Volume 2 No. 3, March 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

©2012 ICT Journal. All rights reserved

http://www.esjournals.org

Managing Micro-computer Systems Vulnerabilities in an Institutional Network – The Case of IBB University, Lapai, Nigeria

Abdulrahman Abdulganiyu
Department of Math's/Computer science
IBB university Lapai, Niger State, Nigeria

ABSTRACT

Information security problems are currently a widespread and growing concern that covers most of the areas of society, such as business, domestic, financial, government, healthcare, and so on. Vulnerability has a high potential risk allowing a lot of destructive things happen in the computer as remote code execution, alteration of computer system files and files owns by the organization making the probability of a computer infection with nasty. Using a systematic approach, the paper offers a framework to deal with such vulnerabilities. The framework suggests specific courses of action for two possible scenarios. When there is no present threat, a proactive approach is suggested. When one or more threats are present, a reactive, Classification approach is suggested. Both approaches will be a strategic method for improving effective and efficient management of micro computing vulnerabilities. A related framework can be used in managing security vulnerabilities of other micro-computing devices in addition to desktops and laptop computers. A real case scenario from a network at the IBB University Lapai, Niger state, Nigeria is used to illustrate the proposed framework.

Keywords: *Micro- computing; cyber security; vulnerability; management; managerial approach, hazard*

I. INTRODUCTION

Computers are widely used in private, commercial, and governmental operations to store vast quantities of information. In many cases the information constitutes a record vital to the continued functioning of organizational systems, particularly in the case of personal data, stock data, and financial or accounting records. Organizations use remote access to information systems to streamline their business processes, become operationally efficient, and to gain competitive advantage. However, the global reach of information systems has raised concerns over security and has made organizations more Vulnerable to security threats [1]

Organizations must pay special attention to information security Vulnerabilities and ensure that their Micro-computers, and other devices and networks are not compromised as a result of this increase in mobility. However, while most organizations consider vulnerability management critical to their operations, few have vulnerability as an integrated part of their operations. This paper offers a managerial framework to solve the issues of management information systems vulnerabilities with a special focus on micro-computers and their use for remote access to organizational networks.

The proposed framework will help system administrators to scan and get rid of vulnerabilities associated with connecting desktop and laptops to internet. Once an assessment is made, the System administrator can managed such vulnerabilities in a systematic and efficient manner [2]

Also, the framework suggests a step-by-step procedure to managed vulnerabilities when the system is under attack, or monitoring and removing vulnerabilities when threats are present. The paper is organized as follows. The vulnerabilities of microcomputer in accessing in internet network. The next section discusses the modelling framework and practical recommendations for system administrators. This framework includes a proactive systematic approach to continuously evaluate the set of vulnerabilities and a technique to identify vulnerabilities that arise from unexpected interactions between system components. Finally, conclusions and recommendations [3]

II. VULNERABILITIES OF MICRO-COMPUTING

Microcomputers are the smallest but most important category of computer systems for end users. However, microcomputer have become much more than small computers used by individual persons organization. Their computing power now exceeds that of mainframe at a fraction of their cost easy. For this reason, they have become powerful professional workstations for use by end users in business and other organizations. Most microcomputers are single user computers designed to support the work activities of a variety of end users.

They have been and will continue to be the computers of choice for individuals and organizations. Some

International Journal of Information and Communication Technology Research

©2012 ICT Journal. All rights reserved

http://www.esjournals.org

microcomputers have become popular because they allow professionals and knowledge workers to access their information when they are travelling or from home offices and at the same time they offer high storage and processing capabilities. The shift toward micro-computing introduced new set of vulnerabilities for information systems. However, a majority of vulnerabilities arise due to interactions among several components such as the operating system kernel; file system, server processes, etc. [4] [5]

Microcomputer are considered by most organizations as the greatest security threat and the most difficult to maintain. A timely and efficient response to microcomputer vulnerabilities has been a major concern for organizations and their system administrators. Micro-computing vulnerabilities can be classified into two major categories: system vulnerability, and internet vulnerability. A brief discussion of those categories is provided below along with a suggested course of actions. [6]

A. System Vulnerability

Micro-computer is a popular target by intruders. Because intruders want what you've stored in your system. They look for bank account information, information used by organization and anything else they can find. By stealing that information, intruders can use your kept secret information and services. Intruders also want your computer's resources, like hard disk space, your fast processor, and your Internet connection. They use these resources to attack other computers on the Internet. In fact, the more computers an intruder uses, the harder it is for law enforcement to figure out where the attack is really coming from.

Micro- computers are typically not very secure and are easy to break into. When combined with organization high-speed Internet connections that are always turned on, intruders can quickly find and then attack organization computers. While intruders also attack organization computers connected to the Internet through dial-in connections, high-speed connections (cable modems and DSL modems) are a favourite target. No matter how an organization is connected to the Internet, intruders' attacks are often successful. Many organizations don't realize that they need to pay attention to computer vulnerabilities.

B. Internet Access Vulnerability

Employees and end users within an organization may unknowingly introduce malware on the network when they run malicious executable code (EXE files). Sometimes they might receive an email with an attached worm or download spyware when visiting a malicious website. Alternatively, to get work done, employees may decide to install pirated software for which they do not have a license. This software tends to have more code than advertised and is a common method used by malware writers to infect the end user's computers. An organization that operates efficiently usually has established ways to share files and content across the organization. These methods can also be abused by worms to further infect computer systems on the network. Computer malware does not have to be introduced manually or consciously. Basic software packages installed on desktop computers such as Internet Explorer, Firefox, Adobe Acrobat Reader or Flash have their fair share of security vulnerabilities. These security weaknesses are actively exploited by malware writers to automatically infect victim's computers. Such attacks are known as drive-by downloads because the user does not have knowledge of malicious files being downloaded onto his or her computer. In 2007 Google issued an alert 1 describing 450,000 web pages that can install malware without the user's consent. [7]

III. MANAGING VULNERABILITIES OF MICRO- COMPUTERS AND INTERNET ACCESS

Managing vulnerability in an organization is to protect the mission and assets of the organization. Therefore, risk management must be a management function rather than a technical function. It is vital to manage systems vulnerability. Understanding the vulnerability, and in particular, understanding the specific vulnerability to a system allow the system administrator to protect the information system commensurate with its value to the organization. The fact is that all organizations have limited resources and risk can never be reduced to zero. It is very important that a continuously improvement plan is in place and vulnerabilities are dealt with in a timely manner and preferably before a threat occurs. Such an approach requires that security perspective is shifted from technical to managerial. The main goal of addressing vulnerabilities will be to improve business resiliency and continuity [8][9]

A. Managing Vulnerabilities: No Present Threat

System administrators must continuously work to reduce the number of vulnerabilities present at any time during normal business operations. Even when there is no immediate threat a systematic, process based, proactive approach must be followed. This approach has three major steps:

1. Identify and classifying present vulnerabilities in the IT security area

International Journal of Information and Communication Technology Research

©2012 ICT Journal. All rights reserved

http://www.esjournals.org

2. How to reduce the likelihood of successful attacks
3. Monitoring and removing vulnerabilities with specific course of action

Identification and classifying of Vulnerabilities

In most areas of life, prevention is better than cure, and security is no exception. When there is no threat to the system in an organization, the system administrator needs security related information. For any security-aware enterprise, this is a huge task.

If you take a look at the incident response process, in every phase, valuable information is collected. In addition to the logs produced by various components of the computing infrastructure such as database, web and application servers and networks, there are security devices such as firewalls, intrusion detection systems and VPNs which produce traffic logs. An enterprise needs a policy, process and tools to manage all this information effectively to decipher evolving vulnerabilities, so future incidents can be prevented, deterred or responded without causing any damage to the organization's assets. These will help system administrators to evaluate potential vulnerabilities of the system[10]. Reference suggests a series of vulnerability categories related to internet access as shown in the Table I. For those Vulnerabilities which are present the administrator must specify any symptom(s), level of risk, and possible attack (s). This process is illustrated with a real case scenario as described below.

TABLE I: vulnerability -threat classification

Vulnerability	Risk	description	Propagation
Worm.Win32.AutoRun.beot	high	Worm copies itself to local disks and accessible network resources. It is Windows (PE-EXE file). It is 47733 bytes in size. It is packed by FSG. Unpacked file size is about 160 Kb. It is written in	The worm copies its body at all writable removable disks connected to the infected computer. The file "AutoRun.inf" is created together with a copy at the root of an infected disk. It provides for a copy to run each time a user opens an infected removable disk using "Explorer".
Trojan.Win32.Agent.nbcc	High	Trojan program that performs malicious activities in the user's system. It is a Windows (PE64 DLL-file). It is 83968 bytes in size. It is written in C++.	The Trojan allows access to the infected system and has a number of commands to manipulate (search, create, move, delete) files and folders, downloading and running files, terminating the processes and logging out of the system.
Trojan.MSIL.Agent.aor	Low	This Trojan is designed to steal confidential user information. It is a Windows .NET application (PE EXE file). It is 1 116 397 bytes in size	The collected data is saved to the following file: %Temp%\TMP.dat and sent to the malicious user's email address on the "@gmail.com" server. To determine the infected computer's IP address, the Trojan accesses the following service
Net-Worm.Win32.Kolab.hzo	Medium	This worm provides a malicious user with remote access to an infected machine. It is a Windows application (PE EXE file). It is 221 696 bytes in size. It is packed using an unknown packer. The unpacked file is approximately 112 KB in size. It is written in C++.	The name of the worm is different from "MsMxEng.exe", the following directories are created with hidden and system attributes in the root directory of the system drive
Trojan-Downloader.Win32.Agent.ehcj	Low	This worm provides a malicious user with remote access to an infected machine. It is a Windows application (PE EXE file). It is 221 696 bytes in size. It is packed using an unknown packer. The unpacked file is approximately 112 KB in size. It is written in C++.	If the name of the worm is different from "MsMxEng.exe", the following directories are created with hidden and system attributes in the root directory of the system drive

International Journal of Information and Communication Technology Research

©2012 ICT Journal. All rights reserved

http://www.esjournals.org

Ma Musa Usman Bala is a systems administrator at the Maths/Computer Science department, in Ibrahim Badamasi Babangida (IBB) University, Niger state, Nigeria. The department has two computer laboratories, 8 computer classrooms, and many lecturing podiums which are well equipped with workstations and projectors, Learning SMART Board. The department has an inventory of 78 laptops that are owns by Students and faculty members for their research and teaching needs. The department has Intranet, a secure Wireless LAN, and an open wireless internet access. Faculty members use their laptops to lecture and access student assignments, classroom information, offline books and research files that are stored in central server around the department's Network. Mr Ma Bala know that Research has also shown that these students direct their own learning, report a greater reliance on active learning strategies, readily engage in problem solving and critical thinking, and consistently show deeper and more flexible uses of technology than students without individual laptops. He allows Students to use their own laptops and laboratory desktop to access classroom notes and other offline materials located in the network places. Mr Ma Bala created a common password for faculty members to access several services, including sensitive information. Students also use their laptops to access their results using an unsecured wireless internet access. Some of the systems are infected due to students downloading harmful documents via the Internet. Several new programs on the faculty laptops and desktops need to be monitor and updated. Students use laptops and laboratory computers to download games and access social Web sites. As Mr M a Bala was inspecting the lab after lectures he noticed that most of the desktop were no shutdown, which some programmes are running, and these computer are still logged onto the network. Mr Ma bala rate possible Vulnerabilities Rating as suggested:

- **High Vulnerability:** One or more significant weaknesses have been identified that make the facility highly susceptible to a terrorist or hazard. This vulnerability is very attractive to the intruder and has high consequences if this vulnerability is exploited. Mr Ma Bala has rated password cracking, gaining access to remote connections, presence of viruses and torangers in this category.

- **Medium Vulnerability:** A weakness has been identified that makes the facility somewhat susceptible to a terrorist or hazard. This vulnerability is somewhat attractive to the intruder and consequences if this vulnerability is exploited are Medium Vulnerability. Mr Ma Bala has rated security policy violation in this category.

- **Low Vulnerability:** A minor weakness has been identified that slightly increases the susceptibility of the facility to a terrorist or hazard. This vulnerability is not very attractive to the intruder and has low consequences if this vulnerability is exploited. Mr Ma Bala has rated software specific and updates in this category.

How to reduce the likelihood of successful attacks

It is impossible to prevent all security incidents. When a security incident does happen, you will need to ensure that its impact is minimized. IT security organizations need to establish a security configuration baseline and a desired state that has a foundation on best practices. Furthermore, security configuration and administration policies must define the technical parameters that a targeted business implementation requires. Along these lines, an organization's effective vulnerability management program should include a formal definition of the desired state and a methodology to audit and evaluate the environment with respect to that desired state. Methodologies may differ in implementation steps from one enterprise to the other, yet the underlying principles of best practices should generally remain the same[11][12]

Even though network-wide patching and antivirus policies are enforced and stringently followed, an infection from some viruses and worms can be caused when users of micro-computers return them to the network. This is because these users may not have properly updated systems. If their systems become infected, they can infect others by simply connecting to the LAN. Likewise, desktop computers that have not been used for some time may lack proper patches and viral protection. Staff may bring systems from home, and contractors may also connect unmanaged, unprotected systems to the LAN. Your policies should take the following precautions to manage vulnerabilities:

General precautions

1. Be suspicious of email attachments from unknown sources.
2. Verify that attachments have been sent by the author of the email. Newer viruses can send email messages that appear to be from people you know.
3. Do not set your email program to "auto-run" attachments.
4. Obtain all Microsoft security updates.
5. Back up your data frequently. Keep the write-protected media in a safe place—preferably in a different location than your computer.

Monitoring and removing vulnerabilities with specific course of action

Using how to reduce the likelihood of successful attacks in the previous step, Mr Ma Bala generates a working

International Journal of Information and Communication Technology Research

©2012 ICT Journal. All rights reserved

http://www.esjournals.org

plan in managing vulnerabilities in the Department of Maths/Computer science. Specifically, Mr Ma Bala immediately he make a revolutionary changes and request password changes, enforce secure wired or wireless connection to sensitive data, update antivirus programs, scan, and clean the infected computers, send a memo and remind students and faculty of relevant security policies, and update and install new patches.

B. Managing Vulnerabilities: Present Threat

When threats are present, system administrators must take reactive approach. The damage computer vulnerabilities can inflict on your system depends on many things, including how sophisticated the vulnerability is. When the system is under attack, a quick evaluation of the threats and quick reaction to these threats is necessary. The reaction is immediate but still systematic, and the following steps must be followed:

1. Differentiate between viruses, worms, and Trojans with their Course of Actions
2. Identify what is not a virus, worms, and Trojans
3. Managing vulnerability-threat with specific course of action

1. Differences between viruses, worms, and Trojans with their Course of Actions

Computer virus

Computer virus is a small program written to alter the way a computer operates, without the permission or knowledge of the user. A virus must meet two criteria:

1. It must execute itself. It often places its own code in the path of execution of another program.
2. It must replicate itself. For example, it may replace other executable files with a copy of the virus infected file. Viruses can infect desktop computers and network servers alike.

Some viruses are programmed to damage the computer by damaging programs, deleting files, or reformatting the hard disk. Others are not designed to do any damage, but simply to replicate themselves and make their presence known by presenting text, video, and audio messages. Even these benign viruses can create problems for the computer user. They typically take up computer memory used by legitimate programs. As a result, they often cause erratic behaviour and can result in system crashes. In addition, many viruses are bug-ridden, and these bugs may lead to system crashes and data loss.

Worm

Worms are programs that replicate themselves from system to system without the use of a host file. This is in contrast to viruses, which requires the spreading of an infected host file. Though worms generally exist inside of other files, often Word or Excel documents, there is a difference between how worms and viruses use the host file. Usually the worm will release a document that already has the "worm" macro inside the document. The entire document will travel from computer to computer, so the entire document should be considered the worm W32.Mydoom.AX@mm is an example of a worm

Trojan horse

Trojan horses are impostors—files that claim to be something desirable but, in fact, are malicious. A very important distinction between Trojan horse programs and true viruses is that they do not replicate themselves. Trojan horses contain malicious code that when triggered cause loss, or even theft, of data. For a Trojan horse to spread, you must invite these programs onto your computers; for example, by opening an email attachment or downloading and running a file from the Internet. Trojan.Vundo is a Trojan horse.

Mr Ma Bala has solve several vulnerabilities but working to enforcing secure information system, performing the latest update to new programs, and full computer scanning. Mr Ma Bala discovers security threats. First, Viruses that spread by email, such as Sobig, and Netsky virus this can generate so much email traffic that servers slow down or crash. Or this may cause organization to the risk shutting down servers. Typically, email-aware viruses depend on the user clicking on an attached document. This runs a script that can forward infected documents to other people. The Netsky virus, for example, searches the computer for files that may contain email addresses (e.g. EML or HTML files), and then uses the email program on your computer to send itself to those addresses. Some viruses, like Sobig-F, don't even need to use your email browser; they include their own "SMTP engine" for sending mail. Second, some staff reporting that many computers in the lab beeps at startup with no screen display, they cannot open a particular document from other computer that is switch on. As the first step, Mr Ma Bala builds vulnerability -threat classification as shown in Table 2. Only the vulnerabilities that are not a virus, worms, and Trojans are listed in this table along with their typical course of actions.

International Journal of Information and Communication Technology Research

©2012 ICT Journal. All rights reserved

http://www.esjournals.org

2. Identify what are not a virus, worms, and Trojans

It is easy to blame any computer problem on a virus. The following are not likely to be caused by a virus or other malicious code; they are cause by hardware failure. Organizations that want to ensure their defenses are up-to-date and are tuned to respond to today's newest attacks and to the most pressing vulnerabilities; these can be managed when system administrator distinguishes from software attack:

TABLE II: what are not a virus, worms, and Trojans

Concept	Description
Hardware problems	No viruses can physically damage computer hardware, such as chips, boards, and monitors.
The computer beeps at startup with no screen display	This is usually caused by a hardware problem during the boot process.
The computer does not register 640 KB of conventional memory	This can be a sign of a virus, but it is not conclusive. Some hardware drivers such as those for the monitor or SCSI card can use some of this memory.
You have two antivirus programs installed and one of them reports a virus	This might be a virus, but it can also be caused by one antivirus program detect the other program's signatures in memory
Microsoft Word warns you that a document contains a macro	This does not mean that the macro is a virus.
You cannot open a particular document	This is not necessarily an indication of a virus. Try opening another document or a backup of the document in question. If other documents open correctly, the document may be damaged.
The label on a hard drive has changed	Every disk is allowed to have a label. You can assign a label to a disk by using the DOS Label command of from within Windows.

As shown in Table II, there are several vulnerabilities that are not cause by virus or trojan. Mr Ma bala need to differentiate what are vulnerabilities that are cause by virus and those cause by hard disk failure. However, Mr Ma Bala is happy to see that his last strategy on security policy, the importance of strong passwords, and his action to request password changes have transformed this potentially high risk threat-vulnerability combination into a Medium Vulnerability level. On the other hand, the spread of new viruses is causing significant damage to the system and other machines that are already infected or which do not have up-to-date antivirus protections.

3. Managing vulnerability-threat with specific course of action

Based on the findings from the previous step, system administrators need to identify the immediate course of action to address the most severe vulnerability-threat. Specifically, Mr Ma Bala take step called safe computing, which he divides in to General precautions when working with files and the Internet and Specific to Antivirus**:**

Take these precautions when working with files and the Internet:

- Before you load a file or install software onto your computer from a floppy disk or CD-ROM, use your antivirus program to scan the floppy or CD.
- If you receive an email attachment from an unfamiliar email address, or an attachment you were not expecting, either scan it or delete it (preferred).
- If you receive an email attachment from someone you know, and your antivirus program does not automatically scan incoming emails, save the attachment to your hard drive and scan it with the antivirus program. Your friend or colleague's computer may be infected with a virus.
- When you download software from the Internet, be sure to download it from the software company's site or a recognized download site or download the file to your hard drive and scan it using your antivirus program before you run or decompress it.
- If someone sends you a 'joke' file or electronic

©2012 ICT Journal. All rights reserved

greeting card that you must launch to view, be very wary.

- Don't use Outlook or Outlook Express as your email program. More viruses are spread from the security holes in Outlook than any other email program.

Specific to Antivirus

- Make sure that you have the most recent virus definitions. We recommend that you run Update at least once per week. Updates virus definitions in response to new virus threats.
- Make sure that you have set your Antivirus to scan floppy disks on access and at shutdown.
- Always keep your Antivirus Auto-Protect running. I strongly recommend that you have Antivirus set to scan all files, not just program files.
- Scan all new software before you install it. Because boot sector viruses spread by floppy disks and bootable CDs, every floppy disk and CD should be scanned for viruses. Shrink-wrapped software, demo disks from suppliers, and trial software are not exempt from this rule. Viruses have been found even on retail software.
- Scan all media that someone else has given you.
- Use caution when opening email attachments. Email attachments are a major source of virus infections. Microsoft Office attachments for Word, Excel, and Access can be infected by Macro viruses. Other attachments can contain file infector viruses. Antivirus Auto-Protect will scan these attachments for viruses as you open or detach them. We recommend that you enable email scanning, which will scan email attachments before the email message is sent to your email program.

IV. CONCLUDING REMARKS

Micro-computer have become the computers of the day for top officers like managers, directors who want to access their organizational documents while traveling or while working from home. With this popularity they also offer the greatest security challenges for system administrators. The paper discus these vulnerabilities and offers a framework for managing them. In general, there are two methods under which a system administrator can manage these vulnerabilities. The first method assumes no presence of threat and is designed to provide a systematic and proactive monitor course of action to continuously update security of Microcomputer and their use to access organizational internet.

The method suggests a course of action based on Identify and classifying present vulnerabilities in the IT security. The vulnerabilities are classified based on two factors: the degree of attractiveness to a potential intruder and the implication of the vulnerability for the organization. The second method assumes the presence of security threats. A frame work is designed to offer a reactive, a systematic monitoring and removing vulnerabilities with specific course of action. Differentiate between viruses, worms, and trojans with their course of actions. Again identifying different kinds of vulnerabilities and what are not virus, worms, and Trojans, followed by managing vulnerability-threat with specific course of action.

As vulnerabilities are discovered at an ever increasing rate and exploits are created with record speed, organizations must position themselves to react immediately and effectively to protect themselves. In order to effectively manage vulnerability response and remediation, it is important for security teams to establish their vulnerability, because there are many people who for a variety of reasons would wish to break into a computer system, it is necessary to build some sort of security into the network. This paper offers a framework for managing Microcomputer vulnerabilities base on system, and internet access. This framework assists organization to create effective and proactive monitor course of plans to deal with the vulnerabilities. When security threats are present, a Classification- based approach is suggested. The classification between vulnerabilities can help the system administrator identify the most severe attack combination and mitigate the risk of such threats. The Classification-based approach is a reactive approach but it is necessary to guide the system administrator when the networks or computers are under attack. A real case scenario from a university laboratory is used to illustrate the framework. The suggested framework is not limited to the use of microcomputers; it can be used by organizations to monitor vulnerabilities in other areas of organizational.

REFERENCES

[1] A.T. Williams, M. Nicolett (2005) “Improve IT Security with Vulnerability Management”.2005. Retrieved august 11 2011 from http://www.gartner.com/DisplayDocument?doc_cd=127481

[2] A. Asllani and A. Ali (2011)"Addressing Vulnerability of Mobile Computing: A Managerial

©2012 ICT Journal. All rights reserved

Perspective"2011 retrieved on September 1, 2011 from http://sites.google.com/site/ijcsis/ISSN 1947-5500

[3] C. Onwubiko and A. P. Lenaghan "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises" IEEE 2007 retrieved august 10 2011 from www.research-series.com/cyril/IEEE-ISI07.pdf

[4] CDW-G (White Paper), "Micro-computing security: protecting data on devices roaming on the perimeter," Retrieved August 10, 2011, from: http://www.edtechmag.com/higher/docs/2008/09/mini-computing-security.pdf.

[5] E. A. Kiountouzis; & S. A. Kokolakis (2011)"Information systems security: facing the information society of the 21st century" Chapman & Hall, Ltd ISBN 0-412-78120-4

[6] McAfee white paper "An Introduction to Computer Viruses (and Other Destructive Programs)" retrieve from www.mcafee.com

[7] N. A. Renfroe and J. L. Smith, (2010)"Threat/vulnerability assessments and risk analysis" November 2010, retrieved on February 7, 2011from http://www.wbdg.org/resources/riskanalysis.php

[8] NIST "Computer Security Division Annual Report"2010, retrieve October 18, 2011,from NIST "Computer Security Division Annual Report"2010, retrieve October 18, 2011,from http://csrc.nist.gov/publications/nistir/ir7751/nistir-7751_2010-csd-annual-report.pdf

[9] Sophos Plc. 'Viruses and spam what you need to know'2004 retrieved on August 10, 2011 from www.sophos.com

[10] Symantec Corporation" What is the difference between viruses, worms, and Trojans",2006 retrieved october,20 2011, from http://service1.symantec.com/SUPPORT/nav.nsf/pfdocs/1999041209131106?Open&docid=1999041209131106&nsf=nav.nsf&view=docid

[11] U.S Air force software protection "cyber security", retrieved October 20 2011, from http:/www.spi.dod.mil/tenets.htm

[12] Wright, Joe; Jim Harmening " Computer and Information Security Handbook Morgan Kaufmann" 2009 Publications Elsevier Inc. p.257 ISBN 978-0-12-374354-1