KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES

Network Intrusion Detection and Prevention Systems in Educational Systems

A case of Yaba College of Technology

Nwogu Emeka Joshua

Bachelor Thesis of the Degree Programme in Business Information Technology
Bachelor of Business Administration (BBA)

TORNIO 2012

ABSTRACT

Nwogu, Emeka Joshua. 2012. Network Intrusion Detection and Prevention Systems in Educational Systems - A case of Yaba College of Technology. Bachelor's Thesis. Kemi-Tornio University of Applied Sciences. Business and Culture. Pages 66. Appendix 1.

The objective of this thesis work is to put forward a solution for improving the security network of Yaba College of Technology (YCT). This work focuses on implementation of a network intrusion detection and prevention system (IDPS), due to constant intrusions on the YCT's network. Various networks attacks and their mitigation techniques are also discussed, to give a clear picture of intrusions. The work will help the College's administrators to become increasingly cautions of attacks and perform regular risk analyses.

The research methodologies used in this work are descriptive and exploratory research. In addition, a questionnaire survey and interviews were used to collect data necessary for in-depth knowledge of the intrusions in the College. The choice of the research methods was found relevant for the current work. Furthermore, the researcher intended to gain an increased understanding of and provide a detailed picture of IDPS and the issues to consider when implementing the system.

Network intrusion has been a security issue since the inception of the computer systems and the Internet. When breaking into a computer or network system, confidentiality, integrity and availability (CIA) are the three most aspect of security that are targets for intruders. The CIA, important aspects of security, and other network resources, need to be well protected using robust security devices.

Based on the research tests and results, this thesis proposes implementation of IDPS on the College's network, which is an essential aspect of securing information and network resources.

Keywords: Information Security, IDPS, Network Intrusion, YCT, Network Attackers, Software Application, Network intruders

CONTENTS

ABSTRACT

FIGURES

TABLES

ABBREVATIONS

1 INTRODUCTION 9

1.1 Background 9

1.2 Motivation 11

1.3 Objectives 12

1.4 Structure of the Thesis 12

2 RESEARCH TOPIC, QUESTIONS AND METHODOLOGY 14

2.1 Research Topic and Question 14

2.2 Research Methodology 15

2.3 Expected Research Results 16

3 INFORMATION ON YABA COLLEGE OF TECHNOLOGY 17

3.1 History and objective 17

3.2 Centre for Information Technology and Management 17

3.3 YCT Network Structure 20

4 NETWORK ATTACKS AND MITIGATION TECHNIGUES 22

4.1 Reconnaissance Attacks 22

4.1.1 Packet Sniffer Attack 22

4.1.2 Port Scan and Ping Sweep Attack 24

4.1.3 Internet Information Queries Attack 24

4.2 Access Attack 25

4.2.1 Password Attack 25

4.2.2 Trust Exploitation Attack 26

4.2.3 Port Redirection Attack 26

4.2.4 Man-in-the-middle Attack 27
4.2.5 Buffer overflow 27
4.3 Denial of Service Attack 28
4.4 Malicious codes Attack 29
4.5 Application Layer Attacks 30

5 INTRUSION DETECTION AND PREVENTION SYSTEM 32
5.1 IDPS Detection Methodologies 32
5.2 Functions of IDPS 35
5.3 Types of IDPS Technologies 35
5.4 Comparison of IDPS Technologies 37
5.5 IDPS add-ons 39
5.6 Challenges and Limitations of IDPS 41
5.7 IDPS Components 42
5.8 Network Architectures and IDPS Sensor Location 43

6 DEPLOYMENT AND TESTING OF IDPS 50

7 DISCUSSIONS AND CONCLUSION 56
7.1 Introduction 56
7.2 Avenue for Further Research 57
7.3 Concluding Note 57

REFERENCES 59

APPENDIX 63

FIGURES

Figure 1. The main security targets in a network …….. 11
Figure 2. Centers for Information Technology and Management Chart …… 19
Figure 3. TCP/IP model layers ……... 21
Figure 4. Inline Network-Based IDPS Sensor Deployment Architecture ……...44
Figure 5. Passive Network-Based IDPS Sensor Architecture …… 45
Figure 6. Host-Based IDPS Agent Deployment Architecture ……..…46
Figure 7. Wireless IDPS Sensor Deployment Architecture ……48
Figure 8. NBA IDPS Sensor Deployment Architecture ……..49

TABLES

Table 1. Comparison of IDPS Technologies ……..……39
Table 2. Fuzzy techniques test result ……..... 52
Table 3. Artificial neural network techniques result …….**.....** 53

ABBREVATIONS

ANN Artificial Neural Network
APs Access Points
CIA Confidentiality, Integrity and Availability
CTIM Centre for Information Technology and Management
DAD Distortion, Alteration and Denial
DNS Domain Name System
DOS Denial of Service
DDoS Distributed Denial of Service
DHCP Dynamic Host Configuration Protocol
FCM Fuzzy C-means
FTP File Transfer Protocol
HOD Head of Department
HTTP Hypertext Transport Protocol
ICT Information Communication and Technologies
IDPS Intrusion Detection and Prevention System
IDS Intrusion Detection System
IEEE Institute of Electrical and Electronics Engineers
IT Information Technology
IS Information Security
ISP Internet Service Provider
IP Internet Protocol
IPS Intrusion Prevention System
KDD Knowledge Discovery in Databases
LAN Local Area Network
MitM Man-in-the-Middle
MLP Multilayer Perceptron
NAC Network Adapter Card
NBA Network behavior analysis
NFAT Network Forensic Analysis Tool
OS Operating System
PDA Personal Digital Assistants
SMBS School of Management and Business Studies
SMPT Simple Mail Transfer protocol

STAs Stations

STE School of Technical Education

SSH Secure Shell

SSL Secure Sockets Layer

SIV System Integrity Verifier

TCP Transmission Control Protocol

UDP User Datagram Protocol

VPN Virtual Private Network

VLAN Virtual Local Area Network

WAN Wide Area Networks

WLAN Wireless Local Area Network

YCT Yaba College of Technology

1 INTRODUCTION

1.1 Background

The title of this work is Network Intrusion Detection and Prevention Systems in Educational Systems. Intrusion is a major threat to security in computer and network systems, and has been an area of interest for software developers, inventing or coming up with methods or applications to combat the dreaded element in the world of computer security. An intrusion is a purposefully illicit endeavor to access information, manipulate information or render a system untrustworthy or inoperative. (Tech-FAQ 2010.) According to Kizza (2005, 14), intrusion is an intentional effort, successful or not, to access or misuse sensitive data in a controlled computer system or network.

For any organization, having a secure network is the primary aim to reach their business goal. A network is said to be reliable when it can withstand attacks, which may damage part or a whole system. An ideal secure network should resist intrusion to the barest minimum. However, in practice, no network is hundred percent secure from intrusion attempts by intruders, either internally or externally. Intrusion attempt can still succeed, in spite of security measures in place. It is therefore imperative to detect intrusion and limit its effects on networks, as much as possible. (Grand 2012.)

There are various forms intruders carry out attacks on a network, either for selfish gain or deliberate attempt to compromise sensitive data. No matter what form attacks are carried out, complex or trivial, these attacks poses a threat to a network. Various forms of threats to network security include eavesdropping of packets over a network, injection of malicious codes into computer system, unauthorized use of network resources, stealing software or hardware components, installing back doors programs into user's computer system to enable illicit remote access, performing denial of service attack. (Tech-FAQ 2010.)

As Information Technology expects are developing enhance ways to tackle intrusion on network and computer systems, intruders are devising and inventing new techniques to perpetuate malicious acts. As a result, applications of firewall, filtering of routers, regular update of anti-malware programs and other defense mechanisms deployed in a network are not enough to prevent the highly sophisticated attacks from intruders.

Therefore, there is need for deployment of Intrusion Detection and Prevention System (hereinafter IDPS) to combat network intrusion. (Grand 2012.)

Network attacks come in various forms as mentioned above. However, these attacks are classified into two major categories, internal and external attacks. Internal attacks are attacks on a network perpetrated by unhappy or greedy authorized users, i.e. insiders within an organization. Authorized users can use their legitimate rights to perform illicit activities in a network, due to the possession of some form of access rights. Most times, insiders conceal their attack and make it look as a normal process, to avoid suspicion. For instance, insiders might have some administrative rights over some data, which gives them the right to add, delete or modify. With such privileges, greedy users might alter data for personal gains, and not considering organization's interest. (Tech-FAQ 2010.)

External attacks are carried out by individuals or entities outside an organization, i.e. outsiders. It is mostly performed by malicious experience crackers, an experienced malicious entities, or script kiddies. External attacks are usually perpetrated by using a predefined plan and sophisticated technologies. These attacks usually involve scanning of network with software application to check for loop holes, vulnerable host and gathering of information, before launching attack. (Tech-FAQ 2010.)

An intrusion in a network usually tries to compromise one or all of the three main aspects of security. The three aspect of security are Confidentiality, Integrity and Availability (hereinafter CIA), which is popularly known as CIA Model or Triad. (Whitman 2004.)

Confidentiality as a key aspect of information security, limits information access and disclosure to authorized users. It is the duty of network administrators to prevent and ensure that unauthorized users do not gain access to confidential information in a network. (Whitman & Mattord 2005.)

Data integrity ensures that information or resources in a network are not modified or altered by unauthorized users. When data is modified or altered, it loses its trustworthiness. (Whitman & Mattord 2005.)

Availability as a concept ensures that information in a network is accessible and used by authorized users. Intruders can block or make information unavailable, so that it would not be used by authorized persons. (Whitman & Mattord 2005.)

Figure 1 depicts the three most targeted security facets in a network (SANS Institute 2012). It literally means the security and validity of assets or data in a network, relies strongly on security of the CIA model. If the CIA model of any network is compromised, it will result to Distortion Alteration and Denial (hereinafter DAD) of resources. Therefore, data becomes invalid or unreliable. (WiseGEEK 2012.)

Figure 1. The main security targets in a network (SANS Institute 2012)

1.2 Motivation

The choice of this topic is informed by the researcher's interest in information security (hereinafter IS), which embodies network security. The research work is aimed at examining known and unknown security threats on Yaba College of Technology's (hereinafter YCT) network.

YCT, which is the foremost institution in Nigeria, still faces intrusions on its network. The researcher's aim is to put forward a system that would help protect the College's network, devoid of easy intrusion from inside and outside attacks. This is carried out by underscoring the need to deploy and implement IDPS, which will detect and prevent internal and external threats. Intrusions on the College's network have a negative effect on the smooth running of academic activities, and also slow down study duration of students. The research work will be essential to ensuring information security such as data confidentiality, data integrity, and data availability in the College's network.

1.3 Objectives

One of the objectives of this thesis is to assess various network attacks peculiar to YCT, and mitigation techniques to withstand attacks. Another objective is to emphasis the importance of security policies and how policies are designed based upon security services and security mechanisms.

Furthermore, this research work presents a solution, IDPS, to improving the College's network security. It also intends to promote further research and development in the field of IDPS and its application on networks. In this research, investigations were carried out on the hardware and infrastructural requirement needed for deployment of IDPS and maximize its benefits. This also includes the technical requirement to implementing IDPS and other add-on technologies needed to supplement it.

This work is not suggesting for the replacement of other security mechanisms with IDPS. Rather, it proposes deployment of IDPS to supplement the existing security models and structure in the College's network, for effective and efficient work result.

1.4 Structure of the Thesis

This research work is divided into seven chapters. Chapter 2 briefly explains the research topic, research questions, research methodology and research output. Chapter 3 gives a brief history of the College, Centre for Information Technology and

Management, which handles all Information communication and technologies (ICT) issues, and network structure of the College. Chapter 4 briefly explains network attacks and mitigation techniques. The attacks explained are reconnaissance attacks, access attacks, denial of service and distributed attacks, malicious code attacks i.e. virus, worm and Trojan horse and application layer attacks. Chapter 5 explains important information on IDPS: common detection methodologies, functions, types, comparison of systems, add-on technologies, challenges and limitations, components, architectural framework and sensor locations. Chapter 6 explains deployment process of IDPS and analysis of test results. Chapter 7 presents a summary of the whole research work and directions for further research.

2 RESEARCH TOPIC, QUESTIONS AND METHODOLOGY

2.1 Research Topic and Question

Research is a methodical procedure of gathering and examining data to increase knowledge of the subject area under study (Matos 2012). The topic of this research focuses on the implementation of IDPS on YCT's network.

As discussed by Matos (2012), research question is a formal statement of the goal of study. The research question states clearly what the study will investigate or attempt to prove. Furthermore, research question is a logical statement that progresses from what is known or believed to be true, to that is unknown and requires validation.

The title of this thesis work is "Network Intrusion Detection and Prevention Systems in Educational Systems - A Case Study of Yaba College of Technology". This research will look at different forms of network attacks and their mitigation techniques, applicable security policies and advantage of having IDPS deployed on YCT's network.

The outcome of this research work will determine the benefits derivable by YCT, if they eventually adopt the system. In determining these derivable benefits, the researcher addresses three different questions in order to fulfill the objective of this work, viz:

RQ 1. In what ways would IDPS improve security on the College's network?

This question indentifies the threats and attacks on the College's network, with a view to implementing an IDPS which would detect and prevent known and unknown attacks.

RQ 2. How can network administrator determine security requirements for different data types?

This research question bothers on security policies that affect data on the College's network. Data are valuable asset to any organization. The entire security of a network can be judged on how the data is being protected. Therefore, appropriate rights and restrictions needs to be placed on sensitive data in the network. Identifying staff roles and restrictions on what they can access will help to checkmate and improve security.

RQ 3. What are the problems associated with IDPS's operation?

The aimed of this research work is to improve information security, through the deployment of IDPS on the College's network. However, the operation of IDPS on the College might face some security challenges, apart from the limitations of the software. Therefore, it is imperative to identify the problems associated with its operation, so as to proffer solutions to them. Problems like physical security, employees training, and outdated or non-adherence to security policies, might jeopardize the smooth operation of IDPS.

2.2 Research Methodology

Research methodology as a concept, refers to the way in which researchers conduct research and how they collect the data they need for the research. Whenever researchers investigate a particular subject, they need to adapt the most situated research methodology for the work, to achieve a desirable result. (Kothari 2004, 1.) According to Matos (2012), research methodology is a logical investigation of sources to set up facts and reach new conclusions, in the subject area. Matos (2012) also defined research methodology as an effort to find out new or gather old data, by scientific study of a subject.

The research work is a Case Study using Exploratory and Descriptive Research. Descriptive Research method is used to obtain information concerning the current status of the College, to describe "what exist" with respect to variables or conditions in the network. Case Study involves a range from the survey which describes the subject, correlation study which investigates the relationship between variables, to development of studies which seek to determine changes over time. (Matos 2012.)

Exploratory Research method is a preliminary study of an unfamiliar problem or subject, which researcher has little or no knowledge about. Exploratory Research incorporates the development of concept, theories and assumptions to find a base and in-depth knowledge about a subject. Also, it is used to gain familiarity with an observable fact or to achieve new insight into the subject matter. (Kumar 2008.)

There are different ways in which exploratory research is carried out such as literature survey, experience survey and study of problems to have an insight into a subject area. Interview, questionnaire, and literature analysis were the supplementary research techniques used in this research. This research is based on the analysis of literature and experience survey.

Secondary data is information gathered for purposes other than the completion of a research project. A variety of secondary information sources is available to the researcher gathering data on an industry, potential product applications and the market place. Secondary data is also used to gain initial insight into the research problem. (Kothari 2004, 11.)

2.3 Expected Research Results

There are many factors to consider when deciding on whether to implement IDPS and if it has potential benefits. With this research work, I intend to come up with a framework for YCT that will improve security on its network and increase work efficiency.

The implementations of IDPS and the existing security measures will be of a good deal to the entire staff, network administrators, top management staffs and students of YCT, at large. To the students, they will receive their grades on time and graduate and at the stipulated time. To the staffs, they will be well educated on the security implications for negligence and interference to other staff duties. To the network administrators and top management staffs, they will implement policies that will differentiate data types, and protect the College's network against intrusions.

3 INFORMATION ON YABA COLLEGE OF TECHNOLOGY

3.1 History and objective

Yaba College of Technology is the first tertiary institution established in Nigeria, third in Africa and twenty seventh in the world. The college is one of the recognized institutions in Nigeria. It is made up nine academic units, which are referred to as Schools. The nine academic units are made of thirty-four departments, headed by heads of departments (hereinafter HOD), while units are headed by deans. The academic units are Arts, Design & Printing, Engineering, Environmental Studies, Liberal Studies, Technology, School of Management and Business Studies (hereinafter SMBS), School of Technical Education (hereinafter STE), Science and School of Part-time Studies. (Yaba College of Technology 2011.)

"Yaba the Great" as the College is fondly called, started out as a technical institute in October, 1947 and was called “Yaba Higher College”. The College was renamed "Yaba College of Technology" in 1969, through decree 23 of the Nigerian constitution. In 1979 it was re-named "Federal Polytechnic Yaba", through decree 33, of the Nigerian constitution. However, as a result of relentless pressure mounted by academicians and scholars on the Nigerian Federal Government, it was reverted back to "Yaba College of Technology", in 1980. (Yaba College of Technology 2011.)

According to the decree establishing the college, its main objectives is to provide full time and part-time education and training in Technology, Commerce, Management and Applied Science, in accordance to the need of the development of Nigeria. The highest authority in the College is the Rector. (Yaba College of Technology 2011.)

3.2 Centre for Information Technology and Management

The Centre for Information Technology and Management (hereinafter CITM) is the Unit responsible for Information Technology (hereinafter IT) processing and managing of the College’s computer resources and network. The duties of CITM are highlighted below:

a. Network infrastructure design, development and deployment.
b. Development and management of the College's portal.
c. Management of IT and network resources.
d. Maintenance and repair of computers.
e. Development of Software application
f. Management of LAN, Intranet and Internet access.
g. Provision of technical advice on computers related issues.
h. Provision of computer training to IT staff. (Yaba College of Technology 2011.)

In 2010, the College management divided CITM into three sub-departments, with each having its specific functions. The sub-departments are as follows; (1) Information Processing Department, (2) Systems Development, Hardware and Training Department, and (3) Yabanet and Web Services Department

Figure 2 below depicts the organizational chart of CITM. The head of CITM is the director, an influential office, which also belongs to the College's decision making board. The HODs of the Information Processing, Hardware & Training and Yabanet departments are directly responsible to the director. The program analysts are sub-ordinate to the HODs, and higher in hierarchy than the data processing officers. The Secretary is subject to the data processing officers and higher in position than the clerk. The Clerk is the lowest authority in the CITM organizational chart.

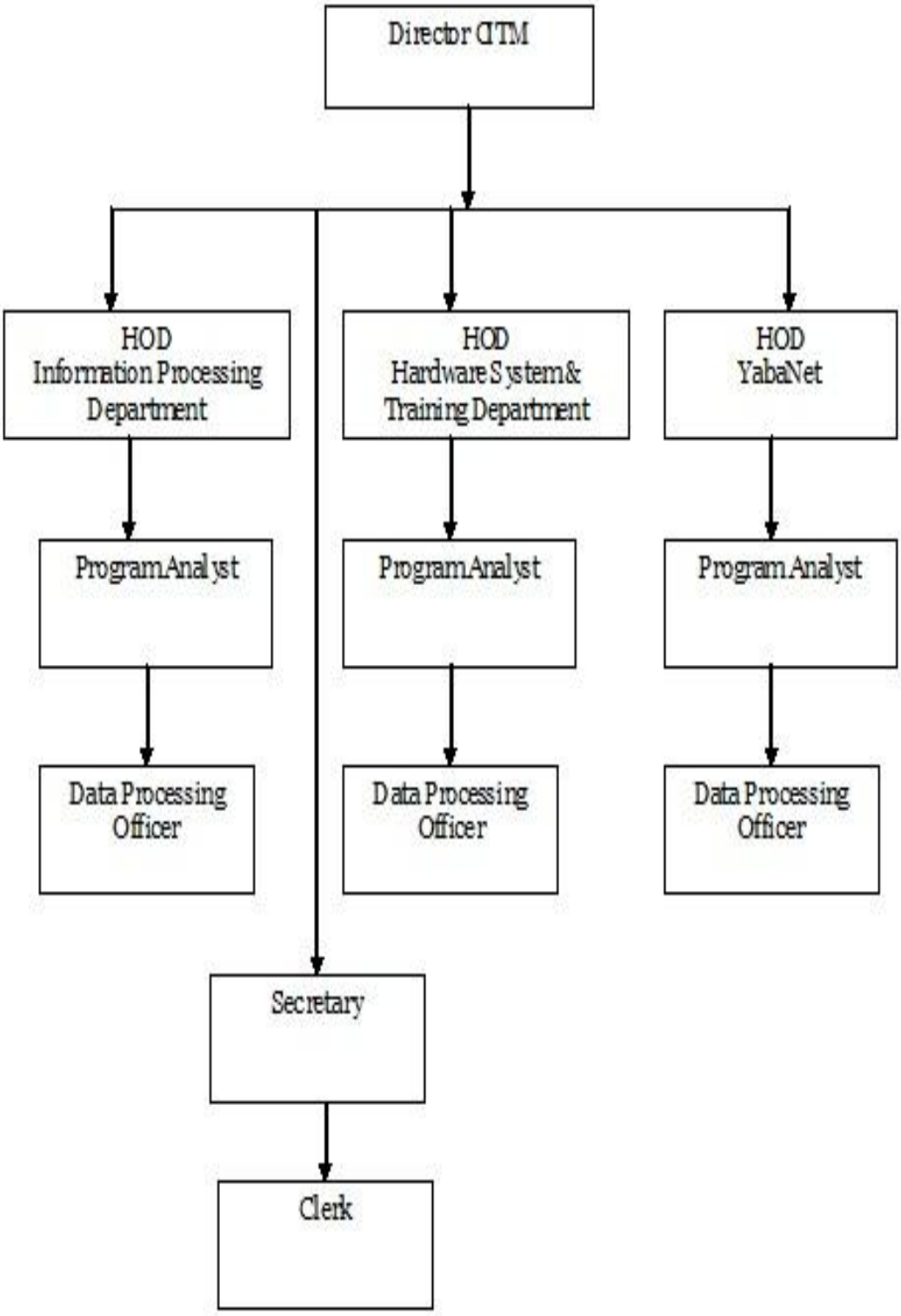

Figure 2. Center for Information Technology and Management Chart (Yaba College of Technology 2011)

3.3 YCT Network Structure

The structure of YCT's network is Transmission Control Protocol/Internet Protocol (hereinafter TCP/IP) model. The TCP/IP model is made of five layers i.e. Application, Transport, Internet, Data link and Physical layer. (Stuart 2011.) The five layers are briefly discussed below.

Application layer provides the brain work needed to support different types of protocols in the network. The common protocols application layer provides supports for are as follows: (1) email application, i.e. Simple Mail Transfer protocol (SMTP), (2) web browsing application, i.e. Hypertext Transport Protocol (HTTP), (3) file transfer application, i.e. File Transfer Protocol (FTP), and remote access, i.e. telnet remote system. (Stuart 2011.)

Transport layer is structured to allow peer entities on the sending and receiving host to communicate without hitches. During transporting process, two end-end protocols are involved. The first one is Transport Control Protocol (hereinafter TCP). TCP is a dependable connection-oriented protocol that permits a byte stream generating from one machine to be delivered without error to other machine. The second is User Datagram Protocol (hereinafter UDP). UDP is not a dependable protocol because it does not maintain a connection, and does not guarantee delivery of communication between peer entities. It is mostly used when prompt delivery is more important than accurate delivery, such as transmitting video between peer entities. (Stuart 2011.)

Internet layer is also called Internet Protocol (hereinafter IP). The internet layer allows host to inject packets into any network and let them travel independently to the desired destination. In this layer, IP is used for addressing and routing across networks, and it is implemented in desktop computers, servers and routers. (Stuart 2011.)

Data link layer in control of exchange of information between machines on a shared network using the same physical medium. It applies the addresses of the sending and receiving machine and can control access to the transmission medium. (Stuart 2011.)

Physical layer defines the physical and electrical interface between a computer and transmission medium. It specifies the features of the medium, nature of signals and data

rates. Local Area Network (hereinafter LAN) is typically used and is denoted as the Ethernet. (Stuart 2011.)

Figure 3 below depicts the levels of TCP/IP model layers, which are discussed above.

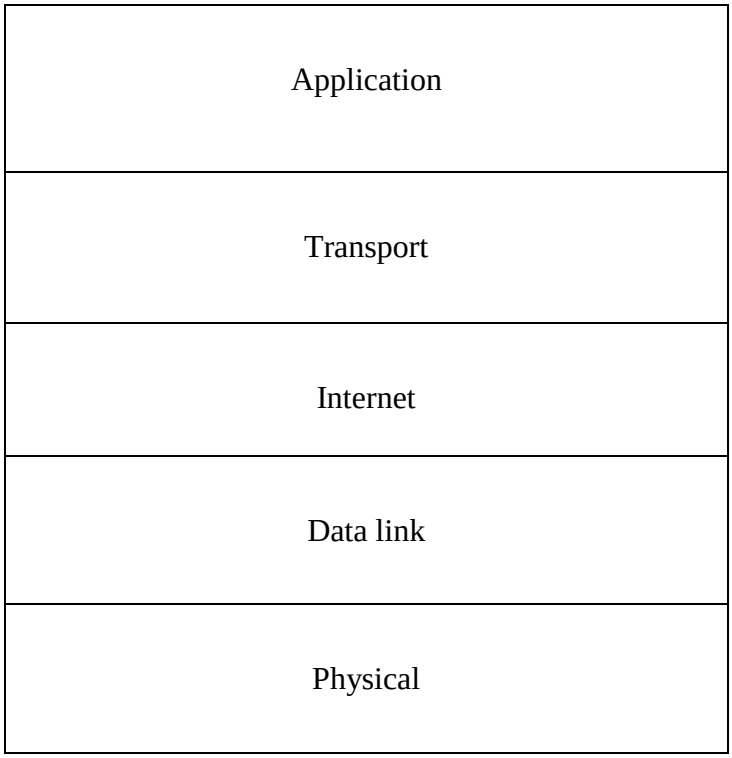

Figure 3. TCP/IP model layers (Stuart 2011)

The TCP/IP model layers structure in figure 3 depicts the sequential arrangement of protocols in the College's network environment.

4 NETWORK ATTACKS AND MITIGATION TECHNIGUES

Network attacks are any means used to maliciously attempt to break into a controlled network system, illegally, to manipulate data. (Tech-FAQ 2010.) As discussed previously, attacks can be internal or external, and can be carried out through a computer that belongs to a network or done remotely.

Today, there are many forms of attacks, known and unknown, which pose serious threat to corporate networks. To protect network from attacks, security administrators must put in place mechanisms or applications to detect all the vulnerabilities present in a network, and know how to defend and mitigate all forms of inevitable attacks. Some attacks require more detailed information about the target network, while some require less. (Meshram & Nalavade 2011.) The major known forms of attacks are discussed below.

4.1 Reconnaissance Attacks

Reconnaissance attack involves collection of information on a network. This type of attack enables attackers to discover loopholes or vulnerable host in a network, before carrying out an attack. Attackers usually gather useful information about the target network before carrying attacks. For instance, attackers may want to know IP addresses that are alive, carry out port scans to know which ports and services that are active on those IP addresses, run vulnerability scan to search for vulnerable host, find out what Operating System (thereinafter OS) is running and what security measures are in place in a target network, before striking. (Orbit-computer-solutions 2011.) Reconnaissance attacks consist of Packet Sniffing, Port scan and Ping sweep and Internet information queries (Csoonline.com 2012).

4.1.1 Packet Sniffer Attack

Sniffing is a process of eavesdropping packets and analyzing traffic in a network. Packet sniffer is software used to captures packets travelling across a network of TCP/IP layer. The software is used as administrative tool for monitoring network

traffic, and as attacking a tool for maliciously eavesdropping packets across networks. (Cisco 2007.)

Mitigation against Packet Sniffing Attack

Packer sniffing attack can be mitigated by using the following techniques: Authentication, Anti-sniffer tools and Cryptography (Cisco 2007).

Authentication

Authentication is a process of identifying authorized users of a network, usually based on a userid and password. This process ensures that users are who they claim to be, by verifying the sender or receiver (Cisco 2006.)

Anti-sniffer tools

Anti-sniffer tools are mitigation technique used for detecting sniffers on a network. These tools cannot completely prevent threat on a network, but can monitor and detect changes in response time of packets sent or received from a host. (Colasoft 2012.)

Cryptography

Cryptography is a process of encrypting data from plaintext to cipher-text over a network. Encryption is a good way to protect data from being sniffed by attackers. Encryption in the real sense won't prevent sniffers from functioning, it will ensure that packets, cipher-text, attackers' sniffs are difficult to understand, when read by them. The standard cryptographic protocols are Secure Shell (hereinafter SSH) and Secure Sockets Layer (hereinafter SSL). (Lawrence 2000, 47.)

4.1.2 Port Scan and Ping Sweep Attack

Port scan and Ping sweep are software used for scanning networks. They can be used as administrative tool for network administrators or as hacking tool for attackers. Network administrators use these tools to search for vulnerable host, loop holes or services in a network, while attackers use it to discover services functioning on a target network. Once insecure hosts or services are found, attackers plan how to launch attack, through the vulnerable openings. (Lawrence 2000, 32.)

Mitigation against Port Scan and Ping Sweep Attacks

It is impracticable to prevent attacker from carrying out port scans and ping sweeps on a network. However, attacks can be mitigated by deploying IDPS in a network structure. IDPS notifies network administrator when a reconnaissance attack is in progress. This warning gives chance for administrator to prepare better for the coming attack. (Cisco 2007.)

4.1.3 Internet Information Queries Attack

Internet querying is a technique of collecting databases of web pages, using titles, keywords or just getting information about an organization. For example, Domain Name System (hereinafter DNS) queries can give information about particular domains, such as who owns the domain and what address is assigned to that domain. DNS translate human-readable domain name into machine-readable IP addresses. So, attackers can get some information about a network using DNS queries. (De Capite 2006, 23.)

Furthermore, network intruders can use query and response protocol like “WHOIS” for getting information from the internet. There is no specific technique to defend or stop information queries. The advisable solution is making sure that only certain organization information, meant for general consumption, are published on the internet. (Cisco 2007.)

4.2 Access Attack

Access attacks are used by attackers to gain access to a network. In gaining access, attackers search for vulnerabilities in a network authentication, File Transfer Protocol (hereinafter FTP) and web services. Once attackers exploit vulnerable protocols, they can gain access to web account and other sensitive data in a network. (Orbit-Computer-Solutions.Com 2011.) Access attack consists of the password, trust exploitation, port redirection, man-in-the-middle and buffer overflow (Cisco 2007).

4.2.1 Password Attack

Passwords are secret words or string of characters that are use for authentication and gaining access to a computer system or network (Whitman & Mattord 2005). Network intruders can try many ways of methods or guessing a user id or administrator's password to gain unauthorized access to a computer or network system (Pfleeger 2006). Password attack can be carried out using the followings methods:

a. Brute-force attack – it is also referred to as dictionary attack. This kind of password attack involves guessing all possible dictionary words until the correct password of authorized users or administrators is found. The intention is to unlawfully gain access to a computer or network system. Today, network intruders use brute-force attack tool, a more sophisticated method in carrying out attacks. The tool searches for detail information, using combinations of character sets to work out every possible password made up of victims' infomation.
b. Packet sniffer – it is used get user ids and passwords details of authorized users, from a computer or network system.
c. IP spoofing Software – this software is used to impersonate network IP address, thereby acquiring user ids and passwords of authorized users. (Whitman & Mattord 2005.)

Mitigation against Password Attack

Network and security administrators can counter password attack using the following techniques: (1) instructing end users to use un-guessable strong password. For example,

upper, lowercase letters, special characters, and numbers would be very difficult to guess or crack, (2) limiting number of unsuccessful login attempts. For example, after five failed login attempts, an account can be disabled, if the correct login details is incorrectly applied, (3) sharing of passwords by authorized users should be forbidden, (4) end users passwords should be changed periodically. For example, system could be programmed in such a way that it asks users to change their passwords every six to twelve months, (5) passwords should be encrypted over a network. If an encrypted password is eave dropped, it would be useless and difficult for attacker or crackers to decode. (Whitman & Mattord 2005.)

4.2.2 Trust Exploitation Attack

Devices operating in a shared environment should trust the information coming from other devices. Trust exploitation attack is aim at bargaining with a trusted host, and in turn, attack other hosts in a network. For example, if a host in a network is protected by a security applications, but is accessible by a trusted host outside the network, the inside host can be attacked through the trusted outside host. (Orbit-Computer-Solutions.Com 2011.)

Mitigation against Trust Exploitation Attack

One effective method to mitigate Trust exploitation attack is, enforcing strict protocols on trusted host within a network (Cathayschool 2011).

4.2.3 Port Redirection Attack

During port redirection attack, compromised host allow traffic through firewall that would be obstructed, under normal circumstances. Usually, port redirection attack does not violate any protocol, but it deceives network or security administrators to think that communication is taking place between two legitimate hosts. For example, when communication is going on between two hosts, initiated by an attacker, malicious software could be installed to redirect traffic from outside host directly to inside host,

therefore, userid/password and protocols used in the network could be stolen. (Stuart 2011.)

Mitigation against Port Redirection Attack

Mitigation of port re-direction attack can be done by double checking appropriate utilization of trust models. Better still, deployment of host-based IDPS can detect an attack and prevent installation of malicious software on a host. (Orbit-Computer-Solutions.Com 2011.)

4.2.4 Man-in-the-middle Attack

Man-in-the-Middle (hereinafter MitM) attack is a common threat posed by attackers. MitM attack is a situation where an attacker intercepts communication between two legitimates host, inject false information and intercept the data transferred between the hosts. Attackers usually use packet sniffers, routing and transport tools, to carry out MitM attack. (Microsoft TechNet 2012.)

Mitigation against Man-in-the-middle Attacks

In Wide Area Networks (hereinafter WAN), mitigation of MitM attack would do by implementing Virtual Private Network (hereinafter VPN) tunnels in a network. VPN tunnels allow attackers to see only encrypted unreadable packets. In Local Area network (hereinafter LAN), configuring port security on LAN switches would be of help against MitM attack. (Microsoft TechNet 2012.)

4.2.5 Buffer overflow

Buffer overflow attack is another common threat on networks. It is a type of attack that occurs when a program or application save more data in a buffer memory than its intended capacity (Fu-Hau & Fanglu & Tzi-cker 2008, 4.)

According to Fu-Hau, et al (2008, 6), buffer overflows attack often occur as a consequence of bugs and improper use of programming languages such as C or C++ that are not memory-safe. For instance, attackers can inject codes into an unsuspecting victim's network system and contaminate services of the host, due to presence of bugs. With the injected codes, attackers can manipulate services running in a network, at will.

Mitigation against Buffer Overflow

Buffer overflow attacks can be restrained by checking buffer's memory constantly. If a buffer contain more data than its intended capacity, it is obvious that the buffer is overflowed and should be restrained to avoid manipulation. (Fu-Hau et al. 2008.)

4.3 Denial of Service Attack

Denial of service (hereinafter DOS) attack is very common on web pages, computer and network systems. In DoS attack, computer or network resources are consumed by attackers' tools, preventing legitimate users from accessing information, and making services unavailable. The attack can also target an entire network, blocking outgoing traffic or incoming traffic to certain network services. Attackers execute DoS attacks using some techniques; Flood, Ping of Death or SYN. The most common type of DoS attack is distributed DoS attack. In distributed DoS attack, attackers flood network host with illegitimate data, which in turn, prevents legitimate traffic from travelling across a network. (IBM.com 2004.)

Mitigation against DoS Attack

Mitigation of Dos attack can be carried out by implementing anti-DoS software application on a network. Also, organization can instruct Internet service provider (hereinafter ISP), to implement traffic rate restrictive software, which restricts amount of needless traffic, travelling across a network. (Orbit-Computer-Solutions.Com 2011.)

4.4 Malicious codes Attack

Malicious codes consist of Worms, Viruses and Trojan horse attacks. The combination of the three codes is also referred to as malware. These codes are common threat to computer systems and network resources. Several researches have shown that malicious codes are easily contacted through email attachments, downloaded knowingly or unknowingly through the internet. (De Capite 2006.)

4.4.1 Virus

A virus is malicious software or program that is attached to a file and it spreads from one computer to another. Computer system or network resources can be infected, if end users intentional run infected programs or unknowingly download software. Virus spreads from one computer system to another with the aid of human interaction. The common ways viruses are transferred are: opening infected files and sharing them over a network. (Whitman & Mattord 2005.)

4.4.2 Worm

A worm is a sub-class of virus which can affect computer system in a same way as virus. However, worm is distinct in the way it spreads, compared to virus. It evokes malicious codes and installs copies of itself in the memory of an infected computer, which in turn spreads to other hosts in a network. Worm usually attaches itself to network hosts and computer servers; this makes its spreading capacity spontaneous. (De Capite 2006.)

The difference between Virus and Worm is that while the former requires human interaction to aid circulation, the latter spreads without any interaction from human or devices. (Whitman & Mattord 2005.)

4.4.3 Trojan horse

A Trojan is a program or software that looks useful, but in real sense has a hidden agenda to harm. The harm is usually not spontaneous as virus or worm. At first, it is made to look useful, but in due cause, it could harm a system. For example, unsuspecting users can download free software application from the internet, which contain a Trojan, without them knowing it. (Microsoft TechNet 2012.)

Most Trojan horses initiate loopholes or backdoor programs on user systems. Once backdoor program is installed, attackers can acquire sensitive information and access infected systems, remotely. (Pfleeger 2006.)

Mitigation against malicious codes Attack

Stopping the spread of malicious code in a network requires prompt actions. Mitigation of Viruses, Worms and Trojan horses can be done through the following techniques below:

a. Scanning infected computers and disconnecting them from a network system.
b. Installing and keeping up-to-date with the latest antivirus software applications from reliable vendors.
c. Keeping network OS up to date.
d. Implementation of host-based IDPS, to detect and prevent malicious codes attacks on network host. (Orbit-Computer-Solutions.Com 2011.)

4.5 Application Layer Attacks

Typically, application layer attacks targets servers by intentionally generating a fault in server's OS or software applications. During such attack, attackers gain ability to bypass normal access controls in a network. By gaining control of applications in a computer or network system, attackers can perform any of the illicit activities as follows: (1) read, add, delete, or modify information, (2) inject malicious programs that has the ability to

copy itself and spread over a network, (3) execute packet sniffer to analyze network and access sensitive information, (4) de-activate authorized users' accounts (5) end software applications running in a network (6) modify OS, and (7) deactivate security measures to facilitate future attacks. It is important to note that application layer attacks can never be eliminated completely, because new vulnerabilities are discovered daily. (Technical News Letter 2008.)

Mitigation against Application Layer Attacks

The risks of application layer attacks can be controlled by implementing some measures. The measures are as follows: (1) reading OS and network log files, (2) subscribing to mailing lists that frequently broadcast network vulnerabilities, (3) up-dating OS with latest patches from reliable vendors, and (4) deploying IDPS on a network. (Knap/SecTools 2010.)

5 INTRUSION DETECTION AND PREVENTION SYSTEM

There are two main types of intrusion detection prevention systems, i.e. intrusion detection (hereinafter IDS) and intrusion prevention (hereinafter IPS) system. The fusion of the two systems brought about IDPS, which is widely used today. On the one hand, intrusion detection is the process of monitoring all activities in a network. It is intended to search for traces of malicious activities that are violations of security policies, peculiar to an organization. Such malicious activities may be deliberately generated by external users, trying to gain illicit access through intranet or the Internet. Malicious activities can also originate from authorized users, misusing their privileges or trying to gain access to vital resources where there are restrictions or are beyond their jurisdictions. Recent research works have shown that large amount of malicious activities are perpetrated by insiders in an organization, misusing their rights and violating security policy. On the other hand, intrusion prevention is the act of conducting detection and blocking detected malicious events from reaching its intended destination in a computer or network system. (Scarfone & Mell 2007.)

IDPS is primarily focused on the following functions: (1) identifying intrusion in a network, (2) logging information from intrusion, (3) attempting to stop intrusion, and (4) reporting intrusion to network or security administrators. Also, organizations use IDPS for other reasons, such as, detecting problems with policies, documenting existing network threats, and restricting violation of security policies. (Kabila 2008.)

5.1 IDPS Detection Methodologies

IDPS detection methodologies are primarily classified into signature-based detection, anomaly-based detection and stateful protocol analysis (Kabila 2008). The three methodologies, along with their major limitations are discussed below.

Signature-based Detection

A signature-based detection is a design that reacts to known and common threats. In a nut-shell, it is a cause of action that compares signatures, known attacks, against

observed incidents in a network, to identify malicious activity. An example of signature is an e-mail titled “Free pictures” or an attachment filename of “freepics.exe”, which are typical features of malicious codes. (Scarfone & Mell 2007, 17)

Signature-based is a simple detection method. It is good at detecting known threats, but unreliable at detecting unknown threats. Very often, attackers conceal threats with the use of avoidance skills, with intension of deceiving security protocols. For example, illustrating with the previous example, if an attacker modifies its code to “freepics2.exe”, as filename, a signature searching for “freepics.exe” would not match it. Thus, such threat would penetrate without being detected. (Scarfone & Mell 2007.)

Anomaly-based Detection

Anomaly-based detection is the means of monitoring system activity and classifying observed events as either normal or anomalous. If the protocol observes events and identifies significant deviations from normal pre-generated “profiles”, it reacts or activates an alarm (Stuart 2011.) An IDPS utilizes anomaly-based detection has profiles that signify normal behavior of end users, service hosts or applications. (Grand 2012.)

An organization utilizing anomaly detection creates a profile for each user group and mechanism on its system. Thereafter, the profiles are used as standard to define end users’ or system activities. If any network activity digresses from the standard, the activity triggers an alarm. (Carter 2002.)

The main advantage of anomaly-based detection technique is that it is efficient at detecting unknown threats. For example, if a system is infected with a new type of malicious code, the code could consume system’s resources and perform other activity that would be different from established profiles; anomaly-based detection would initiate logs to system administrator of deviation. (Scarfone & Mell 2007.) Also, anomaly-based detection easily detects attacks carried out internally, because it deviates from normal activity. For instance, if an authorized user executes actions that are beyond his/her jurisdiction or normal user-profile, the activities would trigger an alarm. Furthermore, because the system utilizing anomaly-based detection is centered on customized profiles, it is tricky for intruders to know what illicit activities they can do

that would, or not trigger an alarm. An anomaly detection system can potentially detect attacks the first time it is perpetrated. (Carter 2002.)

The major limitation of anomaly detection is its complexity, and the difficulty of associating an alarm with specific event. Furthermore, the system has no assurance that a specific attack will trigger an alarm. For instance, if attackers' malicious actions are too close to normal users or system activities, then attacks might go undetected. Also, it is difficult to know which malicious activities would trigger alarm, unless an actual test of attacks against various user-profiles and systems are conducted on a network. (Grand 2012.)

Stateful-protocol Analysis

Stateful protocol analysis is designed to rely on software developer's general profiles that spell out how "particular protocols should and should not be used" (Scarfone & Mell, 2007, 2-6). Stateful protocol analysis provides important capabilities for understanding and responding to attacks.

For example, stateful protocol analysis can spell out unpredictable sequences of commands, such as, issuing same command repeatedly. Another good feature it possesses is that, it performs authentication and keeps records of the authenticator utilized for each activity, and records the suspicious activity (Scarfone & Mell, 2007, 2-6.) Furthermore, stateful protocol analysis can detect variations in command length, minimum and maximum values for attributes, and other potential anomalies that might be not detected by signature- and anomaly-based systems (Scarfone & Mell 2007, 7-8).

In spite of the benefits stateful protocol analysis offers, it also has its short comings. The biggest short coming is the resource requirements. Tracking and analyzing information for systems requires meaningful resources. As performance capacity of processors and networks increases, the challenges associated with resource usage intensify. Another challenge of implementing stateful protocol analysis with IDPS is that malicious traffic may correctly make use of system protocols and, therefore, successfully penetrate without being detected. (Scarfone & Mell 2007, 8-10.)

5.2 Functions of IDPS

Organizations typically have firewalls in their networks today, which filter packets and checkmate traffic, but most still suffer intrusion in their network, YCT not being an exemption. IT professionals are aware of the need for additional protective technologies on a network, therefore, that brought about the development of IDPS.

IDPS is a cost-effective ways to block malicious traffic, to detect malicious codes, to serve as a network monitoring device, to assist in policy compliance requirements, and to act as a network sanitizing device. The main aim of IDPS is detecting and preventing unauthorized intrusions in computer systems and networks. IDPS produces logs of activities in a network, identify when an attack is on, implement the appropriate countermeasures, attempt to stop intrusion and report the incident to security or network administrators. (Kabila 2008.)

Also, IDPS can be designed to recognize violations of organizations security and acceptable user policy. For example, IDPS could be designed to detect and restrict transfers of inappropriate material over a network or downloads of software onto company desktop computers or users laptops. (Grand 2012.)

Furthermore, IDPS is also able to recognize reconnaissance activities, which may signify that an attack is looming. For example, malicious code may perform port scans in order to identify possible targets for an attack. An IDPS might be able to block reconnaissance activity and notify security administrators, who may then enable other security controls and counter the attack. (Kizza 2005.)

5.3 Types of IDPS Technologies

The four main types of IDPS technologies are network-based, host-based, network behavior analysis (NBA) and wireless. Each IDPS technology offers security functions in the following areas: information gathering, information logging, detection of known and unknown threats, and prevention of attacks. However, the systems provide advantages over each other, such as, detecting some malicious activity others cannot or with massive accuracy. (UK Dissertations 2012.)

In many network environments, achieving an effective security solutions require deploying multiple types of IDPS technologies. Thus, achieving an effective security solution, in the case of YCT, require the combination of network-based and host-based IDPS. Network-based and host-based IDPS technologies complements each other The four primary types of IDPS technologies are discussed below:

Network-based IDPS

A Network-based Intrusion Detection Prevention System (hereinafter NIDPS) monitors traffic, and analyzes transport and application protocols to look for suspicious activities, before the unwanted activities gets to the intended hosts in a network (Grand 2012). In addition to its detective and preventive function, it records incidents, notify network administrators, and produce reports to future insight (Brecht 2012).

To achieve an accurate detective and preventive capacity, it is recommended that NIDPS be installed in the inline mode, and not passive. Installing in the inline mode makes monitoring of traffic and blocking of intrusions easier in a network. (Rehman 2003.)

Also, to achieve a desirable result, NIDPS should be deployed in between network devices, such as, switches, firewalls, routers, virtual private network (hereinafter VPN), protocol servers, remote access servers and wireless networks. An example of a reliable open source NIDPS is Snort. (Snort Team 2010.)

Host-based IDPS

Host-based Intrusion Detection Prevention System (hereinafter HIDPS) operate on individual hosts on a network. It monitors all incoming and outgoing packets on a host and notifies an administrator of suspicious activities. (De Capite 2006.) HIDPS is installed locally on host machines, making it a versatile system, compared to NIDPS. HIDPS can be installed on many different types of critical host machines such as in house servers, publicly accessible servers, workstations and notebook computers. (Brecht 2012.)

Network Behavior Analysis IDPS

Network behavior analysis (hereinafter NBA) IDPS detects and prevents suspicious activities on networks in real time. It is structured to give system administrators network visibility needed, to make sure intrusions are promptly identified and controlled. (Violino 2012.)

Violino's (2012) research indicates that NBA analyzes traffic via information collected from mechanisms such as IP traffic flow, or packet analysis tools. NBA exploits signature and anomaly detection techniques to alert security or network administrators of activities that goes beyond the baseline, normal user activities, and responds promptly before damage is done to network resources.

Above all, the primary advantage of NBA systems is the network visibility that it provides system administrators. The visibility helps in two important areas; network operations and security control. (Violino 2012.)

Wireless IDPS

Wireless IDPS monitors frequencies connected to a central server within a network. When monitoring frequencies, it obtains information from spectrum devices and analyzes it for illicit access points, unauthorized entities, policy violations, incorrectly security settings, and wireless attacks such as DDoS. Also, Wireless IDPS can also prevent against threats, by detecting and classifying threats. After detecting and classifying threats, it provides reports and alerts to network administrators. (Brandel 2009.)

5.4 Comparison of IDPS Technologies

As was discussed previously in this work, the main objective of IDPS is to monitor network traffic beyond traditional firewall capabilities, ensuring effective network attack detection and prevention. In some instances, especially busy networks, a single IDPS technology may not provide full security coverage of network resources. As such,

a combination of IDPS technologies may be required for effective network security solution.

In large or busy network environments, an effective IDPS security solution cannot be attained without utilizing different types of IDPS technologies. For example, host-based IDPS cannot monitor network based protocols, and network based IDPS cannot monitor host based activities. Table 1 provides a high-level comparison of the four primary types of IDPS technologies. The strengths highlighted in table 1 depict the circumstances in which each technology type is superior to the others.

Table 1. Comparison of IDPS Technologies (Scarfone & Mell 2007)

Type of IDPS technology	Types of malicious activity detected	Scope per sensor or agent	Strength of IDPS
Network-Based	Network, transport and application TCP/IP layer activity	Multiple network subnets and groups of host	Able to analyze the widest range of application protocols; only IDPS that can thoroughly analyze many of them
Host-Based	Host application and OS activity, network, transport, and application TCP/IP layer activity	Individual host	Only IDPS that can analyze activity that was transferred in peer encrypted communications
Wireless	Wireless protocol activity; unauthorized WLAN in use	Multiple WLANs and groups of wireless clients	Only IDPS that can monitor wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections

5.5 IDPS add-ons

Honey pot

A honey pot is software used to deceive intruders and learn about their tools and methods of attacks, without jeopardizing the security of a network. It is placed in a

strategic location in a network, which will look like loophole, to attract network intruders. While intruders are busy on loopholes and perpetrating a so-called attack, administrators concentrate on the tools and strategies of the attacks and gain more knowledge on their mode of operation. For example, a honey pot can be deployed in demilitarized zone (hereinafter DMZ) or behind a network firewall. (Kizza 2005.)

Deployment of honey pot in a network usually looks as targets for attackers. Also, it can simulate many vulnerable hosts in a network and provide administrators with valuable information on various mode and trends of attacks. As a detective system, it is not a solution to network security, but a tool for discovering malicious activities. It informs administrators on the need and how to improve on network security. (Kizza 2005.)

System Integrity Verifier

System Integrity Verifier (hereinafter SIV) is software that monitors critical files in a network, to find out if they have been accessed or altered. It can also detect other sensitive system components or activities. For example, it usually detect when an authorized user acquires administrator right to access critical files in a network. Additionally, it monitors system registries to find known signatures. An example of SIV is Tripwire; it monitors system files to detect Trojan versions of system binaries. (Kizza 2005.)

Log File Monitor

Log File Monitor (hereinafter LFM) software operates first by creating a record of log files generated by network services. Thereafter, it monitors records, looking for system developments in the log files that would suggest an intrusion is in progress. (Kizza 2005.)

Network Forensic Analysis Tool

Network forensic analysis tool (hereinafter NFAT) is software applications that captures network packets and analyze them according to authorized users' needs. Also, it is used

as a prey to learn about attackers' modes and methods of network attacks, just as honey pot. (Kizza 2005.)

5.6 Challenges and Limitations of IDPS

IDPS technologies act as defensive and preventive mechanism for corporate networks. The system is gradually gaining recognition and acceptance among system administrators. However, there are few challenges faced with the use of IDPS. The common challenge to all IDPS technologies is that they cannot assure complete accurate detection and prevention of attacks. The most common challenges faced with use of IDPS are discussed below.

First, deploying IDPS in switched networks is challenging. Typically, network-based IDPS sensors are deployed in sections in a network where they can sense and monitor packets. However, in switched networks, sensors cannot sense packets accurately, because it is protected from network traffic. Protection of sensor limits the functionality of IDPS. (Kizza 2005.)

Second, IDPS technologies can not yet handle large-scale attack, due to its nature. Typically, IDPS scans every packet, contact points, host and traffic trends in a network. This process takes time in large networks, and sometimes fails to provide real time detection and prevention, thus, limiting its effectiveness. In a nutshell, in large-scale attack, the system cannot be relied on. (Scarfone & Mell 2007.)

Third, IDPS technologies are still reactive rather than proactive. It works on attack signatures. The signature database of IDPS needs to be updated whenever a different kind of attack is detected. This literally means intrusions might still penetrate into a network with IDPS installed. The frequency of signature update varies from vendor to vendor, thereby limiting its effectiveness. (Scarfone & Mell 2007.)

Fourth, IDPS technologies are not totally independent. Sometimes, it requires human intervention or attachment of add-on applications for effective security solution (Grand 2012).

Fifth, IDPS technologies are vulnerable to various forms of attacks. For example, attackers can generate abnormal large volumes of traffic, such as DoS attacks, to attempt to wear out IDPS sensor resource. Once sensor resource is worn out, it becomes blind and cannot detect malicious activity in a network. (Kizza 2005.)

Last, production of false alarms by IDPS sensor or agent is inevitable. False alarm occurs when an IDPS fails to accurately indicate what is actually going on in a network. False alarms falls are categorized into two main subjects: false positive and false negative. On the one hand, false positive occur when authorized users legitimate activities falsely activates an alarm. On the other hand, false negative occur when an IDPS fails to activate an alarm or detect malicious activity in a network. False alarms are a major limitation to IDPS technologies, and often confuse network administrators in carrying out an appropriate action. (Bejtlich 2012.)

5.7 IDPS Components

Typically, IDPS consist of sensors or agents, management servers, multiple consoles, and database servers (Zaugg 2010). The four types of IDPS technologies share the same basic components mentioned. The components are discussed below.

Sensors or agents are critical components that monitor and analyze network for malicious traffic, and notifies network administrators. Sensors and agents are essential components of IDPS, in the sense they play a major role in detecting malicious activities on a network. The IDPS technologies that use sensors are network based, wireless based and NBA, while Host-Based use agents. IDPS sensors can be deployed in two modes; inline and passive mode. In the inline mode, network traffic passes through sensor to analyze traffic for any malicious activity. The basic reason to put sensor in inline mode, in a network, is to stop attacks by blocking traffic, thereby preventing access to network resources. In passive mode, traffic does not pass through sensor itself, rather it analyze copy of network traffic for malicious activity. Typically, sensors in passive mode are deployed at important key locations in a network. (Bejtlich 2012.)

Management servers are centralized devices that receive information from sensors or agents, process and manage information received. Some management servers analyze and correlate information received from various sensors or agents. In larger network environment, there are several management serves that match information received from multiple sensors or agents, compared to small networks, which often use one. (Cisco 2007.)

Database server is used as storage area for information received and recorded by sensors or agents or processed by management servers. Database server is not a vital part of IDPS technologies; however, many IDPS technologies support it. (Bejtlich 2012.)

Console is an application that provides an interface to manage IDPS. The interface is specifically for IDPS's users and network administrators. Some organizations deploy one or more consoles on their IDPS network framework. Some consoles are only used for IDPS administrative purpose, such as configuring sensors or agents, while others are used for monitoring and analyzing packets in a network. However, some IDPS consoles perform both functions: administrative and monitoring. (Endorf & Eugene & Mellander 2003.)

5.8 Network Architectures and IDPS Sensor Location

IDPS is usually deployed in a strategic position in a network, concealed from the knowledge of attackers. The advantages of concealing IDPS in a network are as follow: (1) to safeguard IDPS from being attacked and (2) to ensure that IDPS has sufficient bandwidth to react under hostile situations. (Endorf et al. 2003.)

The sensor in an IDPS does the major task of detecting unwanted activity in a network environment. Therefore, the architectural framework of IDPS borders on how sensors are placed or arranged strategically to provide desired results. Deployment of sensors within an organization's internal network potentially makes them lesser targets, and affords some form of protection, such as filtering obstructions provided by firewalls, switches and screening routers. This section takes a brief insight into the architectural structure and sensor locations of the four types of IDPS technologies.

Network Based IDPS Sensor Location

The location of a network based IDPS sensor in a network is essential for an effective result. As earlier discussed in this research work, sensors can be deployed in an inline or passive mode in a network. Typically, inline sensors are situated where firewalls, routers, switches and other network devices are placed. Deploying sensor in an inline mode, aims at stopping attacks by obstructing network traffic from flowing normally.

Figure 4 shows example of deployment of sensors in an inline mode. Inline sensors are usually situated on the vulnerable side of a network. The location of the sensor reduces work load on network devices, such as a firewall, switch, and router as shown in the figure below.

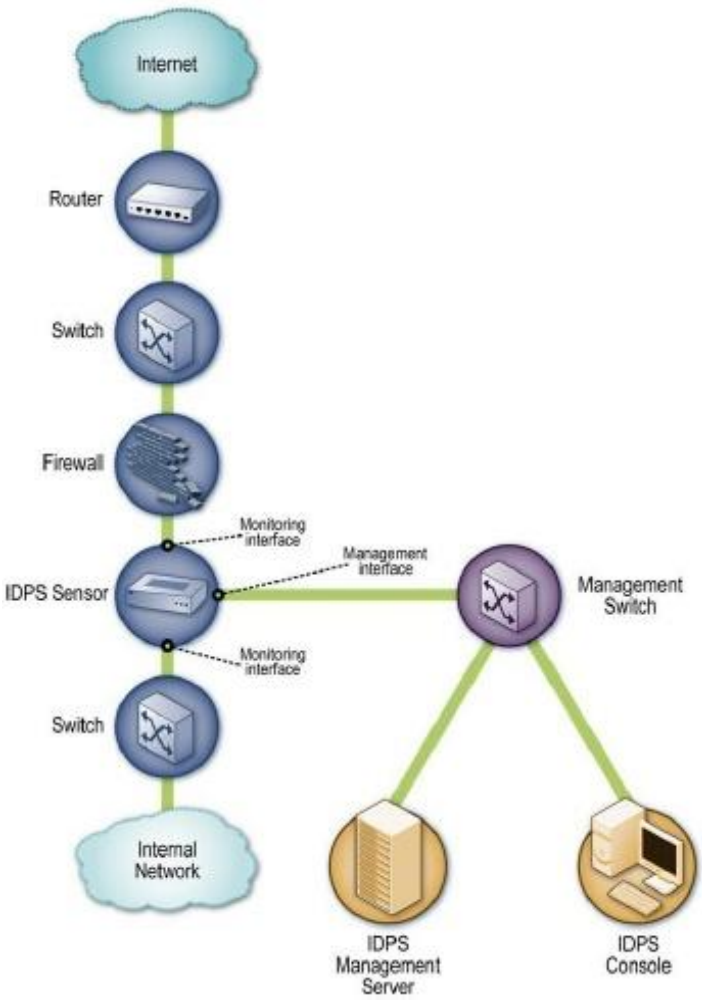

Figure 4. Example of Inline Network-Based IDPS Sensor Deployment Architecture (Scarfone & Mell 2007)

Figure 5 shows an example of deployment of sensors in a passive mode. IDPS sensors are placed before other network security devices; router, switch and firewall. Placing sensor in a passive mode does not guarantee desired result. When a sensor is in a passive mode, it monitors a copy of traffic at a time, which gives way for other traffic to penetrate into a network. It is advisable to deploy sensors in an inline mode; in order to prevent malicious packets.

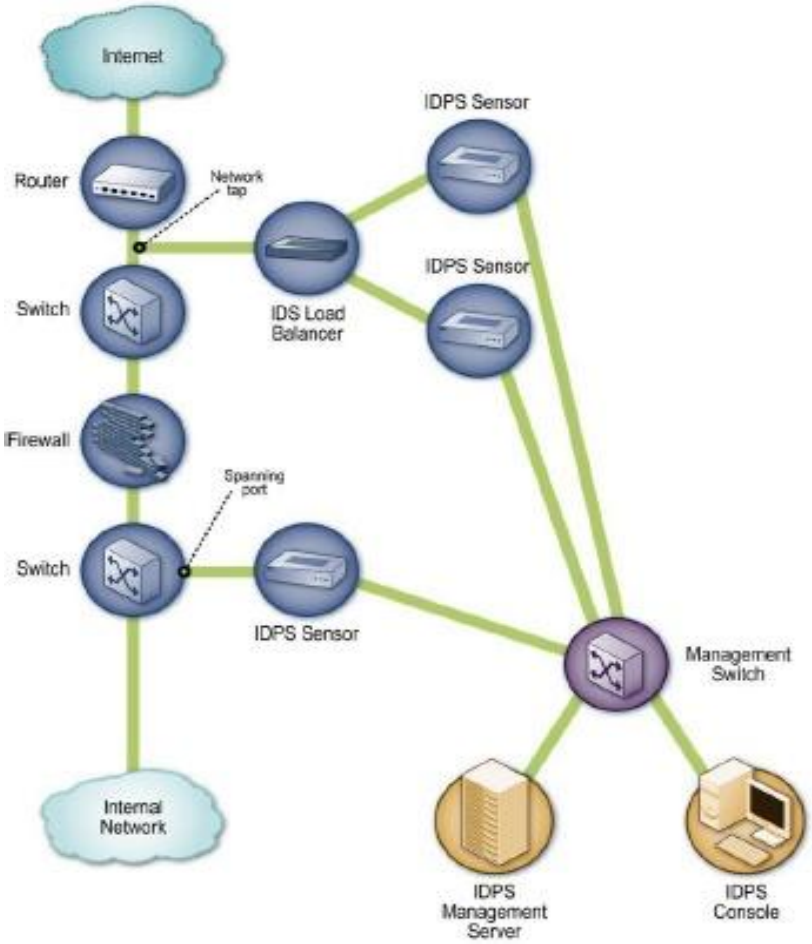

Figure 5. Example of Passive Network-Based IDPS Sensor Architecture (Scarfone & Mell 2007)

Host-Based IDPS Agent Architecture

In the case of host based IDPS, it uses agent and not sensor for detection. Agents are generally deployed on critical hosts in a network. Examples of critical hosts in a network include: servers that can be assessed publicly and servers containing sensitive

data. They are usually installed on hosts of interest. Each agent on a network monitors activity on a single host and performs prevention actions. When an agent detects an unauthorized activity, it logs information to management servers, which process the information and triggers necessary action. (Scarfone & Mell 2007.)

Figure 6 is an example of how agents are installed on different host of interest in a network. The hosts of interests are web server, mail server and DNS sever. The mentioned agents are deployed in inline mode ahead of the hosts that they are protecting. Communications between the mentioned hosts are encrypted, preventing intruders from eavesdropping and accessing sensitive information in the network.

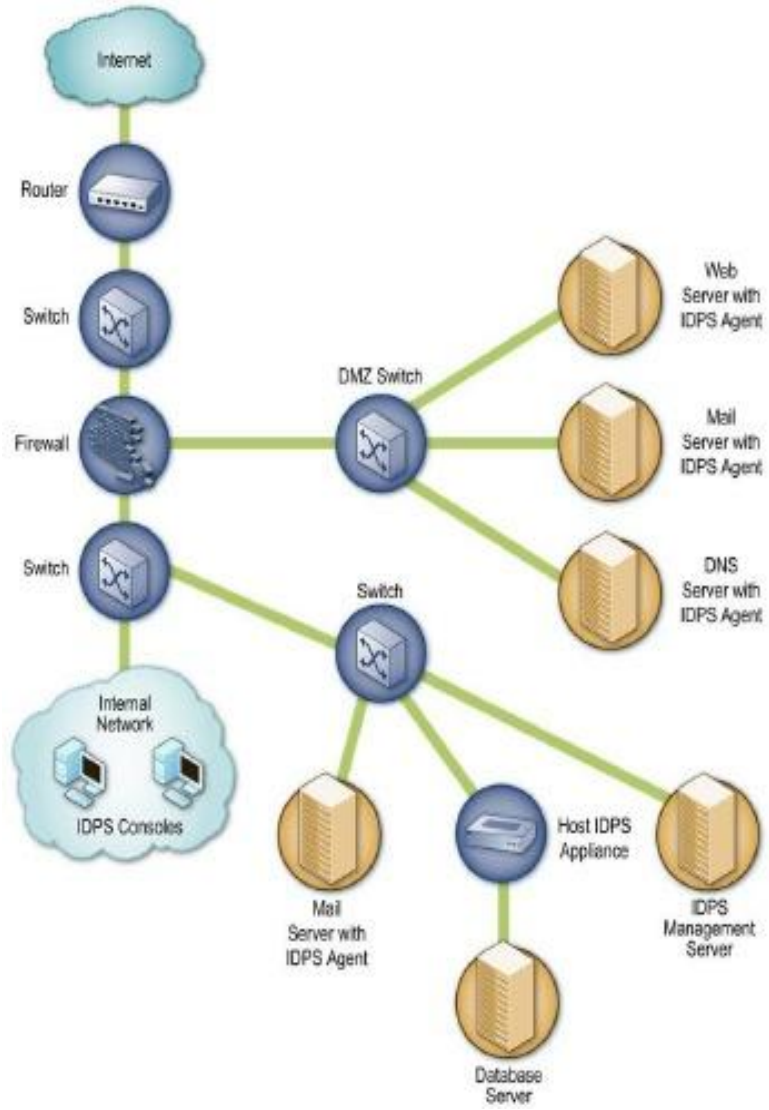

Figure 6. Example of Host-Based IDPS Agent Deployment Architecture (Scarfone & Mell 2007)

Wireless Based IDPS Sensor Architecture

Wireless IDPS sensors perform the same function as network-based IDPS sensors; however, they function in a different way, due to complexities in monitoring wireless communications. Its complexities are drawn to the fact that it cannot see all packets on a networks it monitors, but only samples traffic. Wireless IDPS sensors are deployed in wireless local area network (thereinafter WLAN) network structure. (Scarfone & Mell 2007, 22)

WLAN utilizes wireless networking protocol within a restricted location that broadcast data through infrared signals. Typically, WLAN is used by corporate networks and executed as additional protocol to prevailing LAN to provide improved authorized users flexibility. (Scarfone & Mell 2007, 22-23) Most organization uses the Institute of Electrical and Electronics Engineers (thereinafter IEEE) 802.11 WLANs standards.

Figure 7 shows the deployment of wireless IDPS sensor in network environment. The STAs (stations) are wireless endpoint devices, and APs (access points) are hardware devices that link a wireless network to a wired system. Examples of STAs devices are laptops, desktop computer, personal digital assistants (PDA), mobile phone, and any electronic devices with WLAN capabilities, and that of APs are wireless routers. In the figure below, wireless sensors are deployment in such a way that communication between STAs and APs and the network are filtered and monitored. If the sensors notice malicious packets, they send information to the management server, for appropriate response.

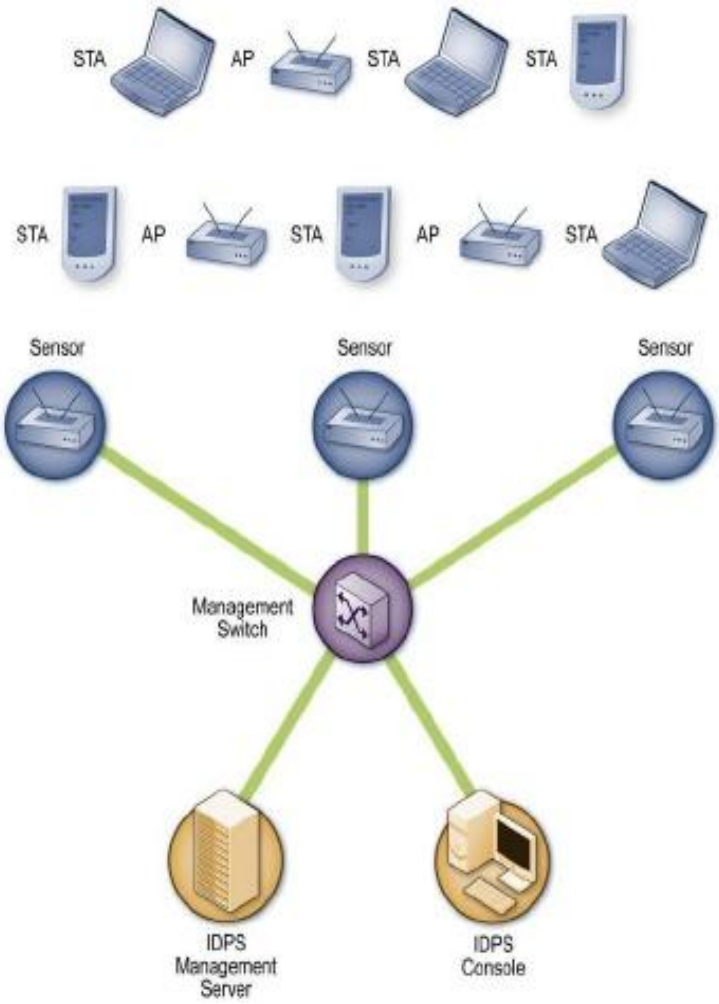

Figure 7. Example of Wireless IDPS Sensor Deployment Architecture (Scarfone & Mell 2007)

Network Behavior Analysis IDPS Sensor

NBA IDPS sensors are usually deployed in passive mode, because they properly monitor key network locations, such as DMZ subnets. NBA sensors are good at detecting large scale malicious activities in a network, such as DOS attack, malicious codes attacks etc. and they can detect when authorized users violate security policies. However, they are less effective at identifying small-scale attacks, such as packet filtering, especially if they are conducted slowly.

Figure 8 shows deployment of NBA IDPS sensors in a network environment. The sensor is in a passive mode and connected to switches and management server. Packets

flow from the sensors to switches, before it gets to the management server. This process is slow and not ideal for a large network, when a timely response to attacks is essential. Additionally, despite sensor being in passive mode, which is better, the process takes time and sometimes malicious activities detected are not marked as abnormal behavior. Therefore, many attacks do not activate alarm until they reach a point in a network, where their activities are considerably distinct from normal. This literally means that attacks that occur speedily may not be sensed until they have altered data, damage files or entire resources in a network.

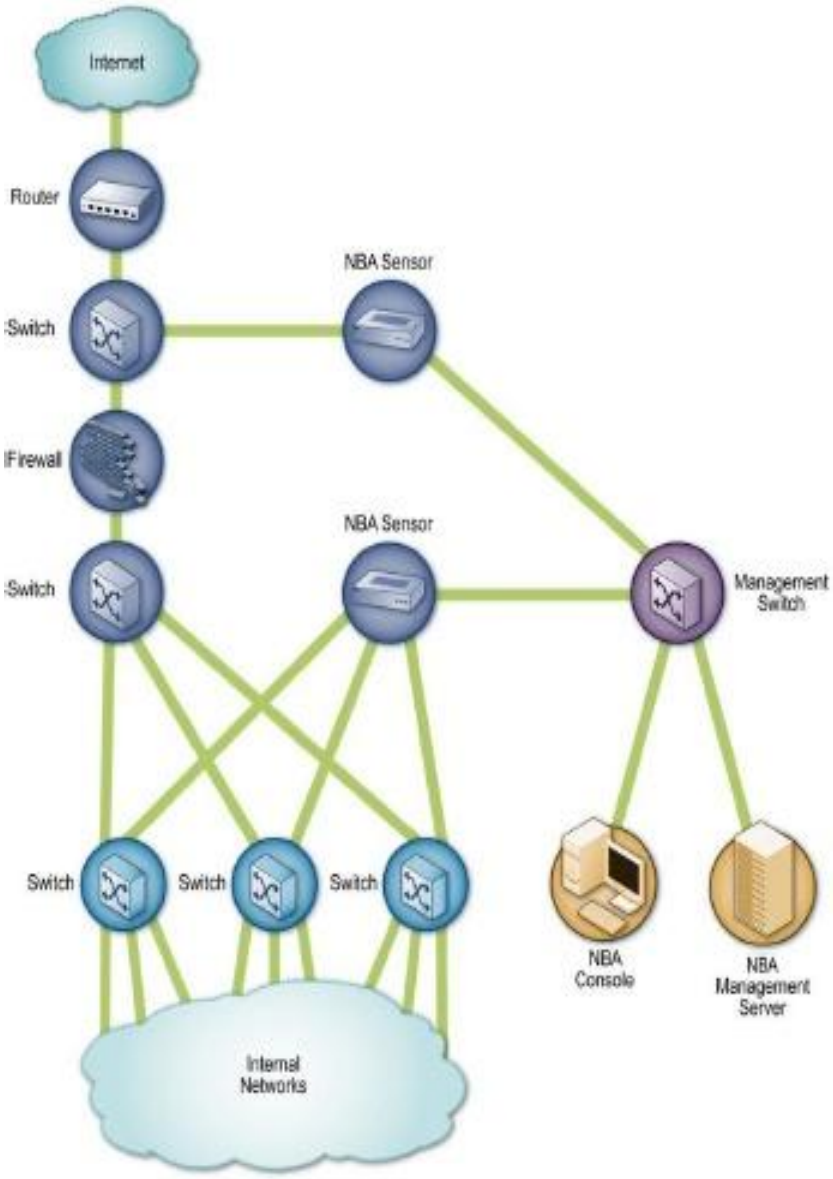

Figure 8. Example of NBA IDPS Sensor Deployment Architecture (Scarfone & Mell 2007)

6 DEPLOYMENT AND TESTING OF IDPS

Several procedures should be considered before deploying and testing IDPS in a network. As a principle, it is better to first deploy and test IDPS in an artificial test environment, before implementing it in a real network. This is to reduce the possibility of interruption for component installations and disruption in work process. Also, deployment of IDPS in a test environment would be helpful in recognizing possible implementation problems and proper solutions when deploying in a real network environment. (Rash & Orebaugh & Clark & Pinkard & Babbin 2005.)

After test running IDPS in an artificial environment, it then can be deployed in the College network. At the beginning of the process, CITM should install only few IDPS sensors or agents, disabling their detection and prevention capabilities. This is because new deployment process could possibly create large amount of false positives until fully modified and customized to the network structure. If many sensors or agents are activated at the same time, it might overwork management servers and consoles, making it difficult for network administrators to perform modification and customization. Therefore, it is better to carry out deployment of sensors or agents in phases, rather than installing them at the same time. Deploying in phases is effective in identifying likely problems with component accessibility. (Rash et al. 2005)

There are other procedures to put into consideration before deployment and testing in the network. Hardware requirement is an aspect that needs to be upgraded. YCT make use of old computers and application components which could hinder speedy deployment process. Up-to-date hardware components for software installations are paramount to ensuring a robust IDPS security solution. Also, OS compatible with specific IDPS is inevitable. Currently, YCT uses Windows OS on its network. Therefore, the College should test run its' OS with IDPS technologies, to check for compatibility.

Placement of IDPS within the network should also be put into consideration. It should be placed in a strategic position that would not be easily detected or seen by attackers. It is a known fact that IDPS is also a target for attacks, as any other resources in a network. Attackers might target IDPS because it often contains logs with valuable information in it about various systems. Once an IDPS is compromised, an entire

network system is vulnerable to any form of attack. As such, IDPS host system should be hardened as much as possible. (Zaugg 2010.)

The Functionality of applications/services running on servers should be considered before deployment. Server applications, web and email, should include logging and auditing features that aid and convey information to network administrators. (Lashkari 2010.)

Lastly, after deploying and testing IDPS, the detection and prevention capabilities of the sensor should be configured, to get started. CITM should bear in mind that regular software and signature updates from reliable vendor is paramount to ensuring that IDPS software components are up-to-date. (Scarfone & Mell 2007.)

Analyses of Test Results

Snort, an efficient and reliable network-base open source IDPS software was used to carry out the test in an artificial environment, using Hybrid Fuzzy and Artificial Neural Networks technique. The reliability of Snort is proven in many research works, and has gained more acceptability by many organizations worldwide, because it analyses traffic and detects malicious packets in real time. (Snort Team 2010.)

The detection methodologies adopted for the test is signature and anomaly-based. On the one hand, signature-based methodology is aimed at seeking defined known patterns of attacks on a network, usually stored in the database of IDPS. On the other hand, anomaly-based methodology assesses what are “normal” acceptable activities in a network, and activates an alarm whenever there are traces of unacceptable activities, which are termed as “abnormal”. (Estévez-Tapiador & García-Teodoro & Díaz-Verdejo 2003, 33.)

Fuzzy technique is derived from the Fuzzy set theory. It is a form of probabilistic logic in testing data types, and deals with observation that is an approximate rather than exact event. Fuzzy techniques are used in anomaly detection of intrusion, because the features to be considered are seen as fuzzy variables. (Estévez-Tapiador et al. 2003.)

Artificial Neural Network (hereinafter ANN) techniques are used in the networking field to detect malicious activities in a network that are complex to be noticed by other computer techniques. (Estévez-Tapiador et al. 2003.)

Results

Fuzzy and artificial neural network techniques were used at different times to carry the test. Different data set and algorithms were used for classifications. The data set and algorithms are briefly explained below:

- Knowledge Discovery in Databases (hereinafter KDD), used to seek new knowledge in some application,
- Multilayer Perceptron (hereinafter MLP), a feed forward artificial neural network algorithm model and,
- Fuzzy C-means (hereinafter FCM), an overlapping clustering algorithm used in Fuzzy technique. (Snort Team 2010.)

After installing Snort, it was tested in a sniffer mode. At first, system takes input from KDD data set and then applies FCM clustering to it. Subsequently, FCM was used to separate normal from abnormal attacks. Then, MLP algorithm was applied to classify the inflow of attacks into the artificial test environment. During testing phase, the accuracy classifications of each attack types were calculated using Fuzzy and artificial neural network techniques. The analyses of the test results are presented in table 2 and 3.

Table 2. Fuzzy technique test result

Type of attack	Input	Output	Detection accuracy
DOS	75	79	98.99%
Reconnaissance	6	6	100 %
MitM	61	61	100 %
Malicious codes	35	35	100 %
Unknown attacks	17	16	95.4 %
Time (in seconds)	4.86		

Table 2 show analyses of the test results conducted in an artificial environment, using Fuzzy technique. Fuzzy technique comprises of FCM clustering algorithm.

Table 3. Artificial neural network techniques test result

Type of attack	Input	Output	Detection accuracy
DOS	68	68	100 %
Reconnaissance	4	4	100 %
MitM	10	5	50 %
Malicious codes	65	66	99.89 %
Unknown attacks	11	17	89 %
Time (in seconds)	3.67		

Table 3 show analyses of the test results conducted in an artificial environment, using artificial neural network techniques.

Conclusively, the overall performance of the proposed System, IDPS, achieves more than 90% accuracy detection for all types of attacks. Network-based IDPS relies on signatures, already known attacks, to identify malicious traffic in a network. Therefore, it is preferable to use multiple IDPS technologies to achieve robust security solution.

Recommended Security Policies and Securing of IDPS in YCT

Security policies and procedure are critical to successful operations of every organization. Security Procedure are statements that outline how policies are enforced, breaches are reported to administrators and consequences for violation of security policy in an organization.

As a rule, security policies should be reviewed periodically and approved by someone or entity other than the author to ensure proper check and balances. A record of the approval should be monitored and maintained for future reference. Good security policies should be precise and easy to understand by authorized users. Security policies should be precise in the following ways: (1) reveal usage of unnecessary service (2) state unwanted software applications (3) address improper user account and password

settings (4) address improper logging and backup settings (5) outline disciplinary or legal action against violators of policies, either internal or external users. (Frye 2007.) Examples of recommended security policies applicable at YCT are briefly explained further below:

Purpose – Access to the network should be controlled because of the danger of an unauthorized person or entity gaining access to the College's network data or resources. This policy should be strictly enforced.

Persons affected – IT staffs, College staff, lecturers and students.

Access policy – Authorized users are issued with user accounts to perform their daily activities. Some employees of the College should be given different rights and privileges to access specific resources in the network, depending on their roles.

Password policy – This policy should generate a standard for creating strong passwords, protection of passwords, and frequency of periodic changes.

Enforcement policy – When any employee, lecturer or student violates the College's security policies, he or she should be subject to disciplinary action. Also, when an employee, lecturer or student leaves or graduates from the College, his/her user account should be disabled three days from the day of leaving, at the latest.

Responsibility policy – Each user should be responsible for protecting his/her information from disclosure. The College's IT department, CITM, which is responsible for creating user accounts, should establish user roles. Furthermore, securing IDPS on the College's network is important, because they are often target of attackers. Once attackers are able to compromise IDPS, they can penetrate into the network and carry out malicious activity.

CITM could implement the following measures to protect IDPS and its components: (1) create separate accounts for each IDPS administrator, since there more than one administrator, and assign only necessary rights and privileges to each of them, (2) configure network devices to limit direct access and contact with IDPS components. Limiting direct contact or access to IDPS components would limit access to only hosts

needed during communications, (3) ensure that communication between IDPS management serves are encrypted by using virtual private network (VPN), (4) application of strong authentication method, two-factor authentication, for remote access to IDPS components. (Scarfone & Mell 2007, 24.)

Deployment of IDPS and implementation of the above recommended measures would provide an additional layer of security on the College's network. Apart from the above recommended measures, YCT's network administrators should also keep in mind that the attacks mitigations methods should not be neglected, but taken seriously.

7 DISCUSSIONS AND CONCLUSION

7.1 Introduction

The main objectives of this thesis work is to explore IDPS and the benefits it provides in counter attacking intrusions and securing network resources in YCT. Although, IDPS technologies are not new, research on intrusion detection began in the mid 1980s. Intrusion Detection Systems were first introduced in the mid 1990s to combat attacks on integrated computer systems, and the fundamental design principles of the systems are unrelenting even until recent years. The increased development of software applications has helped intrusion detection and prevention research to achieve more robust security results. (Pfleeger 2006, 47.)

This area of this research work, intrusion detection and prevention has continued to change, as new research influences design of applications to tackle present day network attacks. Recent trends in the YCT have shown that the use of network defense mechanisms, which includes network firewall hardware and software, anti-malware programs, and switch routers are not enough to tackle the various forms of attacks, perpetrated by internal and external users. Therefore, l recommend implementation of IDPS.

IDPS consists of two systems: IDS and IPS. IDS detect malicious activities or packets, while IPS prevents intrusions or an attack from succeeding or getting to its intended destination. During the course of this research, l found that some organizations utilize IDS and IPS independently to suit their needs. However, the integration of the two systems into one application makes the system more effective.

IDPS is the focal point of this thesis works, and has proven to be an effective security solution for combating intrusions peculiar to YCT. Based on the tests conducted and analysis of the results, using Snort open source application, which recorded over 90% detection accuracy, IDPS would be of help to withstanding attacks and checkmating violation of security policies on YCT's network. However, achieving a desired security solution depends on how IDPS components are strategically deployed and protected, in the College's network. Also, restricting access to IDPS components would go a long way in controlling policy violation and excesses of CITM's staff.

7.2 Avenue for Further Research

Due to the challenges and limitations of IDPS, the researcher has looked at integration concerns and how various network intrusion applications add-ons can be fuse to extend the strength and capacity of the system. However, there still remains the issue of proprietary agreement amongst different IT vendors, to making the fusing of add-on and IDPS a reality. Further research could be done on how open source software could provide for a more open environment, to actualize the concept.

Further research should focus on the need to create common understanding among users of IDPS in various sectors. This is imperative in order to work out meaningful research structures and models, to combat intrusion. Otherwise, the research approaches will continue to be divided and benefits of working out an integrated system model research works will not be achieved.

Lastly, the main objective of this research work centers on providing a lasting solution to the prolonged network intrusion problem of YCT. Since IDPS is not the only application that can be adopted for this purpose, there is room for future research on integrating more open source add-ons to make a more sophisticated system.

7.3 Concluding Note

IDPS is becoming a logical security solution against intrusion for many organizations, after deploying anti-malware programs and firewall application on their network. IDPS offer protection from internal and external attackers, where traffic does not go past firewall or when anti-malware programs fail to prevent malicious codes attacks.

The researcher described four primary types of IDPS technologies: Network-based, NBA, Wireless and Host-based IDPS in this thesis work. Each type of technology proffers the same security purposes: information gathering, logging reports, detection, and prevention capabilities. However, the IDPS technologies offer advantages over each other, such as detecting some activities those others cannot. YCT should consider using multiple types of IDPS technologies to achieve a robust security solution. A robust security solution would offer accurate detection and prevention of malicious activities in

the College network. Also, a robust IDPS security policy checkmates violation of security policy and logs information about violations to security or network administrators.

REFERENCES

Printed

De Capite, Duane 2006. “Self-Defending Networks”: The Next Generation of Network Security. Cisco Systems lnc., 170 West Tasman Dr. San Jose, USA.

Endorf, Carl & Eugene Schultz & Jim Mellander 2003. Intrusion Detection and Prevention. McGraw-Hill Osborne Media, New York.

Este´vez-Tapiador, JM. & Garcı´a-Teodoro, P. & Dı´az-Verdejo, JE. 2003. Stochastic protocol modeling for anomaly based network intrusion detection. Proceedings of IWIA 3–12. IEEE Press, Spain.

Fu-Hau Hsu, Fanglu & Tzi-Chiueh 2008. Scalable Network-based Buffer Overflow Attack Detection. IEEE Xplore, New York.

Frye, Douglas 2007. Network Security Policies and Procedures. Advances in Information Security Vol. 32. Springer Press, USA.

Kizza, Joseph Migga 2005. Computer Network Security. University of Tennessee Chattanooga, Chattanooga, TN, U.S.A

Kothari, C. R. 2004. Research Methodology: Methods and Techniques. 36. New Age International (P) Limited Publishers, New Delhi.

Kumar, Rajendar 2008. Research Methodology. S.B. Nangia, New Delhi.

Pfleeger, C.P. & Pfleeger, S.L. 2006. Security in computing. Fourth Edition. Syngress Publishing, Inc., New York.

Rash, M. & Orebaugh, A. & Clark, G. & Pinkard B. & Babbin J. 2005. Intrusion Prevention and Active Response: Deployment Network and Host IPS. Syngress Publishing, Inc., New York.

Stuart, Jacobs 2011. Engineering Information Security. The Application of Systems Engineering Concepts to Achieve Information Assurance. John Wiley & sons, Inc., New Jersey.

Whitman, Micheal E. & Mattord, Herbert J. 2005. Principles of Information Security. Second Edition. Thomson Learning Inc., Massachusetts.

Whitman, Micheal E. & Mattord, Herbert J. 2008. Management of Information Security Second Edition. Thomson Learning Inc., Massachusetts.

Whitman, Michael E 2004. Defense of the realm: understanding the threats to information security. International Journal of Information Management.

Not-Printed

Brandel, Mary 2009. How to Compare and Use Wireless Intrusion Detection and Prevention Systems. Downloaded January 2012.

<http://www.csoonline.com/article/502268/how-to-compare-and-use-wireless-intrusion-detection-and-prevention-systems?page=1>

Brecht, Daniel 2012. Network Intrusion Detection Prevention. Downloaded March 2012.

<http://www.ehow.com/about_6661697_network-intrusion-detection-prevention.html>

Cathayschool 2011. Intrusion Detection System. Downloaded March 2012.

<http://www.cathayschool.com/Intrusion-Detection-System-a1272.html>

Cisco Systems 2006. A Beginner's Guide to Network Security. Downloaded April 2011.

<http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf>

Cisco Systems 2007. Cisco Networking Academy Program. Downloaded April 2011.

< http://cs.mty.itesm.mx/cursos/ccnp/en_CCNP_ISCW_v5030/ch1/main.html>

Colasoft 2012. Network Sniffer Introduction. Downloaded April 2012.

<http://www.colasoft.com/resources/network-sniffer.php>

Csoonline.com 2012. Network Security. Downloaded January 2012.

<http://www.csoonline.com/topic/41199/network-security>

Carter, Earl 2002. Intrusion Detection Systems. Downloaded April 2012.

<http://www.ciscopress.com/articles/article.asp?p=25334>

Grand, Alberto 2012. Intrusion Detection and Prevention Systems. Downloade January 2012

<http://www.scribd.com/doc/2096981/Intrusion-Detection-and-Prevention-Systems>

IBM.com 2004. Lessons in secure messaging using Domino 6. Downloaded March 2012.

<https://www.ibm.com/developerworks/lotus/library/securemessaging/>

Kabila, R. 2008. Network Based Intrusion Detection and Prevention Systems in IP-Level Security Protocols. Downloaded April 2010.

< http://www.waset.org/journals/waset/v46/v46-115.pdf>

Knap/SecTools 2010. Top 10 Web Vulnerability Scanners. Download May 2011.

<http://sectools.org/web-scanners.html>

Kramer, David 2001. Buffer Overflow. Downloaded January 2012.
<http://searchsecurity.techtarget.com/definition/buffer-overflow>

Lawrence, Teo 2000. Network Probes Explained: Understanding Port Scans and Ping Sweeps. Downloaded January 2011.
<http://www.linuxjournal.com/article/4234>

Lashkari, Arash Habibi 2010. Intrusion Detection and Prevention. Downloaded April 2011.
<http://www.ahlashkari.com/ahlashkari-Coursework/NST/NST-Session-07.pdf>

Matos, Luis Camarinha 2012. Scientific Research Methodologies and Technigues. Downloaded March 2012.
<http://www.uninova.pt/~cam/teaching/SRMT/SRMTunit1.pdf>

Meshram, B.B. & Nalavade, Kamini 2011. Layered Security Framework for Intrusion Prevention. Downloaded December 2011.
<http://paper.ijcsns.org/07_book/201106/20110639.pdf>

Microsoft Technet 2012. Common Types of Network Attacks. Downloaded January 2012.
<http://technet.microsoft.com/en-us/library/cc959354.aspx>

Orbit-Computer Solutions.Com 2012. Computer Training & CCNA Networking Solutions. Downloaded February 2012.
< http://www.orbit-computer-solutions.com/index.php>

Rehman, R.U. 2003. Intrusion Detection Systems with Snort. Downloaded July 2011.
<http://www.informit.com/content/downloads/perens/0131407333.pdf>

Ryabov, Vladimir 2010. Lecture Material on Scientific Writing and Research Work. Downloaded May 2011.

SANS Institute 2012. Information Security Reading Room. Downloaded January 2012.
<http://www.sans.org/reading_room>

Scarfone, Karen & Mell, Peter 2007. Guide to Intrusion Detection and Prevention Systems. Downloaded July 2011.
<http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf>

Snort Team 2010. Snort User's Manual 2.8.0. Downloaded August 2011.
<http://www.snort.org/ >

Technical News Letter 2008. Intrusion Detection Systems. Downloaded March 2010.
<http://ids.nic.in/JCES%20TNL%20OCT%202008/IDS/IDS.htm>

Tech-FAQ 2010. Network Attacks. Downloaded February 2010.
<http://www.tech-faq.com/network-attacks.html>

UK Dissertations 2012. Intrusion Prevention Security. Downloaded February 2012.

<http://www.ukdissertations.com/dissertations/information-systems/intrusion-prevention-security.php>

Violino, Bob 2008. How to Use Network Behavior Analysis Tools. Downloaded February 2012.

<http://www.networkworld.com/news/2008/111008-how-to-use-network-behavior.html>

WiseGEEK 2012. Information Security. Downloaded January 2012.

<http://topics.wisegeek.com/topics/information-security.htm#>

Yaba College of Technology 2011. The Centre for Information Technology and Management (CTIM). Downloaded January 2011.

<http://portal.yabatech.edu.ng/ >

Zaugg, Brian 2010. An Overview of Intrusion Detection Systems Technology and Research. Downloaded October 2011.

<http://www.bzaugg.com/2010/06/an-overview-of-intrusion-detection-systems-technology-and-research>

APPENDIX

1(1)

INTERVIEW QUESTIONS AND RESPONSES

Q1. What version of server, operating system and desktop computers do the College use?
Answer - The College uses web server 2005, Window XP operating system and Pentium 3 desktop computers.

Q2. What security measures are deployed in the network, against intrusions and attacks?
Answer – The College uses net tracker, Noton anti-malware and MacAfee software. Also, for physical protection, there is a fire alarm system, burglary and security personnel in place to guard against fire and theft of software and hard ware components.

Q3. When attack occurs in the network, what and who are the most affected?
Answer – Generally, attacks affects network resources and implementation of certain programs running in the network. Also, it affects students registration, examination registration and students examination grade input in grading systems.

Q4. What types of server does the college use?
Answer - DNS server. The server manages the network and mail system. The DNS server is a system that houses the network monitoring software. It servers has an interface that monitors every operation that goes in the network.

Q5. What challenges do the director, administrators and IT staff face?
Answer – Security structure is customized to the network, which does not give room for flexibility. The College management board sometimes hinders the flow of operations. Also, some Staff exposes vital and confidential information to external persons or entity.

Q6. Does the College organize up-to-date IT training and seminars for its IT staffs?

Answer – Yes, CITM director organizes training in Information processing, hardware components, network intrusion. Every member of the IT staff is trained to fit in into any of the sections.

Q7. Is there restriction to what students can access in the network?
Answer – Yes, students are restricted to certain information in the network. If they (students) try to access anything that is outside their jurisdiction, their operations are stopped, their account disabled and explanation is demanded for their action, before their accounts are restored.

Q8. Who oversee the IT department (CITM)?
Answer – The director is the head and he oversees the running of CITM. Apart from the director, there are two other administrators, but are subject to the director, and most times receive instructions from him. Also, the director overseas all operations units in the college: he makes decision with the head of the departments. Most times, the college management board does not understand reasons why certain policies are implemented.

Q9. Who enforce security policies?
Answer - The director, network administrators and the heads of units enforces implementation of security policies.

Q10. Does the College offer free internet services and what is strength of the bandwidth?
Answer – The College offers internet access on campus, broadband and dial up services for students and staffs. It is interchangeably used, depending on bandwidth consumption. Sometimes dial up tends to be faster than broadband. Staff and Students are restricted to certain websites and software, when accessing the internet.

Q11. Does the College have a defined modality for its network structure?
Answer - The College does not have a defined modality for its network structure. It sometimes has to follow the trend of intrusion or decision made by management board.

Q12. How do network administrators react when there are intrusions in the College's network?

Answer - If administrators notice malicious activities, the malicious packets are suspended, and they try to figure out what is happening to prevent continuity of the intrusion. But if it is a lack scale attack, administrators completely shuts down the network, and decide on the next line of action.

Q13. How often is vulnerability scanning carried out on the network?

Answer - Administrators runs vulnerability scanner on the network every two weeks. But, if there is suspicious in the network, it is done on a weekly basis. The essence of running vulnerability scanner is to search for loopholes in the network. CITM evaluates network vulnerability from time to time, to determine the threats on the network. If there are loop holes in the network, it poses threat, and intruders could strike from the openings (vulnerable host).

Q14. Who determines different data types?

Answer - The Programmers, network administrators, the directors and the heads of units determine different data class in the network. The college evaluates the network vulnerability from time to time, to determine the threats on the network. The College does not have an Incident Response Service (IRS), but has Fire disasters service

Q15. Can you give a brief explanation of the password policy in place?

Answer - The network administrator assign passwords to staffs and students. A new student password is default (password). After registration, it becomes surnames, and thereafter students can change it as they will. There is no limitation to when students can change their passwords.

Q16. Does the college have a security model in place for users of the network?

Answer - The College does not have a specified security model in place for users of the network. However, we are working on implementing a security model, after full consultations and meetings to be held between CITM and the College management board.

Q17. Does the College have a plan to deploy intrusion detection and prevention system in its network?

Answer – Yes, the College is planning to deploy network-based intrusion detection system.

Q18. Do you think a single intrusion detection technology would be strong enough to withstand the numerous attacks it faces on its network?

Answer – For now we would use the network-based intrusion detection system.