3 L.O.S.S.-- Hard To Have Chernobyl

Pradeep Rai
Asst. Prof., CSE Department, Kanpur Institute of Technology, Kanpur-208001(India)

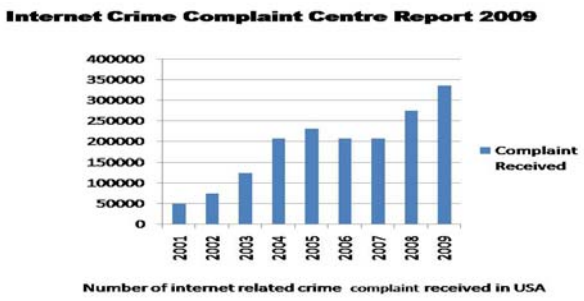
Shubha Singh
Asst. Prof., MCA Department, Kanpur Institute of Technology, Kanpur -208001(india)

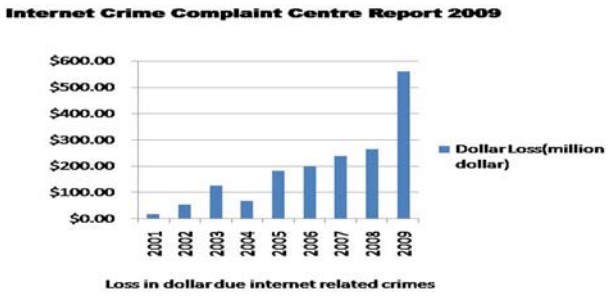
Abstract:
Organizations which are fully computerized and also are linked to outer world through common communication channels are prone to hacker's attack. Hackers search for vulnerabilities through different techniques such as operating system fingerprinting, stealth scanning etc. And then he or she starts exploiting the same vulnerabilities. Hackers can do the same because the servers have the single operating system for controlling all the functionalities and hardware of the machine. In this paper we are introducing a three layered system for controlling the hardware and functionalities of the servers so that exploiting the vulnerabilities, will become tougher. In this technique we are separating mother board of the server into 3 different layers having their own controlling systems and processors. And the data and the applications are separated in different layers as per there usage and confidentiality. These layers can only interact adjacently. And themiddle layer is the verification layers called Storewel layer.

***Keywords**:*
Server Security, Layered Systems, Operating System, Storewel Layer.

1. Introduction

In the recent age of computerized world all the servers, router and active network devices are prone to hacking. Due to the high proliferation of internet based applications almost every network servers which is directly or indirectly connected to internet turned up into a accessible resource for hackers. Same data is reflected in **Internet Crime Complaint Center (IC3) Annual Report 2009, USA as below[7]:**





By analyzing the data related to hacking we come across a fact that Hackers come up with novel, complex, simple or elegant ways of writing new software that restates or replaces the existing constraints thereby exposing either some new functionality or some of the original flexibility of the underlying machine. A typical approach in an attack on Internet-connected system is:

1. Network_Enumeration: Discovering information about the intended target.
2. Vulnerability Analysis: Identifying potential ways of attack.
3. Exploitation: Attempting to compromise the system by employing the vulnerabilities found through the vulnerability analysis.

In order to do so, there are several recurring tools of the trade and techniques used by computer criminals and security experts. The tools are given as below:-

1. Network Exploit:- A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery etc.
2. Vulnerability scanner:- A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners
3. Key loggers:- A key logger is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to

Manuscript received July 5, 2010
Manuscript revised July 20, 2010

confidential information typed on the affected machine, such as a user's password or other private data
4. Password Cracker
5. Spoofing attack
6. Root kit
7. Viruses, worm, Trojan horses etc.

The main cause behind all these intrusions is the single layered controlling; or rather we say that all computer machines have a single operating system. Having single operating system causes any intruder who has the knowledge of functioning of operating system, to access the information which has to be secured.
In this paper we are introducing a new system which is layered in nature. This system is layered in two fashions

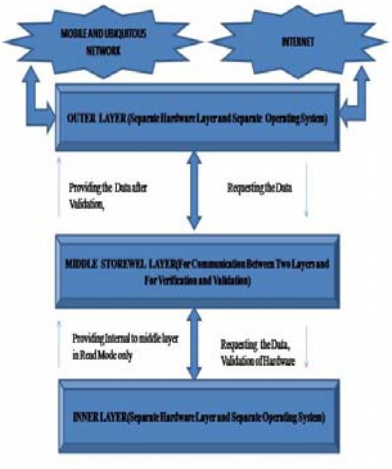
(i) 3 Layered Mother Board
(ii) 3 different Operating System.

This system has a capability to distinguish between the data which is of internal use and data which is for external use. This system stores data which is important and needs security into its inner layer and the data which is of external use to be store in external layer.

2. Three Layered Operated Secured System (3 L.O.S.S.)

In this system we basically separated the complete functioning of the server into 3 different layers. These layers are also physically separated as three different layers of main board. These layers have different type of tasks to do. The Inner and the Outer layers have their different full fledged operating System. The Middle layer also known as Storewel Layer has operating system which is not GUI based, it is only Command based operating system. Each layer have its own harddisk and necessary peripheral devices.
The description of the three layers is as below:

1. **OUTER LAYER**: This layer has its separate full fledged Mother Board and the Operating System. The function of this layer is to interact with the outer world.
   All the connections to outer world are through this layer. All sort of data communication to outside the organization is thorough this layer.
2. INNER LAYER: Inner layer also has its full fledged Mother Board and the Operating System. The Function of this layer is to store the information which is important and need high level of security. All the application which is running only for the sake of organization are installed and run on this layer. There is no linkage to the outer layer.
   This layer cannot directly interact with the outer world.
3. STOREWEL LAYER: This Layer resides in between the outer and inner layer. Configuration of the server and all the installed softwares are first having an entry in the storewel Data. New Hardware and software which has to be installed should have an entry in the storewel layer first. Interaction between the inner and outer layers is through this layer. This layer also validates the instruction passed by each of its adjacent layer. The operating system of this layer is command based and not GUI based. Change to this layers data is made directly by attaching a device to its external port to internet.

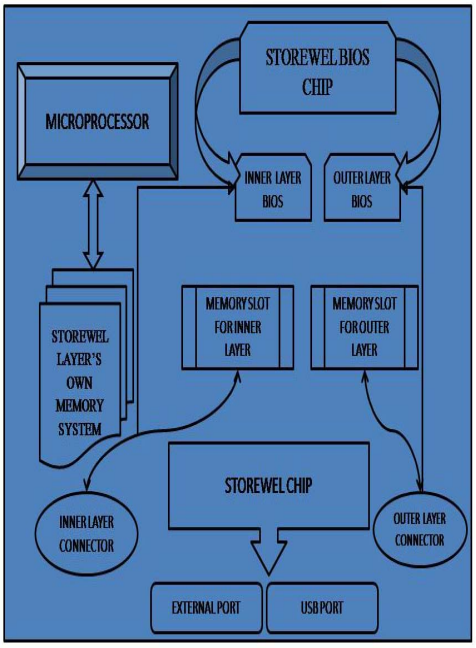


Three Layered Operated Secured System

3. Description of Storewel Layer

Storewel layer has following essential hardware elements:-

1. **Storewel BIOS Chip: -** This is the main BIOS chip of the System. It starts the booting of the System. It then transfers the control to its storewel memory for proper booting of the storewel layer operating system. This Main Storewel BIOS Chip also activate the BIOS chips of Inner and Outer Layers.
2. **Inner and Outer layer BIOS chip:-** This particular layer also contains the Inner and Outer Layer BIOS chips.

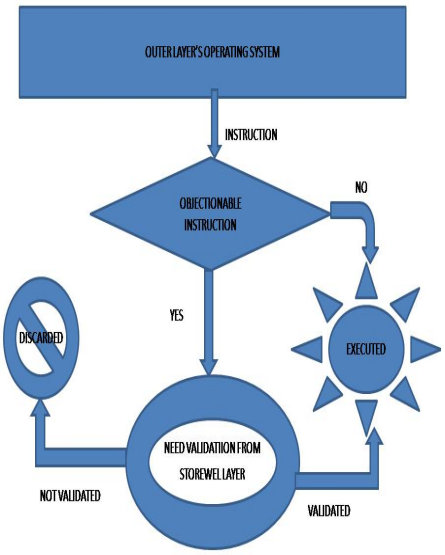


ESSENTIAL HARDWARES IN STOREWEL LAYER

3. **Storewel's Memory System:-** This is proper memory system containing Cache memory and RAM of this layer.
4. **Microprocessor: -** Microprocessor of this layer, which relatively having speed lower than the Outer and Inner layer's processor.
5. **Memory Slots for Inner and Outer Layers:-** This is the specialized memory slots for the instruction and data transfer from Inner and Outer Layers.
6. **Storewel Chip:-** This is the main Validation chip in this layer. It contains the tables for the following:-
   - **a.** Hardware Validation list, with unique id for each hardware already installed or to be installed
   - **b.** Software Validation list, with unique id for each software already installed or to be installed.
   - **c.** Instruction Validation list, for each instruction in the Inner and Outer layer's operating Systems.
   - **d.** Validation list for each application's instruction set installed on inner and outer layer.
7. **Inner and Outer Layer Connectors: -** These connectors are the interface between Inner and Outer Layer and the Storewel Layer.
8. **External Port and USB Port:-** These particular ports are only meant for attaching this layer to Internet.

4. Working of 3 L.O.S.S.

The main feature of this layered system is its ability to separate application and data according to their utility and safety. The 3 L.O.S.S. cannot be taken as networked or clustered systems; instead it has a working difference. The working of the operating systems of the outer and inner layers has a slight difference from the operating systems which are currently available, as when they are not performing any task which has any objectionable instruction in it then there working is similar to currently available operating system. But when they are performing any task which has objectionable instruction in it, then it has to validate from the middle storewel layer. Objectionable instructions are classified and stored in the storewel Chip. The inner layer only provides the data to the storewel layer as per the requirement. The inner layer contains all the data which needs security and of internal use only.



FUNCTIONING OF OUTER LAYER'S OPERATING SYSTEM

The capability of this secured system totally depends on the working of the Storewel layer. All the special feature of this system is due to storewel layer. The functions of the storewel layers are as follows:-

1. It validates the instructions coming from the outer layer's operating systems.

The validation process includes the following clarifications:

a. Whether the application or instruction within that application, which wants the data from inner layer has a privilege to access it or not. This all information is stored in the storewel layer's storewel chip.

b. Whether the instruction is already existed or not ?

2. This Storewel layer's storewel chip works as an extension to System's BIOS.This is the first hardware line which takes the control of the system after starting.
3. This layer also contains the Master Boot Record and it can use chain loading to shift the control.
4. In this System we can use Coreboot technology to load almost any Operating System.
5. Hardware and Software piracy can be somehow omitted by using this storewel layer. This layer can directly be attached to internet via its external port. The information within this chip can be changed by storewel website. After attaching the storewel layer to the internet we need a proper authorization to make changes in the information in the chip.

Only the hardware and software which are in list can only be installed to this server. So for installing a new hardware or software to this server we have to first append the list of hardware and software to the storewel chip with its proper id (which is the genuine unique id given by the manufactures). This unique feature also omits the possibility of attaching any hardware directly to the server for malicious purposes.

5. Improvements Over Current Systems

As in the current situation in the servers having single operating system, intruders just want to exploit the vulnerability of the system. If they somehow got the access to the inner core of the operating system they start extracting the inner information through which they can fulfill their desires. But in our proposed system the secured data and the information which is meant for organizational use is in the different layer and in different operating system. And these two operating system cannot directly interact with each other. They get only the validated information. This particular system is viable for big organizations where security is major concern.

6. Future Work and Proposals

To exactly implement the discussed system we have modify harwares software and even firmwares. The major change will be introduced in the current working of operating system.
And also we need several modifications in the architectures.

7. Acknowledgement

The authors would like to express their cordial thanks to **Prof. Raghuraj Singh (H.O.D., CSE Deptt,HBTI)** and **Mr. Anshul Pandey (Research Engineer Intel, USA)** and for their valuable advice.

References:

[1] Comer, D. (2007), The Internet Book: Everything You Need to Know about Computer
[2] Networking and How the Internet Works. 4th Ed. Prentice Hall.
[3] Erickson, J. (2003), Hacking: The Art of Exploitation. No Starch Press.
[4] Google Hacking Database. (2010). Retrieved January 20, 2010, from Hackers for Charity.Org website: http://www.hackersforcharity.org/ghdb/
[5] Shinder, D. L. & Cross, M. (2008), Scene of the Cybercrime. 2nd Ed. Syngress.
[6] http://duartes.org/gustavo/blog/post/motherboard-chipsets-memory-map
[7] www.ic3.gov
[8] http://www.sans.org/security-resources/idfaq/amap.php
[9] https://secure.sophos.com/security/whitepapers/index.html
[10] http://www.iaria.org/conferences2007/filesICIMP07/TutorialNetworkHackingCalforniaIaria.pdf
[11] http://www.cse.sc.edu/research/isl/agentIDS.shtml,probabilistic agent based approach for intrusion detection. Online article (Last assessed: July 06 2006).
[12] http://www.cs.unm.edu/~immsec/systemcalls.htm.Computer Immune Systems: (Last assessed: July 02,2006).
[13] http://www.dsto.defence.gov.au/publications/2345/DSTO-GD-0286.pdf. Online article (Last assessed: July 06 2006).
[14] http://www.windowsecurity.com/articles/Hids vs NidsPart1.html. Online article: (Last assessed: July 06 2006).
[15] N. B. Amor, S. Benferhat, and Z. Elouedi. Naivebayes vs decision trees in intrusion detection systems.
[16] In Proceedings of the ACM symposium on Applied computing, ACM Press, 2004, pages 420–424.
[17] D. Denning. An intrusion-detection model. IEEE Transactions on Software Engineering, vol. (SE-13),no. (2), 1987, pages 222–232.
[18] K. Ghosh. Learning program behavior profiles forintrusion detection. In Proceedings of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring, 1999, pages 51–62.

[19] O. Paul and M. Laurent, “A full bandwidth ATM firewall,” in Proceedings of the 6th European Symposium on Research in Computer Security ESORICS’2000, 2000.
[20] E. D. Zwicky, S. Cooper, and D. B. Chapman, Building Internet Firewalls. O’Reilly, 2000.
[21] A. Wool, “A quantitative study of firewall configuration errors,” IEEE Computer, vol. 37, no. 6, pp. 62 –67, June 2004.
[22] R. L. Ziegler, Linux Firewalls, 2nd ed. New Riders, 2002.
[23] S. Acharya, J. Wang, Z. Ge, and T. F. Znati, “Traffic-aware firewall optimization strategies,” in Proceedings of the IEEE International Conference on Communications, 2006.

Pradeep Rai received his bachelor degree in computer Science & Engineering from KNIT, Sultanpur in the year 2002 and M.Tech in computer Science in the year 2008. Currently he is working as Asst. Prof. in CSE Department at KIT, Kanpur. His area of interest includes VPN, wi-fi networks, network Security. His many research papers related to Computer Security are published in several international journals.

Shubha Singh received her Master degree in Computer Applications from Agra university in year 2002 and M.Tech in computer science in year 2007. She has worked as associate in govt project at IIT, Kanpur. Presently she is working as Asst. Prof. in Compute Application Deptt. At KIT ,Kanpur.She has more than 8 years teaching experience. Her areas of interest includes DBMS,Networks and Operating Systems. Her research papers related to Computer Security and semantic web are published in several international journals.