

**BUGEMA UNIVERSITY**

**MAIN CAMPUS**

**SCHOOL OF COMPUTING AND INFORMATICS**

**ID BASED AUTHENTICATION TO WI**-**FI NETWORK**

**CASE STUDY: BUGEMA UNIVERSITY MAIN CAMPUS**

**BY**

**WOJA CLEMENT COSMAS SAMUEL**

**REG/No 20/BCN/BU/R/0005**

**AND**

**NAJJUMA JOAN**

**REG/NO 19/BCN/BU/R/0018**

**BPCT 3111 BPCT 311 IT PROJECT MANAGEMENT**

**Introduction**

Wireless Security

Wireless network security is the process of designing, implementing and ensuring security on a wireless computer network. It is a subset of network security that adds protection for a wireless computer network.

Wireless network security primarily protects a wireless network from unauthorized and malicious access attempts. Typically, wireless network security is delivered through wireless devices (usually a wireless router/switch) that encrypts and secures all wireless communication by default. Even if the wireless network security is compromised, the hacker is not able to view the content of the traffic/packet in transit. Moreover, wireless intrusion detection and prevention systems also enable protection of a wireless network by alerting the wireless network administrator in case of a security breach.

Wireless networks are complex; there are many technologies and protocols required to offer a stable wireless network to end users. It also sounds scary to transmit data through the air, where everyone can listen to it.

Wired networks feel secure; after all, you cannot easily listen to this traffic. You could connect to a switch port, but the only unicast traffic you will see is the traffic between your computer and the switch. You will see multicast and broadcast traffic from within the VLAN, though.

Anyone can see the data that travels through the air, which is why wireless security is so important. Someone can monitor wireless traffic, and you will not even notice that it is happening.

In the 802.11 service sets lesson, you learned how wireless clients associate with APs. All wireless traffic has to go through the AP, instead of directly between the sender and receiver. Anyone in range of the AP or other wireless clients can receive the signal. This can be a problem. For example, imagine we have a user who sends a password to a remote server; Wireless Attacker Captures Password

The wireless user transmits a password to the remote server. Because the attacker is in range of our wireless network, he can capture the password.

How can we securely transmit data through the air and ensure that it remains private and is not tampered with? The 802.11 standard offers security mechanisms that provide authentication, encryption, and integrity. I will give you an overview of these three items.

Authentication

To use a wireless network, the wireless client has to discover a BSS. APs advertise beacons with their SSID, and the wireless client selects the wireless network she wants to connect to and associates with the AP. By default, authentication is open, which means everyone is welcome.

Wireless ID base Authentication system.

You probably want to authenticate your wireless clients, though. If you have a corporate network, you do not want just anyone to join the network. Only legitimate users should be able to use your wireless network. After all, the wireless network might be connected to the wired network where you can access all corporate resources.

What if you have guest users? If you want to offer a guest wireless network, you should configure a second SSID, linked to a VLAN with restricted access.

APs can authenticate wireless clients before they associate with the AP. This keeps rogue clients away from our wireless network.

There are many options for wireless authentication. You are probably familiar with the most common choice, a pre-shared key. We configure the pre-shared key on the AP. Any wireless client that wants to join the wireless network has to enter the pre-shared key. Windows 10 Connect To Wireless Network

What happens when someone steals one of the wireless clients? That is a problem because of two main reasons:

The attacker has access to your pre-shared key and can now connect to the wireless network from any device.

You need to configure a new pre-shared key on the AP and all wireless clients.

There are stronger authentication options where we ask users for a username and password instead. This helps. When a device is stolen, at least you can pinpoint which username was compromised and reset the password for that username. You do not have to reset the pre-shared key and configure it on all wireless clients.

**Business case**

Bugema university main campus, with wireless network all over the school compound specifically for the student and any staff member living within the school compound. This is for the students to carry out their research. The non-students/the community members had access to the wireless network, the moment they were within the school premises because they had knowledge for the wireless network password shared with their friends who were in the school.8

**Problem**

Weak wireless network security, Their current technology used by the university was a password based mechanism which anyone who knows the password he/she can have access to the wireless network and which is not secure, because anyone can have access to it at any time. Due to the access of the network by the non-students/the community members, this has affected both the students and the staff members who lives within the school premises. The school wireless network became weak when a student trying to access, when a student was browsing flies in the computer or smartphone it loads too slow hence taking much time and bundles, this has hinder the development of the university.

**Proposed IT Solution**

As a networker, I would like to introduce ID based authentication security to improve on the wireless network of Bugema university main campus so that any student who is not registered will not access the wireless network. By ensuring that any student who wants to access the wireless network the system must ask for the credentials. This will prevent the community members/ non-students from accessing the wireless network.

**Specific Objective.**

Develop an ID based authentication security system.

**Aims of Objectives.**

It allows only users with the credentials to access the network resources.

Enables you to secure a network.

It improves on the speed of the wireless network.

It will reduce on the wastage of the bandwidth.

**Scope of the study**

**Subject scope.**

The study will mainly focus on the development of wireless network System with emphasis on reducing the weakness of wireless network of Bugema university main campus.

**Geographical scope**.

The study was carried out at Bugema University Main Campus

**Time scope.**

The study covered data in Bugema university main campus for the period of two weeks. However, the actual study was carried out in Septembers.

**Significance of the study.**

* It is expected that the wireless network will improve the quality, speediness and efficiency operation of the research in the school.
* It will enable effective and easy two-way communication between students and the staffs.
* The main objective of the study is to improve on the wireless network security by introducing ID based authentication
* This study will stop the community members/the non-student from accessing the school wireless network.
* The study help the researcher to have knowledge on the wireless network security.
* This study will replace the previous wireless network system by adding more security features to improve the wireless network system of Bugema University main campus.
* It will provide good performance in terms of speed and accuracy, because few category of registered students will be allowed to login the system.
* It will require less space and administrative resources and has the potential to detect the student’s credentials/information.
* It will provide integrated support for a wide range of the wireless network all over the school premises.
* This study will benefit the school since many students will be registered such that they are allowed to access the wireless network of the school.

**RESEARCH METHODOLOGY**

**Introduction.**

This chapter focused on methodologies that were used to carry out the study that included data collection techniques, design and investigations.

The methodology that were used for planning, creating, testing and deploying system or software is called the application development life cycle. It is a process of splitting the software development work into different phases with the aim to better plan and manage the whole task. The procedure and incremental development methodology was used for the development of system. With this methodology, the system is developed through repeated cycles (hence iterative) and in smaller portions at a time (hence incremental). This allows the software developer to take advantage of what was learned during the development of earlier parts or versions of the system. The development is started with a basic implementation of the system, and then, iteratively, new features and functionalities are added and design modifications are made, as needed.

**Research design.**

Research design is the framework for the collection and analysis of data. It is also known as the conceptual structure within which research is conducted (Ryman, 2008).

Case study was the research design used in this study. Case study is instrumental and focuses on a particular phenomenon or theory (Pickard, 2007).

In this case, the researcher looked at ID based authentication system in Bugema university main campus hence to improve the wireless network security of the school.

This involved analyzing the existing phenomenon system as well as the proposed system to be implemented, conceptualization of the new system navigation and data flow.

The design phase consists of planning, creating specifications, conceptualizing and framing the material and production of content, preparing the storyboard, layout design and user interface.

**Study Population.**

Population refers to group of individuals, persons, objects or items from which samples are taken for measurements (Bryman, 2008)

Administration the students and staff were the target population since they are the daily user’s often system. It helped to collect accurate data.

**Sampling.**

Sample size is a finite part of a statistical population whose properties are studied to gain information about the whole selected from a larger population for the purpose of survey (Bryman, 2008).

Sample size was provided basing on the respondents in the interview guide.

The sampling technique used is purposive which helped to conduct the study and acquire knowledge about the user needs in the system. With this strategy, the researcher focused on the students ID based authentication system about the current system they use. In this strategy, the researcher also collected data of the students.

**Sources of Data.**

Data will be got from both primary and secondary sources. Primary data will be got from interviews, sampling and observations while secondary data will be got from already published books and internet.

Primary data. Refers to raw facts that have been collected from the field and not yet processed like population census.

Secondary data. Refers to the already processed data into information like magazines, journals among others. All these types of data will be used for establishing the requirements for developing ID based authentication system.

**Data collection methods.**

These different techniques were used for data collection. .

Surveys of respondents were carried out using questioning and interviewing and the respondents were students and staffs.

In data collection, various methods were used to collect data which included; interview, Surveys, document analysis

I used the following methods during data collection: Observation, Interviewing and Surveys as my research method. Through this, I was able to collect raw data in Bugema university main campus these where the existing reports on the current system.

**Data Collection Methods and Instruments.**

Data collection refers to the process of using some methods (Interview, questionnaire, Surveys, observation) to collect data (Powell, 2004).

Instrument refers to a tool that can be used to collect data for example; questionnaire, Surveys, interview guide (Powell, 2004).

The following are the data collection methods and their respective instruments, which was used.

Interview.

An interview is a conversation or dialogue with a purpose between two people. It involved asking questions and getting answers from participants in the study. Interview helped to give accurate information on the current system used and enable the researcher get results.

The interview guide is the instrument that the researcher used to obtain information from the school staffs. The researcher interviewed the network administrator, students and the administrative staff since they are the ones with relevant information mostly about who the system user are, current network system used by students and challenges encountered by both administration and the staff when using the system.

Observation.

I went to Bugema university main campus and observed their daily work in regards to the current network mechanism system that they are using and they were using password-based mechanism as specified by the Network administrator, and some of the staff from other departments.

**Questionnaire.**

Questionnaire refers to the type of data collected where the researcher sets questions to be answered by the respondent. It is both structured and unstructured. It will be used to set questions, collect information from the staff, students and the network administrator. It is referred to as a data collection tool in which there are written questions to be answered and presented to the respondents in written or typed form (Chalcunvong, 2009).

The instrument used was the questionnaire.

Document Reviewing.

This refers to the analysis of documents that contain information about the public, with this method of data collection, the researcher reviewed a number of statistical books and articles about automation, wireless network ID based authentication system. Such documents provided primary and secondary data that helped the researcher get information on how to design the ID based authentication system.

**Data Quality Control.**

Data quality refer to a set of procedures intended to ensure that information produced adheres a defined set of quality criteria or meets the requirements of customer or client(Kcthari,2012).

Data quality control was done to check the validity and reliability of the instrument by carrying out preliminary tests on the interview guide and questionnaire.

**Data Analysis and Presentation**

Data analysis refers to a process of working with data to describe, discuss, interpret, evaluate and explain data in terms of the research questions or hypothesis of the research project (Matthew, 2010).the data was quantitatively analyzed, all data collected was edited to check for its completeness and accuracy data was analyzed to establish the percentage and frequencies Data presentation is defined as presenting the findings which available to the interested parties (Mugenda, 2003) Data was collected, analyzed and tabulated. This helped to check the accuracy, completeness, comprehensibility and legibility of the answers that were given and editing was done before tabulation.

**Examine Existing Documents.**

The researcher reviewed the past different records of wireless network security in order to analyze the problematic areas highlighted. These records generated the overall structure of the past wireless network system.

**Requirements Specification.**

This involves focusing on the information that ID based authentication is expected to generate and the constraints that the system face during its operations and implementation. The functional, nonfunctional, user and the system requirements needed for the system development and implementation are highly defined.

**User requirements.**

This included defining what the users wanted from the wireless Network ID based authentication system. The researcher interacted with users who identified and analyzed the end user requests and needs

The researcher identified end user needs and achieved them by ensuring that there are;

* An error free system.
* Educate Students.
* Immediate access to information.
* Easy Connection to the wireless Network.
* Feedback to the system.
* Registered students are allowed.
* Provide guidance.
* User-friendly interfaces.
* Multiple sharing of information.

**System Requirements.**

System requirements addressed more detailed specifications of the users, which were used to design the ID based authentication wireless network system and define hardware and software requirements for the system to fully function efficiently. The system produced graphical user interfaces, and hardware and software specifications.

These described the kind of services the system provided, how the system reacted to particular inputs, and how it behaved in different situations.

By use of a questionnaire as one of the means of data collection technique, which was presented to the Network administrator, was able to identify authorized users of the system.

Searching for information concerning the existing system is simplified by the system

**Non-Functional Requirements.**

This involved defining the User accounts with their respective ID to the system, which prohibited access by non-authorized users. This eventually helped to define the responsible chosen users who were able to allow updating information in the system. The system is scalable to enable updates and easy to use.

With successful orientation, users of the system got the basics

**Software Requirements.**

Various users of the system will be consulted for different software requirements, which will facilitate the efficient operation of the system. For instance, Micro soft office 2007 version, Microsoft windows XP professional as a window of operating system, is programming languages like Visual basic among others. The purpose of the above-mentioned software has included the following;

1. Operating System: Microsoft XP OS Service Pack 2 windows Vista Windows 7, 8,10 and 11
2. Software Development Language Include:

* PHP
* HTML
* CSS
* JAVASCRIPT
* J QUERY
* AJOX
* Bootstrap

1. MYSQL as the database’s backend was used.

Microsoft XP professional acted as an operating system upon which the inventory system resided for it to run efficiently

Microsoft office version 2007 provided the access package on which the inventory system is to be built to meet the ender user needs.

Visual basic built within Microsoft office 2007 version enabled the researcher to design a coded system that prompted login and logout facilities, search for various records and integrate the system as a single module. This was be achieved by integrating the inventory system with Vb.net (visual basic net)

**Hardware Requirements.**

* + - * Using the necessary requirements like processor with a minimum system requirement of Intel Pentium, cycle speeds of 2GB RAM, band width of 50mbs and disk space of 80GB minimum, Processor: Intel Dual Core 2.0 GHz or higher.
      * Memory: 4GB DDR3, Disk Storage: 500 GB, Drive: CD/DVD-RW 60X, Video Card: 2GB GeForce VC (Optional), USB Slot: USB Port 2.0 for an efficient inventory management system to be obtained.

**Current system.**

Bugema university main campus is using a password based authentication since the security of the wireless network is weak the researcher has come up with an idea of improving the wireless network security.

**Proposed system.**

This section describes the functions and operations of the system in details. It transformed the detailed requirements into complete detailed systems focusing on how to deliver the required functionality. The study adopted a structured approach, which involved the use of entity relationship diagram basing on the identified entities for the system.

Functionalities.

The student credentials will be captured by the system right from the time of registration this to identify the student.

When a student is logging in to access the wireless network, the system will ask for the student’s ID number before he is allowed in to access the wireless network.

The ID based authentication wireless network system needs authorization; if you are not authorized student, there will be no way for you to access the wireless network.

**Ethical Considerations/issues.**

This helped to conduct the study in a systematic way, honesty and integrity throughout the process and the respect of confidentiality of the respondents.

**Limitations of the Study.**

The researcher encountered the following limitations;

Financial problem. The study needed a lot of money for many functions for example printing travelling to the field, feeding hence a limitation.

Attitude of the respondents was another problem in that some respondents reluctant to give adequate information hence time wasting

Time management. Time allocated to the researcher was not enough to gather information from the field and interpret it. However, the researcher tried the level best to do work basing on the work plan.