ISSN 2278-3091
Volume 3, No.4, July - August 2014
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://warse.org/pdfs/2014/ijatcse04342014.pdf

# Optimizing Frame Work for Secure and Reliable Campus Area Network

**Moses Aggor[1], Kamal Kant Hiran[2]**

[1]Sikkim Manipal University, Research Scholar in IT, Ghana, West Africa, mozargat@yahoo.com

[2]Sikkim Manipal University, H.O.D.-IT, Ghana, West Africa, kamalhiran@gmail.com

## ABSTRACT

Security is an essential component of every network design. When planning, designing, and using a network, you should understand the significance of a strong security policy. Computer-oriented system has three interconnected and cherished machineries to be precise, hardware, software, and data. With the growth of large open networks, security threats have increased extensively in the past few years. Hackers have revealed more network susceptibilities, this is due to the fact that network users can now download applications that require little or no hacking acquaintance to contrivance, applications intended for troubleshooting and maintenance. A reliable and secure system must be able to limit damage and recover rapidly when attacks occur on the network. To ensure data integrity, privacy and availability, there is a need to alleviate emergent threats of cybercrime and provide high secure, reliable research institutes campus area network that will provides dependable networks to service the exploding demand for critical information [3].

**Key words:** Cybercrime, Hacking, Integrity, Privacy, Security threats.

## 1. INTRODUCTION

Generally speaking, the numbers of computer and network security incidents have been increasing bizarrely in the past few years. Such a worldwide phenomenon is having various impacts on our campus information communication technology (ICT) infrastructure, changing from the Denial-of-Service (DoS) to virus infection on end-users' node. In order to sustain a stable and secure computing environment, it is advisable that every one of us, including computer system administrators, software developers, advanced users and normal end users, should take appropriate precaution against various possible forms of network and information security. The primary purpose of preventive measures is to minimize the possibilities of security problems on our campus area network infrastructure [4].

## 2. RATIONALE BEHIND THE PAPER

With increasing number of users, endpoints, and applications active at any time, the campus network becomes more complex, tasks such as developing meaningful security strategies from vast main stream of network 'event' data, or effectively monitoring and regulatory bandwidth in the face of new applications and usage patterns have become extremely difficult. It is clearly more ideal to prevent a problem from happening at all than to remedy the damages after it occurs. Campus networks are extremely difficult to protect. Information Technology professionals are constantly challenged to ensure that all devices logging onto the network are secured, and to effectively ascertain and reduce network attacks. This project will also serve as allusion guide for subsequent security professionals to emulate in securing network infrastructure.

## 3. BACKGROUND OF RESEARCH CAMPUS AREA NETWORK

A research campus area network (RCAN) is a computer network interconnecting a few local area networks (LANs) within research institutions, university campuses and corporate organizations where networks in a number of buildings need to be connected together. This is usually accomplished through bridging and routing. A research campus area network is larger than a local area network but smaller than a metropolitan area network (MAN) or wide area network (WAN). Every network needs protection against people-related, hardware-related, and software-related attack, so each of these areas of network security need to be managed carefully. To secure a network against people-related and failures, good network security procedures must be instigated [1].

## 4. BACKGROUND OF LAN & WAN

A Local Area Network (LAN) is a network of personal computers deployed in a small geographical area such as an office complex, building, or campus within the context of this project. A LAN consist groups of computers and devices that shares common communications lines and share the resources on the same network [2].

WAN is a computer network that directly connects computers separated by long distances more than a mile and as much as half the globe. A Wide Area Network (WAN) provides the means to interconnect several corporate offices over disparate geographic regions allowing data to be shared seamlessly between all sites [3]. This is a key enabling technology for today's expanding business markets, allowing all personnel to interact in a cost-effective way while providing optimal collaboration and data consistency.

LANs and WANs can potentially contain and process sensitive data and, as a result, a plan should be prepared for the security and privacy of these networks. Each system's level of security must protect the confidentiality, integrity, and availability of the information [5].

## 5. COMPARISON OF LAN, WAN AND RCAN

A research campus area network as it has been explained, it is larger than a local area network (LAN) but smaller than a metropolitan area network (MAN) and wide area network (WAN). Research campus area network is expected to interconnect a variety of campus buildings, data centers, E-libraries, lecture halls, conference centers and residential structures. The networking equipment (switches, routers) and transmission media (optical fiber, copper twisted pairs cables) are almost owned by the research institution, university or college.

The table below shows summarized comparison in relation to distance coverage, Technologies and equipment used in each.

**Table 1:** Attributes of Cleveland dataset

| Network | Distance | Equipment | Technologies |
|---|---|---|---|
| LAN | Usually Square Mile | Switches, Routers, Cables | Ethernet, Token, FDDI, Arcnet, etc. |
| WAN | Over Square Mile | Switches, Routers, Cables, Radio, DTE/DCE | Frame Relay, ISDN, ATM, X.25, etc. |
| RCAN | Over Square Mile but less coverage than WAN | Switches, Routers, Cables, Radio, etc. | Ethernet, Token, ISDN, Arcnet, ATM, FDDI, etc. |

## 6. PROBLEM STATEMENT

The main objective is to observe the current state of Graduate School of Nuclear and Allied Sciences University of Ghana-Atomic Campus ICT setup infrastructure, taking into account the underlying topology, technology, security threats, possible vulnerabilities, components and services that are running on the Campus Area Network (CAN).

The prime purpose of this project is to provide measures to minimize the security problems on campus area network infrastructure. It is obviously more ideal to prevent a problem from happening at all than to remedy the damages after it occurs. The analysis would involve the identification of limitations of the current the network setup especially Network Security needs of institute and subsequently the proposal of solutions to the current limitations.

### 6.1 Network Security Architecture

Network security is an ongoing process that helps keep unauthorized parties from gaining access to the network. Alternatively network security is having full confidence in the structure and security measures in place to protect an organization or institution's network infrastructure. It can also be extremely helpful in detecting whether or not a hacker tried to access a system, what areas they accessed and what damage was done[1]. Figure 1 shows the Network security wheel.

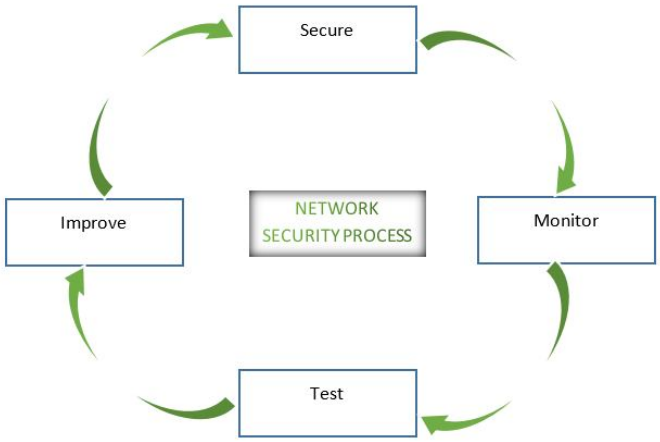


**Figure 1:** Architecture Network security process cycle.
Source: Drawn by Researcher

The diagram briefly explains the various stages involve in securing network infrastructure.

Secure: this is the stage where security measure is set up to protect the network infrastructure and systems on the network.

**Monitor:** this is a stage where the network administrator will critically study the systems to observe the system performance and much it with its expected throughput.

**Test:** Ensures that the system as a whole performs according to the design specification. This is a stage where the security

[1] Rita Anderson:,Veronica Wilkinson, 2004.

measure is critically put into series of test using different inputs to evaluate the results with an expected out come this will help to identify threats and vulnerabilities of the system.

**Improve:** this is a stage where by the whole system is analyzed for a period to identify the system performance build upon the weakness identify from the previous stages to enhance the security performance level and the repeat the cycle [9].

### 6.2 Security

Network security is an ongoing process that helps keep unauthorized parties from gaining access to the network. Network security is having full confidence in the structure and security measures in place to protect the institution's network. It can also be extremely helpful in detecting whether or not a hacker tried to access a system, what areas they accessed and what damage was done [7].

We need to understand the basics of network security, since information is one of the core components of network resources and should be protected from attack. Information security is concerned with three main areas: *namely Confidentiality, Integrity and Availability* of information on the network**.** The figure 2 shows the Information Security Triangle below.

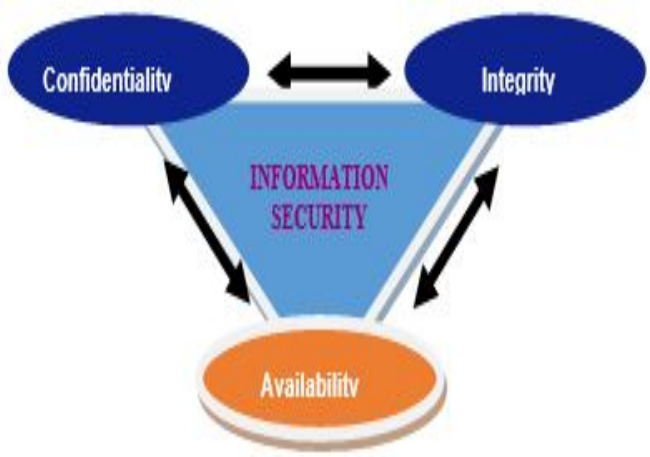


**Figure 2:** Information Security Requirement.
Source: Drawn by Researcher

The above diagram explains the process of information security life cycle. As much as we try to protect and deny authorized access, the information must be available to those who need to access the information at all times when needed [8].

The security methodology described in this document is designed to help security professionals develop a strategy to protect the *availability, integrity, and confidentiality* of data in an organization's information technology (IT) system.

Accidents can occur and attackers can gain access to the system and disrupt services, render systems useless, or alter, delete, or steal information [13].

### 6.3 Network Security attacks analysis flow chart

It is always better to prevent or minimize attacks than to repair the damage after an attack has occurred. It is impossible to prepare against all attacks; therefore, in order to minimize attacks it is necessary to understand the various threats that causes risks to systems. Understanding the main elements of attacks helps us to predict their occurrence [11].

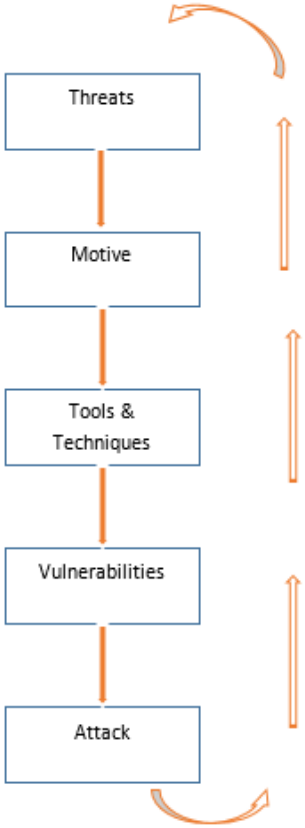


**Figure 3:** Network Security Attack flow Chart.
Source: Drawn by Researcher

From the above diagram, the various facets of an attack can be shown in an equation below to explain stages involve in network attack: Threats + Motives + Tools and Techniques + Vulnerabilities = Attack [12].

### 6.4 Authors and Affiliations

This chapter reviews the literature of the topic *Optimizing Frame Work for Secure and Reliable Research Institutes*

*Campus Area Network Infrastructure*. It consist of theoretical literature which looks into publications related in the research topic and related literature. The definition and function of network security, the concept of Firewall, DMZ (Demilitarized Zone), Network Segmentation, the concept of information security, managing and securing wireless network [10].

The empirical basis of the study in relation to the research fact finding techniques such as observation, interviewing, questionnaire and related literature documentations were used. There are different opinions existing about the nature and meaning of Campus Area Network Security, many people interpret the term *Campus area Network Security* as the steps taken by institutions to prevent network attach either by employees, students and guest users of the campus area network. The institution is highly dependent upon networking and computing technologies. The infrastructure must be protected in order to ensure continuity of services for the core functions such as research, education, and business processes. In every institution, there must be mechanisms and systems that will ensure effective and efficient adherence to the institution's security policy agreement [14].

### 6.5 Methodology

This section covers the methods, techniques and the procedures that were used in gathering the information related to the project. It also explains research design for implementing the project, research style that were adopted and the data collection methods. Methodology therefore plays one of the most important roles in research works. As a result, this chapter looks at the various method, techniques, and procedures, how they were developed and used.

Data collection in research is the stage where the necessary data useful according to the purpose of the research are gathered from the field for the research. The ways for gathering these data for the research is what is termed as data collection method. There are various types of data collection methods, the most commonly used ones are observation, Interviews and questionnaires.

The procedure used in data collection includes primary and secondary data collection. Primary data was collected by administering questionnaires to the management and staffs of the institution as well as conducting interviews and on-site observation. Secondary data was collected from hand books, brochures, text books, internet website, seminars etc.

Questionnaires were designed on a scale for closed ended questions. On the whole, there were averagely seven questions per questionnaire to all categories [15]. The questions in the questionnaire were categorized into six main subheadings namely as follow:

a. Bio-Data
b. Physical Access Controls
c. Logical Access Controls
d. Backup and disaster recovery Controls
e. Network Access Controls
f. Internet & E-Mail Access Controls

Data collected from questionnaires were analyzed using SPSS frequencies, charts, and tables.

### 6.6 Figures and Tables

The table below shows the statistics of response in percentages of the various categories of questions that were administered.

**Table 2:** Category of Questionnaire and Response

| Category | Freq | No | Res. | Yes | No | %yes | %No |
|---|---|---|---|---|---|---|---|
| Bio-Data | 6 | 50 | 36 | N/A | N/A | N/A | N/A |
| Physical | 12 | 50 | 48 | 30 | 18 | 63% | 36% |
| Logical | 8 | 50 | 48 | 34 | 14 | 71% | 29% |
| Backup Recovery | 5 | 50 | 48 | 20 | 28 | 42% | 58% |
| Network | 8 | 50 | 48 | 18 | 30 | 38% | 63% |
| Internet & E-Mail | 3 | 50 | 48 | 35 | 13 | 73% | 27% |

## 7. ANALYSIS

This unit will deal with the detail frame work redesigning the network infrastructure of institution which is the focus of this study and also deals with the background analysis of the data, findings and discussion related to the project work.

Data collected from the research is represented in table forms and pie charts for better interpretation. Analysis was done to draw conclusions in the questionnaires distributed for response. The study population was based on the total number of fifty out of this number distributed; forty-eight questionnaires were retrieved constituting ninety four percent respondents. The following percentages and figures were obtained from the analysis of the sample size. Forty-eight are respondents and two non-respondents.

The following break-down deduction were inferred from the questionnaire responded by simple random sampling and non-probability sampling. Thirty questionnaires responded "yes" for Physical Access Control and eighteen questionnaires responded "no", representing approximately sixty-three percent and thirty-seven percent respectively.

Thirty-four people responded "yes" and fourteen people responded "no" to Logical Access Control questionnaires, this representing approximately seventy-one percent and twenty-nine percent respectively.
Twenty respondents answered "yes" to Backup and disaster recovery Control whiles twenty-eight people answered "no" representing percentage of forty-two and fifty-eight respectively.

Eighteen responded "yes" and thirty people answered "no" for Network Access Control questionnaire, representing thirty-eight percent and sixty-three percent respectively.

Thirty-five respondents answered "yes" thirteen answered "no" for Internet and E-mail Access Control, representing seventy-three percent and twenty-seven percent respectively.

The Bio-data response were not technically significance to the study, therefore they were not critically applicable in the analysis.

**Mathematical Analysis Formulae**

- Quantity of questionnaires=X
- Respondent=Y
- Non respondent=Z
- Yes=α
- No=β

Calculating percentages for both "Respondent" & "Non Respondent" in the analysis table was done using the following mathematical extrapolation formulae:

**Analysis of Respondents and Non-Respondents**
**Respondents**
Y /X*100%
48/50*100%= 96%

**Non-Respondents**
Z /X*100%
2/50*100% = 4%

**Table 3:** Analysis of Respondents and Non Respondents

| Response | Frequency | Percentage |
|---|---|---|
| Respondents | 48 | 96 |
| Non Respondents | 2 | 4 |
| **Total** | **100** | **100** |

The above analysis is illustrated in the graph below.

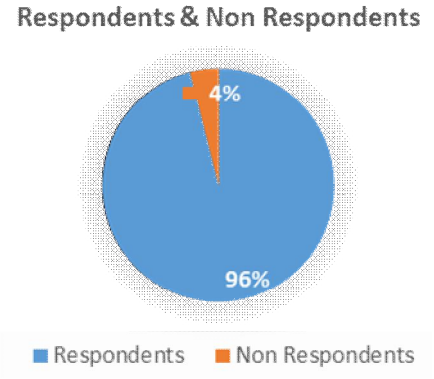


**Figure 4:** Respondents and Non Respondents Chart

Extrapolating percentage calculation for "yes" or "no" respondents using Network Access Control results for clearer inference.

**Yes (α) Respondents**
α/Y*100%
18/48*100% = 37.5%

**No (β) Respondents**
β/Y*100%
30/48*100% = 62.5%

**Network Access Control Analysis Results**

Eighteen responded "yes" and thirty people answered "no" for Network Access Control questionnaire, representing thirty-eight percent and sixty-three respectively.

**Table 4:** Network Access Control Analysis Table

| Response | Frequency | Percentage |
|---|---|---|
| Yes | 18 | 37.5 |
| No | 30 | 62.5 |
| **Total** | **100** | **100** |

The above analysis is represented in the figure 5 bellow:

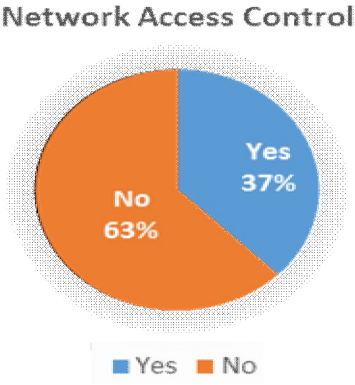


**Figure 5:** Network Access Control Questions Chart

Figure 5 shows, an extrapolation from the questionnaire shows that sixty three percent of respondents attest to the fact that the network access control is of low quality in terms security control mechanism whiles only thirty seven percent of the respondents opt for good network security access policy. In view of this, it can be concluded from the inference that there are no suitable security infrastructural mechanism in place, therefore, it is recommended that the appropriate network security policy systems is implemented to enhanced the level of network access control, Backup and disaster recovery systems to provides business continuity of the institution.

## 8. CONCLUSION

Network security consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of services and network-accessible resources[18]. This project is purposed to deal with network infrastructure security such as computer users, students, professionals, lecturers and researchers, how to deal with network attack on research institutions network infrastructure [17].

When designing a secure network, some goals need to be taken into consideration. These goals of network security are to protect networks against attacks, with the intent of ensuring data and system availability, confidentiality, and integrity. A good network design must meet all these requirements. This paper covered the basics of network design, network design principles, network design methodology, and physical security issues [19].

## ACKNOWLEDGEMENT

Firstly, we would like to thank our families for enduring the piles of manuscripts and late-night proofing that goes with putting together an anthology and special thanks to Dr. M. K. Doshi, who constantly inspired to involve in the research work. Finally we are thankful to Dr. Abhishek Tyagi, Dean, Sikkim Manipal University, LC Ghana, West Africa for providing the necessary facilities for the preparation of the paper.

## REFERENCES

1. Danquah, P. (2008). **Campus Area Network**. Pentvars Business Journal, P.84.
2. Hvalshagen, M. (2004). Transforming the IT organization for the state of Virginia. **Information Systems Management**, 21(4), 52-61.
3. networkdesign/article3.html. (n.d.). Retrieved from www.relativitycorp.com:
4. Rita Anderson:,Veronica Wilkinson. (2004, January). www.educause.edu. Retrieved from www.educause.edu: http://www.educause.edu/library/resources/securing-campus-network
5. http://www.freewimaxinfo.com/campus-area-network-can.html
6. Aggor, A. & Boateng, F. A. (2011). **Securing Canpus Area Network**. Final Year Project work , P.34.
7. Resources/SecuringtheCampusNetwork/160832. (n.d.). Retrieved from www.educause.edu:
8. Tobin, D. P. (2010). **Information Security**. Accra-Ghana: Lecture Note.
9. Benson, C. Bensch, D., Human, D., Klerk, L. D. & Grobler, J. (n.d.). **Technet Microsoft**. Retrieved from technet.microsoft:
10. Westra, B. (n.d.). library.uoregon.edu. Retrieved from library.uoregon.edu: https://library.uoregon.edu/datamanagement/storage.html
11. http://my.safaribooksonline.com/book/networking/security/1587051672
12. Babb, D. L. (2004). www.drjimmirabella.com. Retrieved from www.drjimmirabella.com:
13. Blanding, S. (2013, 12 02). www.cccure.org. Retrieved fromwww.cccure.org:
14. Benson, C. Bensch, D., Human, D., Klerk, L. D. & Grobler, J. (n.d.). technet.microsoft. Retrieved from technet.microsoft: http://technet.microsoft.com/en-us/library/cc723506.aspx
15. Budd, C. & Berg, G.. (n.d.). en-us/library/cc723506.aspx. Retrieved from technet.microsoft.com:
16. Cisco-Cisco-Catalyst-3560-24PS-SMI-Switch-24-Ports. (n.d.). Retrieved from www.shopping.com: www.shopping.com/Cisco-Cisco-Catalyst-3560-24PS-SMI-Switch-24-Ports-EN-Fa/prices
17. forum/remark,15183569. (n.d.). Retrieved from www.dslreports.com: http://www.dslreports.com/forum/remark,15183569
18. Berman, F. (2013, o7 2). Data Replication. Data and Computing. Data and society.
19. gns3.net. (n.d.). Retrieved from www.gns3.net: http://www.gns3.net
20. IT-security-services.aspx. (n.d.). Retrieved from www.koenig-consultancy.com: http://www.koenig-consultancy.com/IT-security-services.aspx