International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 03 | Mar-2018 www.irjet.net p-ISSN: 2395-0072

SANDBOX TECHNOLOGY

Arockia Panimalar.S[1], Tamilselvi.K[2], Vani.K[3]

[1]*Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*
[2,3] *III BCA 'A', Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*

Abstract: *The sandbox technology aims to create a secure and virtualized sandbox environment at the level of respective applications. The sandbox is considered to have a minimal impact on the semantics as well as the program which is executed at a time and provides an efficient sandbox configuration. The malwares which are called as viruses, worms and bolts have an anti analysis functions to confirm the connectivity of certain hosts which detects the virtualized environments. To avoid the impacts from the Internet, the analyzed environments should be disconnected from the Internet but they must be able to make malwares believe that they are connected to the real Internet.*

Key Words: **Sandbox, System Sandbox, Operating System Security, Controller Nodes.**

1. INTRODUCTION

Sandbox technology is used to avoid a security threat which runs as separate programs in computer systems. Sandbox is especially used to execute the code which is not tested or it may be possibly unverified without harming the host machine or the operating system. A set of guest programs are set for the disk to run in a tightly controlled set of resources. Sandbox in a testing environment is that the untested codes can be changed and production environment can be experimented as out righted which includes revision control and web development.

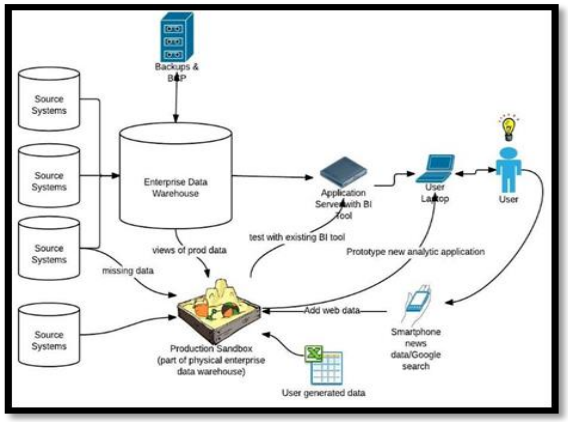

Fig 1: Production of Data Warehouse in Sandbox

The live servers are protected by sandboxing where the source code gets distributed and the changes may cause some of the damages to a mission critical system. The main aim of the sandbox is to test the minimal functionality of the code or to test the programs accurately under the wed development process. To access the development environment variables are needed. The sandbox can be also called as a test server or as a working directory or directory server. This test directory is built with the help of revision control software. The revision control softwares are CVS and sub version (SVN). These softwares are used by developers to copy a source code tree or a branch of code to work and examine the process. After testing the code, if the developers find any changes in the code they should move back to the own sandbox and merge with their repositories and thereby it will used by other users or else by end users.

2. IMPLEMENTATION OF SANDBOX

A sandbox is especially implemented for testing the software in an operating system environment. It is also used for controlling the resources like file descriptors, memory, file system space. If the implementation is made by any unified process then individual system resources are accessed which are provided by the operating system. So the system sandbox provides access control to the individual operating system components.

3. KEY SYSTEM OF SANDBOX

Some of the operating system key system components are files, the registry, network interfaces, the CPU, I/O, locks and processes.

A. Files

The user and operating system data are stored in the file system. If there is any change in the file system without the knowledge of user then the data can be removed or it can be modified directly using the operating system security. The target of file system is to access the requests which are to be mapped directly to the required directory containing the root of the file system. There are two ways for accessing the file: 1) host of the file system does not know the content 2) another process reads the arbitrary files in the host system.

B. Registry

The registry contains the configured data of operating system and also the other applications. As registry is the main component, it should be specifically secured. Malware doesn't alter the data which is stored in the registry.

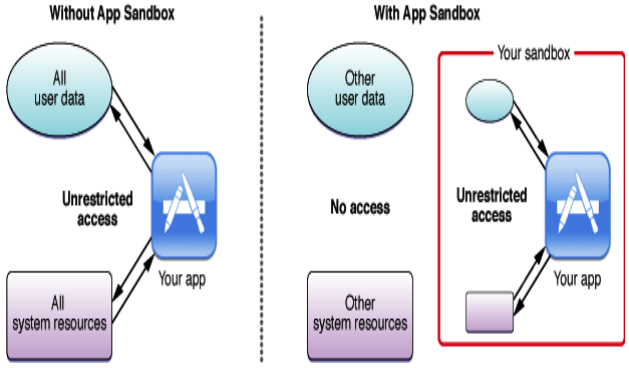

Fig 2: Sandbox

C. Network Interfaces

Network interfaces are the computer worms which are contacted through remote servers and also they coordinate their activities within the system. Network is the creation of independent environment where the process of arbitrary communicates with the local network and also on the internet. Any of the process is unique with its virtual IP address then the kind of isolation does not get supported with the sandbox systems. Network isolation is the most specific sense which is used for controlling and limiting the access during the process of communication on local network and also on the internet.

4. ISOLATED SANDBOX AND CONTROLLER NODES

The nodes can be built with the help function based on the isolated sandboxes. When the environment is disconnected, it can be managed through actions such as executing and introducing specimens. The related logs are collected and carried out without network connections. It can separate virtual local area network which acts as a security gateway and a controller node. The control messages from the management terminal are maintained by mimetic internet and the malware incubator. The nodes are collected from the malware incubator.

5. MIMETIC INTERNET

The main role of mimetic internet is to identify the mistakes made by the malwares. The end view host can be modeled as the collection of behavior to target the hosts which involves services like the count of gateways and some of the link qualities such as the bandwidth and a term called as RTT which targets each hosts. The mimetic internet consists of emulated routes and a mimetic target hosts. Mimetic internet constructs on the virtual environment because it helps to detect the virtualized environment techniques.

6. CONCLUSION

The goal is to design a system sandbox in the Microsoft windows system which provides security for the executed applications. The sandbox model helps in solving the current security problems. The security test shows the functionality model. The main drawback of the sandbox is the waste of storage space. The mimetic internet and the malware incubator are used with a renewable node. A tool is used by developers and it is applied to java sandbox to the applications. Due to the large number of existing frameworks and libraries without the knowledge arise some of the complaints which are too difficult

7. FUTURE SCOPE

The mechanism of malwares is isolated in a sand box. By using the mimetic internet the malware incubator can be renewed actual node. The specimens can be enabled to download the files and to join the command through real networks. The applications of the mimetic internet can be experimented by IP trace based routing devices.

8. REFERENCES

[1] E. Skoudis and L. Zeltser, “MALWARE – Fighting Malicious Code”, Prentice Hall PTR, ISBN 0-13-1014056, Pearson Education Inc., 2004.

[2] S. Miwa and H. Ohno, “A Development of Experimental Environments ”SIOS” and ”VM Nebula” for Reproducing Internet Security Incidents”, Journal of the National Institute of Information and Communications Technology, Vol.52 Numbers 1/2 (pp.23-34) 2005, ISSN 1349-3205, Oct. 2005.

[3] E. Eilam, “Reversing: Secrets of Reverse Engineering”, ISBN 0-7645-7481-7, Wiley Publishing, Inc., 2005.

[4] M. Vrable, J. Ma, J. Chen, D. Moore, E. Vandekieft and A. C. Snoeren, “Scalability, Fidelity, and Containment in the Potemkin Virtual Honeyfarm”, Oct. 2005.

[5] S. Crosby, D. E. Williams and J. Garcia, “Virtualization with Xen: Including Xen Enterprise, Xen Server and Xen Express”, Syngress Media Inc., ISBN 1-597-491675, 2007.

[6] T. Miyachi, K. Chinen, and Y. Shinoda, “StarBED and SpringOS: Large-scale General Purpose Network Testbed and Supporting Software”, Valuetools, Oct. 2006.