International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Network Security using NAC on Threats Plagiarism Sabotage Data breaches

Supriya Menon[1]& Spurthi.K[2]

[1]Associate professor Dept. OF CSE Medha Institute of Science & Technology for Women
Mail Id: - **supriyamenon05@gmail.com**
[2]Asst professor OF CSE Medha Institute of Science & Technology for Women
Mail Id: - kolluspoorthy03@gmail.com

Abstract—
The threats for information security are increasing at an alarming rate. This is mainly because of the availability of hacking tools on the Internet, USB devices, wireless connectivity, etc. This paper presents the brief understanding about risk management, network threats, firewalls, software licensing types and more special purpose secure networking devices. It suggests mitigation techniques in network security to meet the organization's standard. Our studies show that the proposed enhancements provide better data confidentiality with some degree of computing cost as the trade-off.
Keywords -Network Access Control (NAC); Information Security Strategy; Insider's Threats; Plagiarism; Sabotage; Data breaches

1. INTRODUCTION

Whenever new software is created, lots of hard work, money and time have to be put in by the company that develops it. So, as a rule, the company that developed it does not reveal the details of the source code to outsiders. Their business and profits depend on the secrecy of the source code. So they guard it very carefully and prevent others from sharing their profits by the easy method of copying!

Source Code:

Programmers write software programs using a programming language, e.g., C, C++ and Java. The programming language provides a series of instructions they can use to create the program they want. The instructions a programmer uses to build the program are known as source code. We can compare source code to the recipe or formula of drink like coke or Pepsi anywhere to the bottled drink easily but you do not get the secret recipe or formula that makes the drink anywhere just as easily! Source code is a very closely guarded secret.

Software License:

A software license (or software license in common wealth usage) is a legal instrument (usually by way of contract law) governing the usage or redistribution of software. All software is copyright protected, except material in the public domain.

Software licensing Types:

There are many different types of software, which can be a little confusing for the uninitiated. Following is a brief definition of each type, and the differences between them.

Shareware: This software is downloadable from the Internet. Licenses differ, but commonly the user is allowed to try the Social and Ethical Issues program for free, for a period stipulated in the license, usually thirty days. At the end of the trial period, the software must be purchased or uninstalled.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Crippleware: This software is similar to shareware except that key features will cease to work after the trial period has ended. For example, the "save" function, the print function, or some other vital feature necessary to use the program effectively may become unusable.

Demo software: Demo software is not intended to be a functioning program, though it may allow partial functioning. It is mainly designed to demonstrate what a purchased version is capable of doing, and often works more like an automated tutorial. If a person wants to use the program, they must buy a fully functioning version.

Adware: This is free software that is supported by advertisements built into the program itself. Some adware requires a live Internet feed and uses constant bandwidth to upload new advertisements. The user must view these ads in the interface of the program. Disabling the ads is against the license agreement. Adware is not particularly popular.

Spyware: Spyware software is normally free, but can be shareware. It clandestinely "phones home" and sends data back to the creator of the spyware, most often without the user's knowledge.

Freeware: Freeware is also downloadable off the Internet and free of charge. Often freeware is only free for personal use, while commercial use requires a paid license. Public domain software: This is free software, but unlike freeware, public domain software does not have a specific copyright owner or license restrictions. It is the only software that can be legally modified by the user for his or her own purposes.

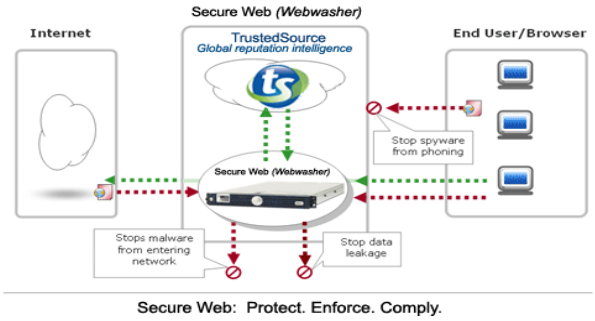

Fig. 1. Secure computing

Ethical and Legal Use of Software:

Software enables us to accomplish many different tasks with computers. Unfortunately, in order to get their work done quickly and conveniently, some people justify making and using unauthorized copies of software. They may not understand the implications of their actions or the restrictions of the U.S. copyright law. Here are some relevant facts:

- UNAUTHORIZED copying of software is illegal. Copyright law protects software. Authors and Publishers, just as patent law protects Inventors.
- UNAUTHORIZED copying of software by individuals can harm the entire academic community. If unauthorized copying proliferates on a campus, the institution may incur a legal liability. Also, the institution may find it more difficult to negotiate agreements that would make software more widely and less expensively available to members of the academic community.
- UNAUTHORIZED copying of software can deprive developers on a fair return for their work, increase prices, reduce the level of future support and enhancement, and inhibit the development of new software products.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

2. Software And Intellectual Rights

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgement and the right to control over the form, manner, terms of publication and distribution

Closed source software (i.e. Microsoft Windows and Office):

It is developed by a single person or company. Only the final product that is run on your computer is made available, while the all important source code or recipe for making the software is kept a secret. This software is normally copyright or patented and is legally protected as intellectual property. The owner of the software distributes the software directly or via vendors to you the end user. You cannot legally give it away, copy it or modify it in any way unless you have a special license or permission to do so.

Open Source Software:

In general, open source refers to any program whose source code is made available for use or modification as users or other developers see fit. Open source software is usually developed as a public collaboration and made freely available. Open Source is a certification mark owned by the Open Source Initiative (OSI)[5]. Developers of software that is intended to be freely shared and possibly improved and redistributed by others can use the Open Source trademark if their distribution terms conform to the OSI's Open Source Definition.

To summarize, the Definition model of distribution terms require that:

• The software being distributed must be redistributed to anyone else without any restriction.
• The source code must be made available (so that the receiving party will be able to improve or modify it).
• The license can require improved versions of the software to carry a different name or version from the original software.

Let us see the most popular open source software available in market that anyone can freely download and use, or even modify, without restriction:

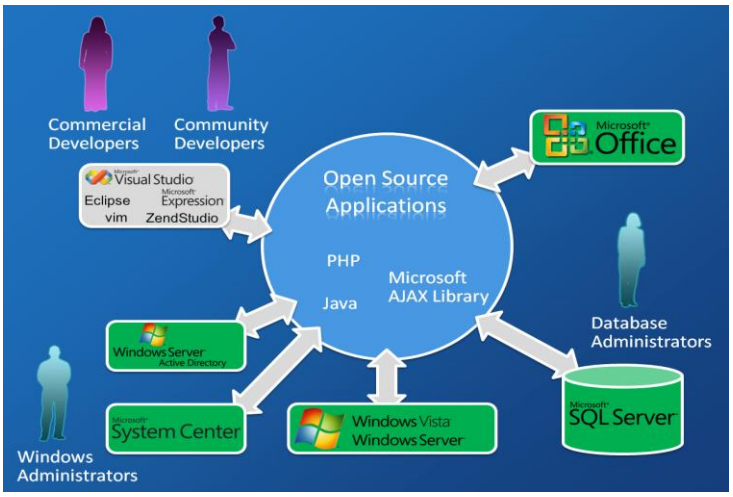

Fig. 2. Open Source Strategy

Linux:

A computer operating system and kernel originating as a UNIX system. It exists in many versions.

Apache:

A web server program (for supplying pages in response to requests) used in most web server computers and available for Windows as well as Linux and other UNIX systems.

OpenOffice:

An office application set (for word processing, spreadsheet manipulation, picture drawing and data

base access) compatible with all other major office application sets such as Office and available for Windows and Mac as well as Linux and other UNIX systems.

GNOME:
A desktop development environment providing tools for developing desktop applications (as well as its own basic desktop applications) and available for Linux and other UNIX systems.
Operating systems and Desktop environments
Examples:
Linux: Operating system kernel
Ubuntu: Linux distribution with full compliment of software for everyday use.Ubuntu is an easy to use operating system based on and made possible by the Debian project. Google Chrome OSLightweight operating system based around the web browser Android smart-phone operating system. By Google / Open Handset Alliance.
Graphics and Multimedia Examples:
GIMP: Bitmap graphics editor, similar to Adobe Photoshop
Inkscape: Vector graphics editor
Blender: Advanced 3D modelling and rendering application;

Office software Examples:
OpenOffice.org:

- Office productivity software.
- Comparable to Microsoft Office.
- As well as having using an open file format it can read and write Microsoft Office files.

PDFCreator:

- ✓ Creates PDFs from any Windows program.
- ✓ Use it like a printer (Windows only).

Koffice: Office suite for KDE desktop (Unix / Linux).

Programming Related Examples:
Eclipse: Software framework and Java IDE.
Kdevelop: Programming IDE for Linux / Unix.
Java: Programming language.

Advantages of Open source Software:
There are a number of advantages that open source code offers over closed source. Some of the most important advantages area as follows:
Bug-fixing:
All software releases contain bugs. Hopefully, the people developing the software will have spotted and dealt with anything obvious, but any development team has only so much time in which to test a piece of software before it is released. When a bug is spotted in proprietary software, the only people who can fix it are the original developers, as only they have access to the source code. Open source software is different. As a large number of users can access and change the code, bugs tend to be more visible and more rapidly corrected.

Security:
Having access to the source code allows the user of that software to choose the approach to security that they want. In other words, it allows you to take ownership of your own security. It also enables certain approaches that are not available with closed source and it is possible to decide on your own security priorities and to allocate resources accordingly.

Customization:
Closed source applications can only be customized or adapted within the scope provided by the original vendor but never outside its boundaries. Open source applications may be customized by anyone with the requisite skill. Thus, open source software can be readily adapted to meet specific user needs. Even if you cannot program yourself, if you would like something added or customized

you can generally pay an appropriately skilled software developer to do it for you.

Translation:
With access to the source code it is easy to translate the language of the software interface. Large closed source commercial software vendors are usually unwilling to translate their products into less widely spoken languages, as the market for them would be too small to guarantee profit.

Learning from examples:
If you are interested in programming, open source code provides an excellent resource from which to learn, and open source projects provide a practical environment in which to test your skills. Just watching the development process can provide an education in itself. If you choose to submit code to an open source project, it will generally be checked and commented on by experienced programmers. Once you have convinced the project community that your code is of appropriate quality, you may be granted full committee rights yourself.

Being part of a community:
By adopting open source software you become part of a community of users and developers who have an interest in working together to support each other and improve the software. The extent to which you engage with this community is up to you, but you may obtain the intangible benefits of goodwill if you do. Programmers, in particular, can benefit from belonging to an open source community. It can help them to establish reputation and respect, and gain valuable experience.

Cost:
Many open source programs can be obtained at no cost or at a very low cost. This is often an important issue for individuals and in many cases this has been the main reason for an individual adopting a particular open source solution over a closed source alternative. However, other costs may arise: training, consulting, maintenance, etc. As a result, the total cost of ownership may not differ greatly between a closed source solution and an open source alternative for institutions. However, in some markets the difference in price between a closed source solution and an open source solution can be significant

Disadvantages of open source software:
• Since nobody in particular is responsible for the codes, there is no exact knowledge and assurance on when the codes are going to be fixed if there a bugs in it. Thus, users will have to use the problematic software until someone rectifies the problem.
• The codes are too complicated for novice users to understand.
• There is no particular official monitoring the works of a programmer improving the codes. This is because anyone is free to use, modify or even distribute the codes. Open source usually comes without warranty and after sales support should the software fail or malfunction. This is because the software usually distributed free of charge or sold for very minimal fees.

Netiquette:
Netiquette is etiquette for the Internet. Conduct while online that is appropriate and courteous to other Internet users. It is all the more important on the net because there are no facial clues or body-language to help us understand another person, as there is in face to face meetings. Quite simply, "netiquette" is Internet etiquette - the informal rules of behavior to be followed when using the Internet. These Internet customs have evolved over time, and help make the Internet a pleasant place.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Netiquette: Rules of Behavior on the Internet

1. Imagine your message on a billboard. Anything you send can be forwarded, saved and printed by people it was never intended for. Never send anything that will reflect badly on you or anyone else.
2. Remember that company emails are company property. Emails sent from your workplace can be monitored by people besides the sender and reader, and are technically company property.
3. Avoid offensive comments. Anything obscene, libelous, offensive or racist does not belong in a company email, even as a joke.
4. Keep your message Cool. Email messages can easily be misinterpreted because we don't have the tone of voice or body language to gives us further cues. Using multiple explanation points, emoticons, and words in all capital letters can be interpreted as emotional language.
5. Be careful about forwarding messages. If you aren't sure if the original sender would want to forward the message, don't do it.
6. Don't expect an answer right away. Email messages may be delivered quickly, but your recipient may not read it right away.
7. Don't sacrifice accuracy for efficiency. Don't send sloppy, unedited email.
8. Include the message thread. Keep the original message for a record of your conversation. However, when sending a new message to the same person, start a new thread with a new subject line.
9. Don't type in all CAPS. It's perceived as YELLING. However, don't write with only small letters, as this is perceived as your being lazy, because it makes it more difficult for people to read.
10. Write clear, organized messages, with a subject line that gives enough information for the reader to file it and find it later.

Plagiarism:

The word plagiarism comes from a Latin word for kidnapping. You know that kidnapping is stealing a person. Well, plagiarism taking someone's words or ideas as if they were your own. Plagiarism is a piece of writing that has been copied from someone else and is presented as being your own work. Plagiarism is when you use someone else's words or ideas and pass them off as your own. It's not allowed in school, college, or beyond, so it's a good idea to learn the proper way to use resources, such as websites, books, and magazines. Plagiarism is a form of cheating, but it's a little complicated so a kid might do it without understanding that it's wrong.

Avoiding Plagiarism:

• To be on the safe side, always make it clear where the information comes from.

• Sometimes, teachers ask kids to write a bibliography that’s a list of the sources you used for a project or report.

To do that, you'll need to know the author, the title, and the date it was published. For instance, if you did a report on giraffes, you could give credit to an author this way: Smith, Hazel B. "All about Giraffes." 2005.

Downloading a file:

When you download a file, you transfer it from the Internet to your computer. The most commonly downloaded files are programs, updates, or other kinds of files such as game demos, music and video files, or documents. Downloading can also mean copying information from any source to a computer or other device, such as copying your favorite songs to a portable music player.

Risks involved while downloading files:

Whenever you download a file, there is always a small risk that the file will contain a virus or a

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

program that can damage your computer or your information.

3. PRECAUTIONS TO BE TAKEN WHILE DOWNLOADING FILES:

Here are some precautions you can take to help protect your computer when you download files are as follows:

Install and use an Anti virus program. Anti virus programs scan files before opening them and notify you if a file is potentially unsafe. Be sure to keep your Anti virus program up to date.

Download the files from websites that you trust.

Be cautious of certain file types. Some file types are less safe because they can carry viruses. The main file types to avoid are program files with extensions such as .exe, .scr, .bat, .com, or .pif. Often, a potentially dangerous file is disguised as a less risky file type, because it has two file name extensions, such as filename.txt.exe. This example might look like a text file, but it's actually an executable file.

Free and open source software [FOSS].

It is software that is both free and open source. It is liberally licensed to grant users the right to use, copy, study, change, and improve its design through the availability of its source code.

In the context of free and open-source software, free refers to the freedom to copy and re-use the software, rather than to the price of the software.

Understands the difference between Closed Source software and Open Source software.

Lists the different open source software available.

Know the advantages and disadvantages of Open Source Software.

Know the Risk involved in the downloading from Internet.

Understand about Plagiarism.

4. THREATS TO NETWORK SECURITY

Bad practices when configuring the following aspects of a network can INCREASE the risk of attack.

- **Insecure Architectures:** A misconfigured network is a primary entry point for unauthorized users. Leaving a trust-based, open local network vulnerable to the highly-insecure

- **Broadcast Networks:** System administrators often fail to realize the importance of networking hardware in their security schemes. Simple hardware such as hubs and routers rely on the broadcast or non-switched principle; that is, whenever a node transmits data across the network to a recipient node, the hub or router sends a broadcast of the data packets until the recipient node receives and processes the data. This method is the most vulnerable to address resolution protocol (*ARP*) or media access control (*MAC*) address spoofing by both outside intruders and unauthorized users on local hosts.

- **Centralized Servers:** Another potential networking pitfall is the use of centralized computing. A common cost-cutting measure for many businesses is to consolidate all services to a single powerful machine. This can be convenient as it is easier to manage and costs considerably less than multiple-server configurations. However, a centralized server introduces a single point of failure on the network. If the central server is compromised, it may render the network completely useless or worse, prone to data manipulation or theft. In these situations, a central server becomes an open door which allows access to the entire network.

Ways that insiders can attack

An insider threat is defined by the Computer Emergency Response Team at Carnegie-Mellon

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

University (CERT) [1], as "a malicious insider who is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system or data, and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information system". Insider Threat is about breaching [2] the confidentiality, integrity and availability of organizational information system by using authorized or unauthorized access.

- IT Sabotage
- Data breaches
- Fraud
- Theft of Intellectual Property
- National Security Espionage
- The Unintentional

5. PREVENTATIVE CONTROLS

- ✓ Know your assets and know what needs to be protected.
- ✓ Clearly document and enforce policies and controls. Train employees to raise awareness of such policies and controls.
- ✓ Organizations should monitor and respond to suspicious behavior, which starts with the hiring process
- ✓ Implement proper access control and account management.
- ✓ Enforce proper segregation of duties.
- ✓ Be extra cautious with system administrators and technical users with privileged access.

6. MITIGATION TECHNIQUES

To ensure organizations pay necessary attention to the information security, various legal compliances are required to be met – for e.g. SOX, HIPAA, PCI, ISO27000, etc. These are various compliance standards required to be met: Surbanes-Oxley (SOX) is for business compliance, HIPAA is for medical records and information, PCI is for credit card and related transactions/sales (used in retail chains, etc.), ISO27000 is a corporate security requirement standard.

To check and enforce the security policies, a concept termed as Network Access Control (NAC) is becoming essential. The job of checking end point security posture, integrating with authentication, patch and anti virus management is done by NAC. Users are allowed access to network resources only if the desired security policies have been adhered to. NAC works at the network layer and continuously checks the security posture.

To ensure that data is not leaked out from the endpoints, most end point security solutions provide integrated feature list that includes Anti-Virus, Anti-Spyware, Host based Intrusion Prevention Systems (HIPS), Data Leakage Prevention (DLP) software and personal firewall. Data leakage prevention provides control on removable USB drives as per policy as well as measures to prevent theft sensitive data on laptops, etc.

A number of coordinated and infected PCs can launch DoS (Denial of Service attacks) or DDoS (Distributed Denial of Service attacks) attacks.

Proactive measures are applied before an endpoint or user is granted access to the network, after an appropriate authentication and after its security posture checks are carried out. These checks ensure that the user system is a corporate resource and it is not trying to connect its personal system to the corporate network. To overcome the problem of passwords, techniques like dual factor authentication are used. Dual factor authentication use dynamic passwords, which keep changing with time.

Mitigation in rate limiting:

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

Unlike Access Control Lists, rate limiting techniques does not separate the attacking network completely off the victim. Instead it places a cap or sets up a threshold limit of traffic that the server would be able to withstand. This method is adopted by most of the data providers as it proves to be extremely effective and saves the network components from permanent denial
of service. However this cannot be an ideal solution as it still permits controlled traffic from attacking system as well. The following commands limit the traffic from the attacking network 192.168.2.0 to certain level. The best feature of this technique is that the network administrator is capable of deciding how much traffic to be let inside the network. This traffic rate depends on the size of the company, the traffic it can withstand and the server's processing capacity.

Cisco applies rate limiting to the traffic in the name of Committed Access Rate (CAR) and Distributed Committed Access rate(DCAR). The rate limiting rules could be applied to incoming or even on the outgoing traffic in a particular interface. When an IP packet conforms or exceeds a specific rule, various decisions could be made on it. Every access list created in the Cisco router could be given a number for identification and the same can be used here in rate limiting using the Command "ACL index". The rate of traffic could be determined by the network administrator and could be specified along with this command in bits per second. Burst normal and the Burst maximum are the compulsory keywords specified to handle the traffic fluctuations and maintain steady flow of packets respectively.

Network Security Common Mitigating Threats:

Improper and incomplete network device installation is an often-overlooked security threat that, if left unaddressed, can have terrible results. Software-based security measures alone cannot prevent intended or even accidental network damage caused by poor installation. Now we will describe how to mitigate common security threats to Server Routers and Switches.

Physical Installations:

Physical installations involve four types of threats: **Hardware, Electrical, Environmental and Maintenance.**

Hardware threats

Hardware threats involve threats of physical damage to the router or switch hardware. Mission-critical Cisco network equipment should be located in wiring closets or in computer or telecommunications rooms that meet these minimum requirements:

- The room must be locked with only authorized personnel allowed access.
- The room should not be accessible via a dropped ceiling, raised floor, window, ductwork, or point of entry other than the secured access point.
- If possible, use electronic access control with all entry attempts logged by security systems and monitored by security personnel.
- If possible, security personnel should monitor activity via security cameras with automatic recording. Hardware threats involve physical damage to network components, such as servers, routers, and switches.

Electrical threats

Electrical threats include irregular fluctuations in voltage, such as brownouts and voltage spikes, Electrical threats, such as voltage spikes, insufficient supply voltage (brownouts), unconditioned power (noise), and total power loss, can be limited by adhering to these guidelines:

- Install uninterruptible power supply (UPS) systems for mission-critical Cisco network devices.
- Install backup generator systems for mission-critical supplies.
- Plan for and initiate regular UPS or generator testing and maintenance procedures based on the manufacturer-suggested preventative maintenance schedule.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 3, Issue 01, January 2016
Available at http://internationaljournalofresearch.org

- Install redundant power supplies on critical devices.
- Monitor and alarm power-related parameters at the power supply and device levels.

Environmental threats

Environmental threats include very low or high temperatures, moisture, electrostatic, and magnetic Interference Environmental threats, such as temperature extremes (too hot or too cold) or humidity extremes (too wet or too dry), also require mitigation. Take these actions to limit environmental damage to Cisco network devices:

- Supply the room with dependable temperature and humidity control systems. Always verify the recommended environmental parameters of the Cisco network equipment with the supplied product documentation.
- Remove any sources of electrostatic and magnetic interference in the room.
- If possible, remotely monitor and alarm the environmental parameters of the room.

Maintenance threats

Maintenance threats include not having backup parts or components for critical network components; not labeling components and their cabling correctly Maintenance threats include poor handling of key electronic components, electrostatic discharge (ESD), lack of critical spares, poor cabling, poor labeling, and so on. Maintenance-related threats are a broad category that includes many items. Follow the general rules listed here to prevent maintenance-related threats:

- Clearly label all equipment cabling and secure the cabling to equipment racks to prevent accidental damage, disconnection, or incorrect termination.
- Use cable runs, raceways, or both to traverse rack-to-ceiling or rack-to-rack connections.
- Always follow ESD procedures when replacing or working with internal router and switch device components.
- Maintain a stock of critical spares for emergency use.
- Do not leave a console connected to and logged into any console port. Always log off administrative interfaces when leaving a station.
- Do not rely upon a locked room as the only necessary protection for a device. Always remember that no room is ever totally secure. After intruders are inside a secure room, nothing is left to stop them from connecting a terminal to the console port of a Cisco router or switch.

CONCLUSION

Network security teams need to contend with threats from increasingly sophisticated and well-funded cybercriminals, while the very infrastructure they are chartered with protecting goes through fundamental paradigm shifts. In this paper, we define major discrepancies and vulnerabilities in an ISP network. Our goal is to provide appropriate solutions and suggest a best-practice approach to protect digital assets. As illustrated in a number of examples, the framework may promote improved efficiency and coordination of security services across communication layers. To address these challenges and secure "the new network," organizations need capabilities that ensure persistent security, while enabling continued evolution in IT.

REFERENCES:

[1] "2010 Cyber Security Watch Survey – Survey Results" Conducted by *CSO* magazine in cooperation with the U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte.

[2] "2010 Data Breach Investigations Report by Verizon Business" Authors Wade Baker, Mark Goudie, Alexander Hutton, C. David Hylender, Jelle Niemantsverdriet, Christopher Novak, David Ostertag, Christopher Porter, Mike Rosen, Bryan Sartin, Peter Tippett, M.D., PhD, Men and women of the United States Secret Service.

[3] IDC Worldwide Quarterly PC tracker Sep 2009 Report

[4] Cisco Visual Networking Index report June 2, 2010 titled "Hyper connectivity and the Approaching Zettabyte Era"

[5] ISO, "Information Processing Systems-OS1 Reference Model,- is0 Pub. No. 7498, Oct. 1984.

[6] T. DeMarco, Structured Analysis and System Specification, New York, NY: Yourdon Press, 1978.

[7] D. K. Branstad, "Considerations for Security in the OS1 Architecture," IEEE Network Mag., pp. 34-39, Apr. 1987.

[8] M. D. Abrams and A. B. Jeng, "Network Security: Protocol ReferenceModel and the Trusted Computer System Evaluation Criteria," IEEE NetworkMag.. pp. 24-33, Apr. 1987.

[9] V. L. Voydock and ***S.*** T. Kent, 'Security Mechanisms in High-Level NetworkProtocols," Comp. Surveys, pp. 135-1 7 1, June 1983.

[10] L. K. Barker and L. D. Nelson, "Security Standards-Government and Commercial," AT&T Tech. J., pp. 9-18, May/June 1988.

Authors Profile

Author 1

SUPRIYA MENON
Associate professor OF CSE
Mail Id: - supriyamenon05@gmail.com
MEDHA Institute of Science & Technology for Women

Author 2

SPURTHI.K
Asst.Prof, Dept of CSE
Mail Id:- kolluspoorthy03@gmail.com
MEDHA Institute of Science & Technology for Women