Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 1– No.3, February 2015 – www.caeaccess.org

Isolation of Private Network from Internet, Secure Internet Virtual Environment

Ahmad Alamgir Khan

ABSTRACT
There are numerous ways to secure computers including utilizing security-aware design techniques, building on secure operating systems and installing hardware devices designed to protect the computer systems. At the same time, many organizations are improving security and many types of cyber criminals are finding ways to continue their activities. Cyber threats will continue to rise, interconnectivity of people, devices and organizations, poses more risk than ever before. The employees poses a significant risk to an organization, due to the lack of security awareness and inherit insecure nature of the Internet. The dependency on Internet has increased enormously and staying connected is no longer choice but necessity. So keeping this is view, this research paper aims to present a novel approach to isolate the private network (Organization or Home Network) from the public (Internet). It is an approach in which the Internet is accessed through Open Source Secure Customized Linux Operating System where only necessary packages are installed. The Customized OS is configured with necessary security features. In the Host Machine the customized OS runs through a Virtual Machine in its own separate network which is connected to Internet. There will be no interconnection between the Host and the VM network. By isolating the Private from Public network, there will be significant improvement in the security of the private networks.

General Terms
Hardware and Software Virtualization, openSUSE, Subnetting, Network Isolation, Organizational Security, et. al.

Keywords
SIVM (Secure Internet Virtual Environment), VMWare Player, VM Virtual Box, SUSE Studio, Linux Packages, Private and Public Network Isolation, Host Machine, Sandboxing.

1. INTRODUCTION
Almost every type of cyber-attack is on the rise. In 2009 [1] respondents to the CSI Computer Crime and Security Survey admitted that malware infections, denial-of-service attacks, password sniffing, and web site defacements were significantly higher than in the previous two years.

Cyber threat will continue to rise, interconnectivity of people, devices and organizations, poses more risk than ever before. The employees poses a significant risk to an organization, due to the lack of security awareness. Around [2] 40% of the world population has an internet connection today. In 1995, it was less than 1%. The number of internet users has increased tenfold from 1999 to 2013. The first billion was reached in 2005. The second billion in 2010. The third billion in 2014. The 2014 global study of U.S.-based companies, which spanned seven nations, found that over the course of a year the average cost of cybercrime climbed by more than 9% to $12.7 million for companies in the United States, up from 11.6 million in the 2013 study. The average time to resolve a cyber-attack is also rising, climbing to 45 days, up from 32 days in 2013.

Cybercrimes are the biggest threat to any organization and people. It is clearly evident that immediate steps must be taken to secure the growing threat. However, the challenges are numerous and the task is not an easy one, everyone is not aware of the security risks and threat they poses when they are connected to Internet. The latest firewalls, host intrusion prevention systems, antivirus or spywares cannot guarantee 100% security. Instead they provide false assurance of security. Yet, it is crucial to have all these security controls in place. As long as any device is connected to Internet it is constantly under grave danger. It is very likely that the separation of private network from the public will be mandatory for providing efficient security. In this paper, the focus is primarily on having a secure customized operating system with all the necessary security features built-in. By selecting only necessary Linux packages for Internet to function reduces the surface area for attackers. This entire operating system is essentially sandboxed, as it doesn't have access to anything outside of the virtual machine. The Internet could be accessed on VM's operation system as if it is accessed on a standard machine. Virtual Machine support snapshot feature, if incase, it is attacked by viruses, spyware, malware or hacked, a user can roll back to the stable previous state. Since, there is no access from VM to Host machine, infected VM may not cause any harm to the host machine. Both the Host Machine and VM has latest Antivirus, spyware and firewall installed.

In this paper, the SIVM (Secure Internet Virtual Machine) aims to put forward a new approach to overcome the limitation of existing security mechanisms.

The paper is structured as follows: Section 2 provides a brief overview of the background and related work. Section 3 presents an example that shows how the SIVM works, and provides details about its implementation. Section 4 presents future work and concludes the article.

2. BACKGROUND & RELATED WORK
Antivirus or antimalware is often efficient in protecting the known virus, but inefficient for newly released virus. Hackers always release new variants of virus that evades the latest antivirus softwares. Till antivirus vendors updates their signature database, most of the organizations are already compromised. So it is clear that just having an antivirus/antimalware/antispyware is not enough to protect the system. Some advanced antivirus software [3] includes heuristic-based detection methods in addition to signature-based detection. The major difference between the two methods is that unlike signature-based detection, heuristic-based detection has the capability of detecting malware that was previously unknown. The heuristic-based detection methods has its disadvantages too, first it takes long time to complete which utilizes all the hardware resources thus making system slow. Second it may produces false positive by detecting a valid program as threat. This too doesn't provide

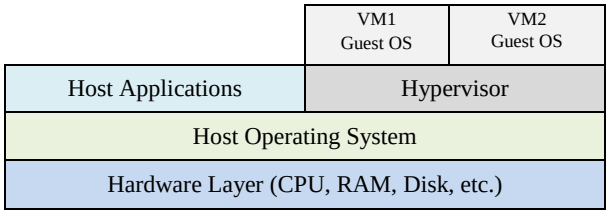
an efficient security solution. Users are left with no choice and no full proof security measure exist till now. They are simply exposed to multiple threats on the Internet. According to the Norton Cybercrime Report of 2012 [4]:

24% of online adults globally "can't live without the Internet"
41% say they "need the Internet in their everyday life"
32% of social network users think they would "lose contact with friends" if they had to live without social networks

The dependency on internet is growing, more and more people are now facing the imminent threat. SIVM can provide more security by isolating the private network from the Internet. It limits the surface area for the attackers and helps to recover quickly. It does not expose the Host (real) machine to the internet thus keeping private files / organization safe.

Hardware virtualization [5] or platform virtualization refers to the creation of a virtual machine that acts like a real computer with an operating system. Software executed on these virtual machines is separated from the underlying hardware resources. For example, a computer that is running Microsoft Windows may host a virtual machine that looks like a computer with the Linux operating system Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

Fig 1. VM Architecture



OpenSUSE [6] is a PC operating system based on GNU and Linux. It's a free/open source and gratis alternative to e.g. Microsoft Windows with many advantages. openSUSE is suitable for laptops, desktops, netbooks, servers and multimedia center PCs at home or in small offices. openSUSE is among the leading GNU/Linux distributions and is also one of the oldest existing ones.

The Microsoft's Azure RemoteApp [7] preview builds on the Windows Server Remote Desktop Services infrastructure while also leveraging Azure's global scale and utility-grade reliability. The service, released, enables user to run Windows applications on a variety of devices from the Azure cloud. RemoteIE provides access to the latest Internet Explorer on the Technical Preview via Azure RemoteApp. With RemoteIE, user can test the latest preview version of IE from your Windows, Mac, Android or iOS device.

3. SIVM IMPLEMENTATION

SUSE Studio is free and easy to use online Linux distribution creation tool where users can create their own customized distributions. Using SUSE studio [8], a Linux distribution is created. Only the necessary packages required for internet connectivity and security of OS are selected. It is easy to customize, system administrator can easily create own custom distribution. After careful selection of packages, the SIVM is built in (.vmdk) format as shown in Fig 2.

Fig. 2 Building SIVM Packages using SUSE Studio

SUSE Studio		
SIVM	SIVM openSUSE 13.2, GNOME 32-bit x86, based on openSUSE 13.2	
Default Format:	VMware Workstation / VirtualBox	
Additional Formats:	☐	USB Stick / Hard Disk Image
	☐	Live CD / DVD (.iso)
	☐	Preload ISO (.iso)
	☐	OVF Virtual Machine (.ovf)
	☐	Hyper-V Virtual Hard Disk
Build		

The format is VMDK (Virtual Machine Disk), it is a file format that describes containers for virtual hard disk drives to be used in virtual machines like VMware Workstation or VirtualBox. Since, the default format is VMDK, there is no need to install the OS, and it directly operate on the VMware or VirtualBox emulator on the host machine. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it.

The Host machine which runs on Windows 7/8 is updated and have latest updates for antivirus/malware/spyware. The best practices to secure the Windows 7/8 are applied, which includes drive encryption, firewall settings, disabling unneeded services, renaming the user accounts, changing default passwords and the most important accessing the machine using low privilege user account. The host machine network is separated from the SIVM, only SIVM have access to Internet while Host machine can only access the organization private network.

Since there is separation of networks, if SIVM is attacked or compromised it may not transverse to the host network. It is recommended to take SIVM snapshots regularly so that it can be restored to good working state. It is one of the benefit of SIVM that the restoration of functionality is easy, fast and secure. It is recommend not to install additional guest OS additions as it may pose some risk to the host machine.

There are some guidelines users should follow while using SIVM, they should not store any sensitive files, passwords or any other information. The communication between the guest and host should be restricted. And in case suspicious behavior of SIVM is detected, users should immediately report to the security team or in case of home user, they should restore the SIVM to the last good backup.

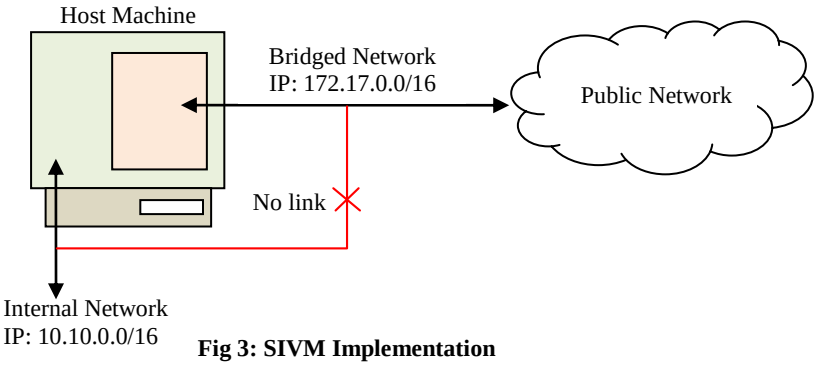


Fig 3: SIVM Implementation

4. CONCLUSION

Virtual environments are a tool that security researchers and security software use to automatically analyze and detect malware. But according to Symantec research [9], virtual machines (VMs) are becoming more common in enterprise operational environments—so malware authors are learning to write their code to attack that infrastructure more effectively while avoiding detection.

There have been some white-papers published over the years describing ways that researchers have managed to infest a host OS from a VM. These are usually seen, rightly so, as security vulnerabilities by the VM vendors and treated as such. Since those papers, Intel has made some significant processor instruction-set improvements in allowing separation of VM and hypervisor. In 2008 [10], Core Security Technologies have discovered vulnerability in VMware's desktop virtualization software that allows an attacker to gain complete control a system and launch executable files on the host operating system.

The Virtualization is becoming the new trend in cloud computing and computing in general, so there is great need to address the security related issues. There is lot of future scope for researchers to work on securing the VM infrastructure. Many further improvements needs to done in order to keep the Host and VM secure and reliable. The existing or forthcoming pitfalls in Hardware layer, hypervisor and guest VMs need to be addressed. Tara Seals [11] from Infosecurity magazine stated the fact that the use of virtualized systems in a corporate environment can provide a lot of benefits, but these systems need some special attention paid to security.

Cybercrime is increasing rapidly but many users are unaware of the facts. Criminals are finding new ways to accomplish their malicious goals. It is the responsibility of the Internet user to be aware of the threats, and be caution while performing any action on network. It is important to be aware of dangers of internet attacks and their devastating impact.

5. REFERENCES

[1] Richardson, R. (2010). 2009 CSI Computer Crime & Security Survey. Computer Security Institute. Computer Security Institute.

[2] http://www.internetlivestats.com/internet-users/*1:21 pm 19 Jan 2015*

[3] http://antivirus.about.com/od/virusdescriptions/a/Antivirus-Software-Technology.htm *2/18/15*

[4] http://in.norton.com/cybercrimereport/promo *Wednesday 2/18/2015*

[5] Turban, E; King, D; Lee, J; Viehland, D (2008). "Chapter 19: Building E-Commerce Applications and Infrastructure". Electronic Commerce A Managerial Perspective. Prentice-Hall. p. 27.

[6] www.opensuse-guide.org 27 Jan 2015 at 12:43 pm *Updated: 23 November, 2014*

[7] http://blogs.msdn.com/b/ie/archive/2014/11/02/announcing-remoteie-test-the-latest-ie-on-windows-mac-os-x-ios-and-android.aspx *27 Jan 2015 at 12:47 pm*

[8] https://susestudio.com *accessed: 28 Jan 2015 11:23 am*

[9] http://www.infosecurity-magazine.com/news/malware-no-longer-avoids-virtual/

[10] http://www.zdnet.com/article/researcher-critical-vulnerability-found-in-vmwares-desktop-apps/ *Wednesday 2/18/2015*

[11] http://www.infosecurity-magazine.com/news/malware-no-longer-avoids-virtual/*Wednesday 2/18/2015*