and NI Jun; "A Flexible Policy-Based Firewall Management Framework", School of Computer Sciences and Technology, Wuhan, China*

[11] *Alex X. Liu, Eric Torng and Chad R. Meiners; "Firewall Compressor: An Algorithm for Minimizing Firewall Policies", Department of Computer Science and Engineering, Michigan State University, U.S.A.*

[12] *Eric Horvitz," Artificial intelligence", Microsoft research, Washington DC,*