Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication – A Case Study at UMaT*

[1]F. L. Aryeh, [2]M. Asante and [1]A. E. Y. Danso
[1]University of Mines and Technology, P.O. Box 237, Tarkwa, Ghana
[2]Kwame Nkrumah University of Science and Technology, Kumasi, Ghana

Aryeh, F. L., Asante, M. and Danso, A. E. Y. (2016), "Securing Wireless Network Using pfSense Captive Portal with RADIUS Authentication", *Ghana Journal of Technology,* Vol. 1, No. 1, pp. 40 - 45.

Abstract

Wireless network has become very significant in offices, industries, homes, colleges and universities. It serves as a platform for users to connect to resources on a local network or the internet without intrusive wiring. As a result, it is very crucial to use a good authentication method to avoid unauthorised users to have access. An unsecured wireless network can put users in danger. Anybody can spy their online activities and have access to their files and documents depending on how the network is configured. Currently, one of the most effective ways of achieving a secure wireless network authentication is by using a Captive Portal with Radius authentication method. Captive Portal is a web page that controls any Hyper Text Transfer Protocol (HTTP) browser access to the internet. A user on the wireless network trying to access the internet would be redirected to a web page either for both authentication and payment or just for authentication. Authenticated users are identified by the MAC address of their Ethernet card. RADIUS is a networking service that authenticates and authorises users to networks and network infrastructures. This paper seeks to demonstrate how to use an open source pfSense, a firewall on FreeBSD operating system with Captive Portal and Active Directory for managing user authentication on the University of Mines and Technology (UMaT) wireless network.

Keywords: Securing, Wireless, Network, pfSense, Captive Portal, RADIUS Authentication

1 Introduction

In this 21st century, the internet has become a powerful tool for everybody regardless of age. Its purpose varies among users. Some see it as a reliable source of getting information and making a business transaction. Others also use it as a medium to connect to different people across the globe on social networks, play online games, upload and download music and videos, etc.

People can connect to the internet either through a wired or wireless network. A lot of universities prefer wireless means of providing internet to the wired connection using wireless local area networks (WLAN). This is because it has flexibility in installation and cost. Since it uses Orthogonal Frequency-Division Multiplexing (OFDM), it allows users to move around within a local coverage while still connected to the network. However, wireless networks are prone to some security issues (Appenzeller *et al.*, 1999). So necessary measures must be taken to ensure security. Therefore, it is very important to deploy secure methods for authentication and encryption so that the network can only be used by those individuals and devices that are authorised.

In a WLAN, communication and data transfer use radio transmission, which is open to all users (Soewito, 2014). This attracts people to use WLAN without permission. The reasons behind are to get free internet access, steal data, spy on other users' activities or even damage the system. As a result, Wired Equivalent Privacy (WEP) was the 802.11 standard initially published in 1997 by the IEEE to avoid unauthorised access and encrypt data (Radvan, 2010).

WEP has been deprecated because of the vulnerabilities associated with obtaining the security keys. In response to these vulnerabilities found in WEP, Wi-Fi Protected Access (WPA) was introduced in 2001 by the WiFi Alliance (WFA) to curb the problems associated with WEP. WPA uses the Temporal Key Integrity Protocol (TKIP) which uses dynamic keys that were not backed up with WEP and RC4 for encryption. The TKIP method used with WPA was utilized until vulnerabilities were found in TKIP. These vulnerabilities centre on the fact that TKIP uses some of the same mechanisms that WEP does which allow similar attacks. In response to the vulnerabilities in WPA/TKIP, the IEEE 802.11i standard was defined and implemented in June 2004. WPA2 replaced TKIP with Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) which is based on Advanced Encryption Standard (AES) (Sean, 2011).

However, some researchers have uncovered a vulnerability in the WPA2, which is the strongest for Wi-Fi encryption and authentication currently standardized and available (Mamat *et al*., 2013). Hence, to improve the security of WLAN, a new

*Manuscript received August 23, 2016
Revised version accepted September 16, 2016

secure mechanism called Captive Portal has been introduced which uses a webpage to authenticate users. If a user tries to access the internet, the web browser redirects the request to a login page. As long as the login process is transported over a secure connection like TLS it will be difficult for malicious users to intercept other users' login details (Cisco, 2011).

Also, IEEE has developed advanced authentication and encryption protocol called 802.1X to solve the vulnerabilities found in WPA2. However, the 802.1X standard needs devices that work with the protocol, making it complicated than Captive Portal. Therefore, 802.1X is not widely deployed in WLAN. Another advantage of Captive Portal is that users need not install the access controller software on their mobile device. All they need to do is start a web browser to authenticate themselves.

There exist quite a few numbers of Access controller, which are licensed for free or commercial use that integrates Captive Portal. Few examples are:

(i) Air Marshall, software-based for Linux platform (commercial);
(ii) LofiSense, Billing &OSS / Network Access Control (commercial);
(iii) PacketFence, Linux-based Network Access Control Software with Captive Portal (open source); and
(iv) pfSense, FreeBSD-based firewall software derived from m0n0wall (open source).

pfSense is an open source firewall/router software which is based on FreeBSD operating System (Mamat *et al.*, 2013). It also supports the installation of third-party packages like free Radius or Squid through its Package Manager.

2 Resources and Methods Used

2.1 Resources Used

Several softwares and hardware were employed to successfully complete this research paper.

2.1.1 Software Employed

The softwares used are: Virtual Machine, Microsoft Windows 10 Operating System, FreeBSD, Windows Server 2012 R2, Windows 7 and Windows 8.

2.1.2 Hardware Employed

The hardware used are: Dell Laptop and Cisco router.

2.2 Methods Used

A virtual player was installed on a notebook computer running Windows 10 operating system. The notebook computer was connected to a wireless router which provided internet service obtained from an internet service provider. The virtual player has FreeBSD, Windows Server 2012 R2, Windows 7 and Windows 8 installed as individual Operating Systems serving specific functions.

Windows 7 and Windows 8 in this setup represent users who have to authenticate themselves in their web browser before granting access to the internet. Windows Server 2012 R2 has Active Directory (AD) and Network Policy Services (NPS). AD contains users' credentials for authentication whiles NPS allows network administrators to create network policies to authenticate and authorise connections from wireless access points and authenticating switches (also called RADIUS clients). As a result, the Network Policy Server is acting as a local RADIUS server. The Windows server must be assigned to a static IP address.

The FreeBSD runs pfSense solution which basically performs four different functions in this setup. These are:

(i) It acts as a firewall, i.e. a software that secures data from being accessed outside the network and also prevent data from leaving the network through an inside source.
(ii) Acts as a router by serving as a gateway for all users on the network to the internet.
(iii) Act as a DHCP server, i.e. assigns IP addresses to clients on the network dynamically.
(iv) Acts as a Proxy Server, i.e. acting as an intermediary for clients seeking resources from other servers.

Fig. 1 shows the setup for the whole experiment. pfSense provides an option in the terminal to configure interfaces and also set their IP addresses. Based on the setup of the experiment, the virtual player will use a Network Address Translator (NAT) to provide pfSense WAN interface with an IP address.

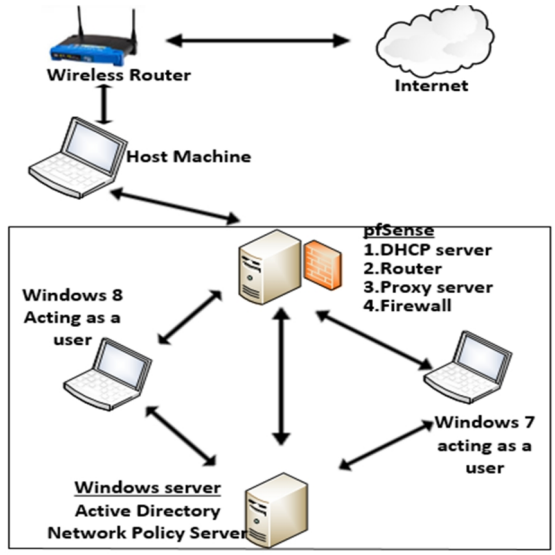

Fig. 1 Experiment Setup

In order to use pfSense Captive Portal for UMaT wireless network, pfSense has to be installed on a server and configured with one LAN interface to assign an IP to the appliance. This configuration can be done using a bootable CD that can boot pfSense using a PC as shown in Fig. 2.

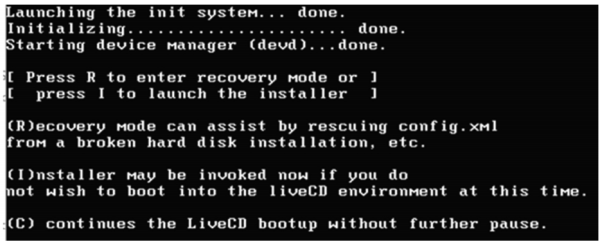

Fig. 2 pfSense Installation

The LAN interface has to be assigned a static IP address and default gateway. Every user on pfSense LAN has to pass through this default gateway before he/she reaches WAN network. Fig. 3 shows the configuration of WAN and LAN interfaces with the necessary IP addresses.

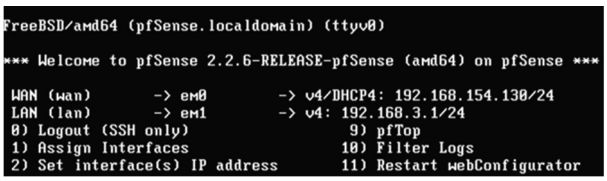

Fig. 3 pfSense WAN and LAN Interface Configuration

By using the experiment setup as above, we investigate the following:

1. How to configure pfSense Captive Portal?
2. How to configure RADIUS server?
3. How to set the policy and security mechanism?
4. How to manage user credential?

3 Results and Discussion

3.1 pfSense Captive Portal

Captive Portal can only use the LAN interface of the pfSense firewall. In setting up the portal with RADIUS authentication, the Captive Portal check box was enabled, interface selected, RADIUS authentication checked, and upload an HTML page with portal contents as described in the section called "Portal page contents" of the Captive Portal configuration page. The configuration of a local user on the Users tab of the Services Captive Portal page was then completed. The Captive Portal detail configuration options are as follows:

1. Interface – select the LAN interface Captive Portal will run on.
2. Maximum concurrent connections – This field specifies the maximum number of concurrent connections per IP address. It has a maximum limit of 50. This limit exists to prevent a single host from exhausting all resources on pfSense firewall, whether inadvertent or intentional.
3. Idle Timeout – Set the time to 15 minutes. It will disconnect idle users and users will be able to log back in immediately.
4. Hard Timeout – To forcefully log off users after a specified period. It will ensure sessions are removed if users do not log off, as most likely will not. Users will be able to log back in immediately after the hard timeout, if their credentials are still valid.
5. Logout Popup Window – Check this box to enable a logout pop up window. Most browsers have pop blockers hence logout popup windows may not work in most browsers.
6. Concurrent User Login – Check this box. If this box is checked, only one login per user account is allowed. The most recent login is permitted and any previous logins under that username will be disconnected.
7. Authentication – Choose RADIUS authentication. Do the necessary configuration by entering the RADIUS server IP address, Port number and shared key to let Captive Portal communicate with RADIUS server.
8. Authentication Error Page Content – Upload an HTML page to be displayed on authentication errors. An authentication error occurs when a user enters a bad username or password.

3.2 Local RADIUS Server

The purpose of the RADIUS server is to serve as an authenticating server. In configuring the server, there is the need to create a RADIUS client that will forward the user authentication request to the RADIUS server. The static IP address assigned to the Windows Server will be the exact address for RADIUS, since the Windows Server serves as a host of RADIUS. Fig. 4 shows the configuration of a RADIUS client in a RADIUS server.

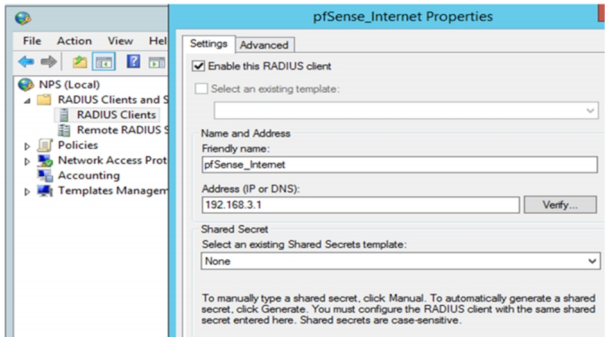

Fig. 4 Creating RADIUS Client

After creating the RADIUS client, you have to set network policies to tell RADIUS which AD groups to authenticate. You can also specify the kind of authentication protocol that the RADIUS server should use. In this setup, the RADIUS server uses Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2). Fig. 5 shows the set policies for the network in the RADIUS server.

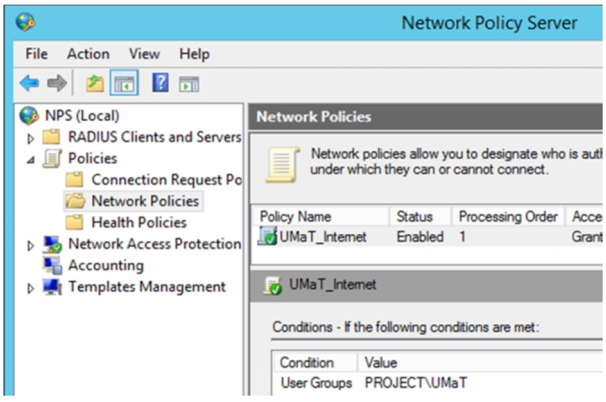

Fig. 5 Network Policies for RADIUS Client

3.3 Managing Users' Credentials

AD is used to store users' credentials. The highlighted rows are few user credentials that are linked to the RADIUS server in this setup. They belong to a single AD group. About 5 user credentials were created. These credentials were put into a created user group called UMaT. This differentiates the credentials from the default users' groups already stored in the AD. By so doing, more user credentials can be added and deleted on this interface. Fig. 6 shows Users credentials created for the experiment.

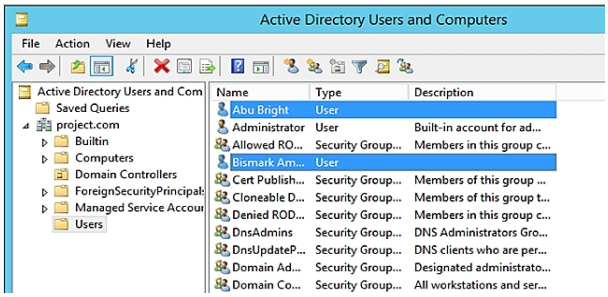

Fig. 6 Adding User credentials in AD

This paper aims at disabling concurrent logins for Captive Portal, hence, provision was made by generating vouchers for guest or visitors to the university to also have access to the internet. The voucher option in the Captive Portal was enabled before the generation of the voucher codes. In generating voucher codes, the necessary requirements need to be specified before saving. The voucher will be generated automatically based on the specification. The blue button on the far right side of the voucher row is the download link for the generated voucher codes. Consequently, generating codes for visitors or guests who come for conferences on UMaT campus becomes very easy. Fig. 7 shows generating 15 voucher tickets with a time span of 2 days i.e. 2880 minutes.

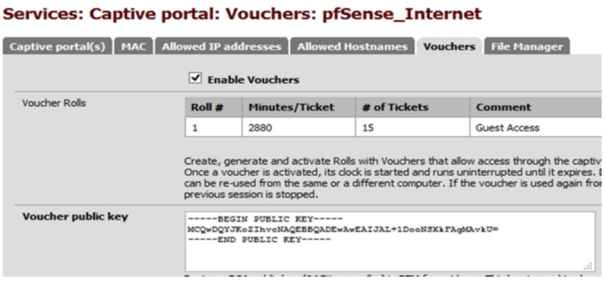

Fig. 7 Voucher Generation for Guest Access

3.4 Setting Policy and Security Mechanism

There are several policies that can be set when using pfSense Captive Portal. These include Bandwidth restrictions, User time limited, Pass-through, Allowed IP and Allowed Hostnames. pfSense also provides other features for securing the network (Miller, 2008). These features are:

(i) pfBlocker – This security mechanism is used to assign any IP or interfaces that we want to block or monitor both inbound and outbound.

(ii) Firewall Rules – This security mechanism is used to control what traffic is allowed to enter an interface on the firewall.

(iii) Firewalls Traffic Shaper - This is a mechanism for controlling computer network traffic in order to ensure performance, lower latency and increase usable bandwidth by delaying packets that meet certain criteria.

3.5 Adding Login and Error Page

The pfSense Captive Portal has default pages for login, login error and logout, but they look pretty awful. Fig. 8 is part of the Captive Portal configuration that allows the upload of a customized login page, error page, and logout page. Also Fig. 9 shows an embedded file manager in the Captive Portal where the upload of files like picture, cascaded style sheet (CSS), JavaScript (js), etc. are done. Every file uploaded in this location always automatically precedes with "captiveportal-" then follow by the file's name.

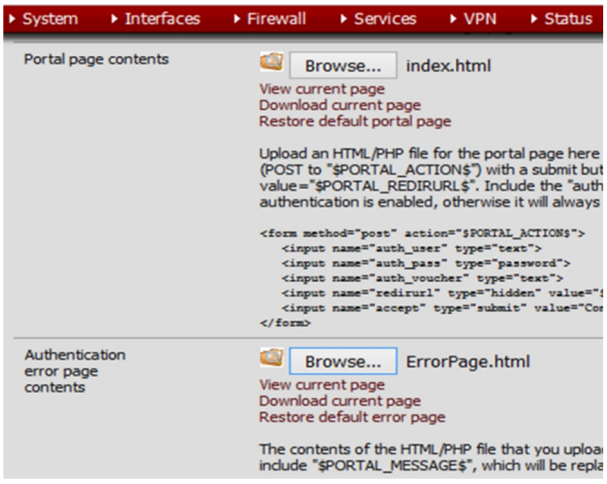

Fig. 8 Login and Authentication Error Pages

Fig. 9 Adding Files Needed for Login and Error Page

Before users have access to the internet, they are expected to launch a web browser and enter any URL of any HTTP site e.g. www.umat.edu.gh to authenticate themselves. Fig. 10 shows what a user has to do before he can be authorised to enjoy internet service.

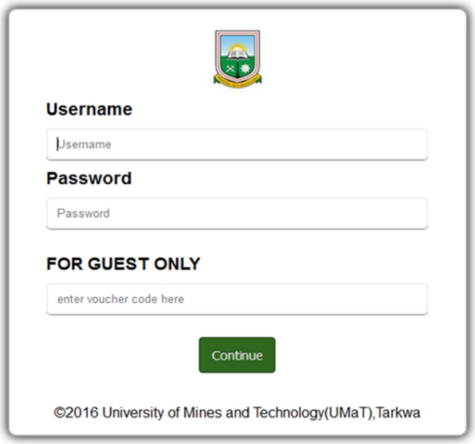

Fig. 10 Portal Login Page

If a user types in wrong credentials, he will be sent to an authentication error page as shown in Fig. 11. But with the right credentials, a user will be directed to the requested HTTP website. Fig. 12 shows the right HTTP page requested by the user.

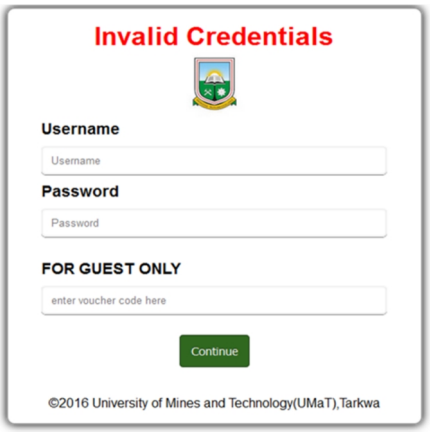

Fig. 11 Error Page Displayed

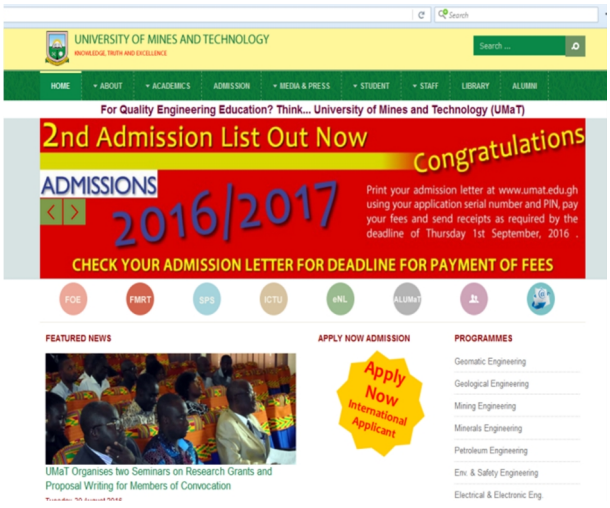

Fig. 12 Requested page has been displayed

4 Conclusion and Recommendation

Security is indeed essential when deploying a WLAN. This paper sort to find a simple way to incorporate already existing users in an AD to communicate with the Captive Portal instead of manually entering details into the pfSense local user account. The approach used by Mamat and Ruzana (2013) will be difficult for large organisations like UMaT with over 2000 user login credentials in AD.

The experiment conducted demonstrated how to achieve the configuration of pfSense Captive Portal and a local RADIUS server for authenticated users on a wireless network and secure their credentials. A user connected to the wireless network is assigned an IP address by the Dynamic Host Configuration Protocol in the pfSense and any web request from the user is redirected to the Captive Portal page. Only legitimate users with the correct login credentials are able to gain access to the internet. Once the user authenticates, Captive Portal stops redirecting the user's requests.

The RADIUS authentication method combined with Captive Portal technology was able to achieve the set objectives of this paper. Thus, there would not be any instance where the same credentials would be used by multiple users. Visitors have permission to access the internet using voucher ticket and credentials cannot be sniffed.

Hopefully, this paper could be useful for people who want to implement this technology to secure users on their institutional wireless network.

It is recommend that other packages like Apache with mod-security development available at pfSense package manager be integrated in the future to enhance the level of security at the OSI reference model layer 7 by protecting a range of attacks against web applications and also to allow for HTTP traffic monitoring, logging, and real-time analysis.

References

Anon., (2011), "Cisco" *www.linksysbycisco.com?EU?en?learningcenter/HowtoSecureYourNetwork* , Accessed: 27th February, 2016.

Appenzeller G., Roussopoulos M., Baker M., (1999), "User-Friendly Access Control for Public Network Ports" *IEEE INFOCOM'99. Eighteenth Annual Joint Conference*, Vol. 2, pp. 699-707.

Danen, V. (2009), "Tech Republic", *http://www.techrepublic.com/blog/linux-and-open-source/diy-pfsense-firewall-system-beats-others-for-features-reliability-and-security,* Accessed: 17th March, 2016.

Joanie W. (2010), "Network World", *www.networld.com/article/2214616/wireless/wpa2-vulnerablility-found.html*, Accessed: 16th February, 2016.

Mamat, K, Ruzana Mohamad Saad; "Home Wireless Network Security Using pfSense Captive Portal", *Proceedings of 8th International Conference on IT in Asia 2013 (CITA'13) {IEEE/SCOPUS/ISI},* Accessed: 12th April, 2016.

Miller, S. (2008), "Free Software Magazine", *www.freesoftwaremagazine.com/articles/configure_professional_firewall_using_pfsense* Accessed: 6th April, 2016

Radvan, S. (2010), *Wireless and mobile networking overview for Fedora Linux, Red Hat*, Vienna, edition 1.2.

Sean W. (2011), "pluralsight", *www.pluralsight.com/blog/it-ops/wireless-encryption-authentication,* Accessed: 11th February, 2016.

Soewito, B. (2014), Building secure wireless access point based on certificate authentication and firewall Captive Portal, EDP Sciences, Paris.

Stahie, S. (2014), "Softpedia", *http://news.softpedia. com/news/PfSense-2-1-1-Firewall-Distro-Can-Replace-Any-Commercial-Alternative-436111.shtml,* Accessed: 21st February, 2016.

Authors

Felix Larbi Aryeh is an Assistant Research Fellow at the Computer Science and Engineering Department of the University of Mines and Technlology. He holds a BSc in Statistics and Computer Science from the University of Ghana and an MSc in Information Technology from the Kwame Nkrumah University of Science and Technology. His research interest includes Wireless and Wired Network Security; Computer Graphics; and Web Applications and Internet Technologies.

Michael Asante is a Senior Lecturer at the Kwame Nkrumah University of Science and Technology KNUST. He holds PhD in System Enginerring with specilisation in Data Communications and Computer Networks from University of Reading, UK ., MSc in Scientific Computing and Information Technology from London South Bank University and Diploma in Mine Survey from University of Mines and Technology, Tarkwa in 1990. His reasearch interest includes Data Communication, Network, Computer Security.

Adrain Enos Yaw Danso is currently a National Service Personnel in the University of Mines and Technology. He holds a Bachelor degree (BSc) in Computer Science and Engineering from the University of Mines and Technology (UMaT), Tarkwa, Ghana.. His research interest is in Wireless network security.