A Serial Number Based Identification Model for a Computer in a Wireless Local Area Network

Joseph Chebor
Kabarak University

Abstract:

With today's technological evolution, wireless networks have become very common for organizations, homes and public places. For any device to be authenticated and authorized to use any of the wireless network services, it must first be identified then authenticated and authorized to have access to the wireless network resources. One of the biggest challenges with implementing wireless networks, though, is implementing the identification of the wireless devices. Apart from port numbers and IP addresses at application and network layers respectively, devices in a network use MAC addresses for identification at the physical layer. However MAC addresses can be altered thereby compromising the security, robustness and uniqueness qualities of a device identifier. This study therefore examined the inbuilt access and use of a serial number prototype system as an alternative method of identifying devices in a network. The model was constructed using evolutionary prototyping and proof of concept methods through test runs and was found to actually identify a device in a network based on a computer's serial number. It is then recommended that prototype be scaled up then adopted as network device identification method

Key Words: Computer, Serial Number-Based Identification, Wireless Local Area Network

1. Introduction

Wireless LANs (WLAN) also known as Wireless Fidelity (WiFi) or 802.11 standard is a type of a local area network that allows users access network services using mobile devices (wireless stations) such as laptops, personal digital assistance and even smart phones. The wireless stations use a base station usually an access point (AP) as an entry point to the network services. Unlike wired LANs, WLANs uses radio wave frequencies to transmit information over the local area network.

According to Mohapatra *et al*. 2014, currently most deployed WiFi technologies include Tri-band WiFi or WiGig or IEE802.11ad, Light Fi (LiFi), Advanced Enterprise WiFi, WiFi CERTIFIED™ AC and Wi-Fi CERTIFIED Passpoint™ in the order of their technological advancement. Something common about all these technologies is in the improvements of speed of transmission in each subsequent technology. In addition to speed improvement, Advanced Enterprise WiFi allows users log in to a WiFi network using their social credentials. Wi-Fi CERTIFIED Passpoint™ ultimately allows online-sign up for mobile devices without a SIMM card.

WLAN come with a number of benefits as compared to wired LANs, notably mobility, rapid deployment, reduction in infrastructure and operational cost, flexibility and scalability (Idris & Kassim, 2010; Mandy, 2002; Nicopolitidis *et al*, 2001). Due to these benefits hotpots are now virtually found everywhere; in enterprises, at homes and in public places. Wireless devices come with WiFi features integrated in them. Despite the numerous benefits that come with wireless

LANs, network insecurity has become a thorn in the flesh for proprietors of such kind of networks. Frankel *et al*. (2007) points out that an attacker simply needs to be within the range of the WLAN access point to intrude into the network as opposed to wired LANs where an attacker requires physical access to the LAN or remotely use porous firewall systems to gain access to the LAN. WLANs are therefore easily targeted by attackers through spoofing, denial of service, eavesdropping, man-in-the-middle, masquerading, message modification, message replay and traffic analysis (Vollbrecht & Moskowitz, 2002; Idris & Kassim, 2010; Stallings, 2011). Mandy, 2002 describes the reasons for the threats as default configurations, network architecture, encryption weaknesses, and physical security.

Identification, authentication and authorization as identified by Bruhn *et al*. (2003), are essential functions in providing the required services in a network. The essential network services as suggested by Frankel *et al*. (2007) are confidentiality, integrity, availability and access control. The most common authentication and authorization techniques that are currently applied as a security measure in wireless LANs include WEP, WPA, WPA2 and RADIUS together with usernames and passwords.

Yet for authentication and authorization to take place, devices in a network must first be identified. According to Takahashi *et al*. (2010), devices in a network can only be explicitly identified by their port numbers, IP address or MAC address. Whereas MAC addresses are used by messages to identify actual physical destination and source network addresses, IP addresses are used by information to be effectively routed from network to network in an internetwork. On the other hand, port numbers are used specifically to identify processes running on sending and receiving stations (Kurose & Ross, 2006).

Problem Statement

Normally, every product (including a computer) or a thing of concern to an institution has an identifier to identify the product uniquely. In normal circumstances, hosts are identified by either a MAC Address or an IP address. Takahashi *et al*. (2010), refers to such identifiers as explicit or indirect identifiers because the identifiers are actually not meant to identify the devices rather they identify processes running in the devices and location of the devices. As such, whereas MAC addresses are used by messages to identify actual physical destination and source networks, IP addresses are used by information to be effectively routed from network to network in an internetwork. On the other hand, port numbers are used specifically to identify processes running on sending and receiving stations (Kurose & Ross, 2006).

In particular, a MAC address at the physical layer is usually hard coded or 'burned' into the network hardware therefore it is difficult to alter it. However copy of the MAC address in the operating system can easily be modified by an attacker to suit the valid MAC addresses spoofed.

If devices in a network cannot be correctly identified, then it can go a long way in contributing to security flaws in as far as authentication and authorization is concerned. It is for this reason then that the study seeks to investigate how a serial number may be used for physical identification of devices in a wireless LAN

Research Objectives

The main aim of the study was to investigate how a serial number may be used for physical identification of a computer in a wireless LAN. The specific objectives are:

1. To analyse the suitability of network device identifiers that are currently in use

2. To develop an algorithm that can obtain a remote computer's serial number in a wireless LAN
3. To Design a model that uses a computer's serial number to identify the computer in a wireless LAN
4. To implement the prototype that uses a computer's serial number to identify the computer in a wireless LAN

Related Work

An identifier, according to Hoffer *et al.* (2009), is an attribute (or a combination of attributes) whose value distinguishes instances of an entity type (device) from another. Coulouris *et al.* (2005) further cites examples of identifiers as could be a code (identification number, serial number, ISBN) name (domain name) or an address (IP, MAC or Port Number). Clark, 2003 cites port numbers, IP addresses and MAC addresses as the most commonly used identifiers or what is referred to as service access point identifiers (SAPIs) for network address and hardware addresses.

An attribute should possess uniqueness, universality, collectability, security, data dependence, robustness and mnemonic (Danev *et al*. 2015, Leo, 2004 and Bolle *et al*. 2003) qualities to be a good identifier. Whereas uniqueness ensures that no two devices have the identifier, universality ensures that devices in the same space have an identifier, collectability is the ability of an identifier to be captured from existing systems, security ensures availability, integrity and confidentiality of an identifier, data dependence is the ability of an identifier to be associated with other device attributes, robustness or reliability or permanence is the ability of an identifier not to vary with time and mnemonic defines a standard and meaningful structure of the identifier.

Port numbers are numbers on hosts/devices that identify sending and receiving processes. According to Lee, 2010, port numbers are usually captured when a system requests for a page with usernames and password details. Process identification in communication is crucial because a host could be running several applications. Although port numbers can be used in conjunction with other numbers, namely, IP address and MAC address to identify a host, port numbers can pause as threat to network security. Intruders can use a port scanner that listens to well-known port numbers so as to detect services running on a system, therefore can easily break into the system (Canvan, 2000).

An IP address is number assigned to a host or a router in the internet for identification and location of the device as stated by Tanenbaum, 2003. An IPv4, which is currently in use (Kurose & Ross, 2006), is composed of four dotted decimal notation (example 243.246.0.28) each part range between 0 and 255. Depending on the class or the subnet mask of the IP address, some parts (first) belong to network identification and the other parts (usually from the second part) belong to host identification. IPv4 was designed to use 32-bit address space (Shay, 2004). This translates to 2^{32} or approximately four (4) billion addresses which is not sufficient for the global needs. Actually, the numbers were projected to have been exhausted by 2013 (IEEE-USA, 2009). A temporary solution of conserving IP address used by network administrators in apart from organizational LANs, has also found use in residential and wireless LANs, is the use of DHCP (Kurose & Ross, 2006). DHCP assigns devices IP addresses on demand, therefore two devices can use the same IP address but on different occasions.

MAC address also known as LAN address or a physical address is a number used to identify a network adaptor on a LAN. As Kurose & Ross, 2006 puts it "it is not hosts and routers that have link-layer addresses but rather their adapters (that is, network interfaces) that have link-layer addresses." In other words a MAC address is used not by devices but by information to identify a particular physical network like an Ethernet network. A device with multiple interfaces has multiple corresponding MAC addresses. Kurose & Ross, 2006 further puts it that the management of MAC address space is the prerogative of IEEE internet standard. This then implies that different adaptors from different manufacturing companies cannot have the same MAC address. Furthermore, the possibility of a MAC address being spoofed renders it not unique, variant and therefore unreliable.

Identification is the process of association an object or an individual with an identity (Jain *et al.* 2000), thus establishing the identity of the entity. Identification answers the question that concerns who or what the entity is. It's a means of series of identification that the identity of an entity is constituted and specified. Luis-Garcia et al. 2004, sites examples of identification strategies as could be something known to the entity such as password or a personal identification number (PIN) or something owned by the entity such as a card, a token or a key. From the time of the use of identification friend or foe (IFF) during the Second World War, (Lehtonen et al, 2008), identification technologies advances such as barcode readers, optical character recognition (OCR), biometric identification system (BIS) and radio frequency identification (RFD) took effect.

Methodology

The study adopted a proof of concept (PoC) evolutionary prototyping approach to proof that a serial number can be used to identify a computer in a WLAN. Apart from proofing the functionality of the system (Yang and Epstein, 2005), evolutionary prototyping is used when an initial version of a system is developed using the best known and highly prioritized requirements. The method involved (1) Development of the abstract requirements specifications, (2) Building of the prototype system, (3) Evaluation and testing of the prototype system and (4) Documenting and delivering the prototype. The figure 1 below summarizes the research design procedure.

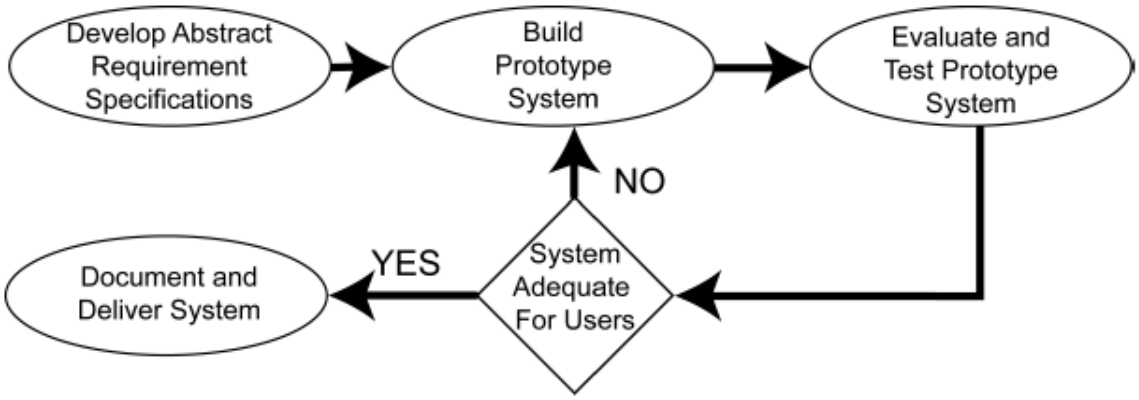

Figure 1: Research design (Source: AlWahhab, 2014)

Despite the fact that the prototype was based on a client-server architectural design, the prototype was developed to run on the server. The components of the prototype were the serial

number collection module, the computer identification details processing module and the identification details display module.

The identification details collection module is code on the server that loads the computer name, IP address and serial number of client when logged on to a network. The loaded details are then processed in the identification details processing module the displayed on connected device interface using the identification details display module running at the server as well. Java development kit (JDK) NetBeans was used for creating and implementing the computer identification interface and in the construction of the prototype modules. The identification details were be managed using MySQL database on the authentication server.

Eventually evaluation and testing of the prototype was basically based on whether a serial number of logged computer can be collected and displayed on an interface using different access points.

Results

The key findings from the literature review indicated that between port numbers, IP addresses and MAC addresses, devices in a network use MAC address as an identifier at the physical layer. The initial encoding of a MAC address in the network hardware is to make it independent from the operating system supposedly rendering it permanent and hard to alter (Cardenas, 2003). But due to some valid reasons (testing out networks for configurations, security applications or new protocols, workarounds and nefarious means), a copy of the MAC dress in the operating system can be altered. For whichever reasons in changing a MAC address, it leads to the conclusion that a MAC address is not unique, not secure, not permanent and therefore unreliable. It is for these reasons then that the study was carried out with an aim of investing to how serial numbers may be used for physical identification of computers in a wireless LAN.

Although computers have their serial numbers is tagged on them as part of serialization of the product, modern laptop models have their serial numbers coded into their basic input output (BIOS) chips. This makes it possible for the identifier to inwardly be accessed using a program so that it can be processed for a given desired function

The Serial Number Based Identification (SNID) System

For a serial number to be collected from the system then displayed for purpose of identification, the database that contains the identification details has to be started first. This then is followed by establishing a connection to the database, then the existing details have to be deleted to pave way for the newly connected computers, prepare database for new records, fetch identification details of connected computers, post the details to the database, retrieve and display the details on an interface for identification, in that order as illustrated in the algorithm below.

1. Start the database
2. Connect to the database
3. Delete existing records to pave way for the newly connected device records
4. Prepare the interface for the new records
5. Get connected computer details
   - 5.1 Get computer name
   - 5.2 Get computer raw IP address
   - 5.3 Get computer serial number

6. Process computer serial number
7. Post Connected Computer Details to the Database
8. Retrieve and Display the Connected Computer Details from Database

The nature of these tasks prompted the employment of divide and conger algorithm design technique to simplify the design and deployment of the problem. In a nutshell, divide and conger algorithm design paradigm enables a problem to be divided smaller, more easily solvable sub problems, solve and combine the problems into the overall solution (Skiena, 2008).

This way, the problem was firstly divided into the application part and the database part. The application section used a code that was able to collect the computers name the then computers IP address which was used to fetch and process the computer's serial number. For the serial number to be displayed for identification purposes, the database had to be started, connected then prepared for newly logged on device details to be captured and managed. The illustration in the figure 2 below show how the divide and conquer algorithm was employed

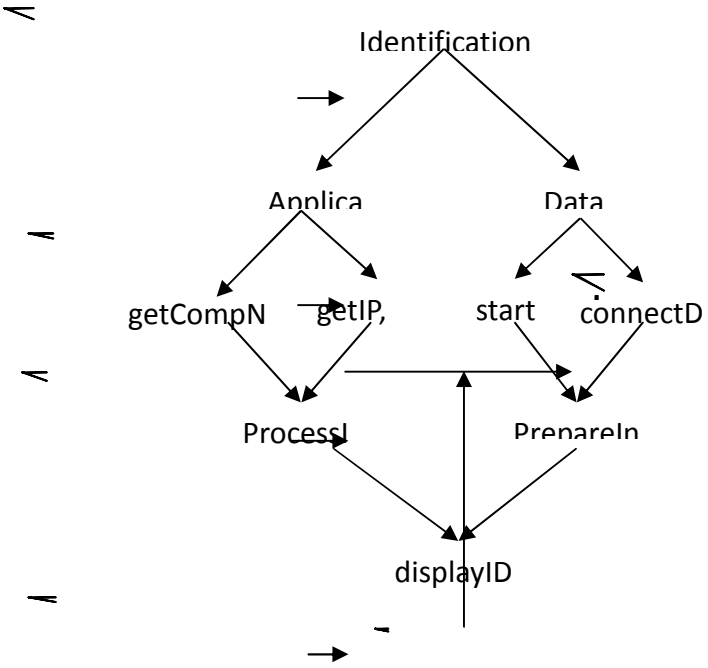

Figure 2: Application of divide and conquer method structure to SNID

The Generic Serial Number Based Identification System Model

The generalized model for identifying computers based on the serial numbers comprise the Data storage, database initialization, data collection, and data processing and data display modules.

Whereas the storage subsystem contains the structure that facilitates the storage and access of IP address, computer name and serial number details, initialization module involves database connection, deleting of existing records and preparing the database for new records. The responsibility of the data collection module is to fetch the IP address, computer name and serial number details necessary of computer identification process. The IP address, computer and serial number details are both from the local host computer and other computers connected to the network.As a part of the other subsystems, the serial number processing system can be said to be

the pivot or the engine of the SNID system. It is at this section that the DNS resolves the host names and IP addresses, then performs IP address format conversions and ultimately uses the IP address to the get the serial number of the corresponding computer. The ultimate detail for identification is the serial number record. But for the number to be used as an identifier, then it must be displayed on an interface. The display subsystem is designed therefore to access apart from serial number, the hostname and IP address details that are essential for device identification. All these are illustrated in the figure 3 below

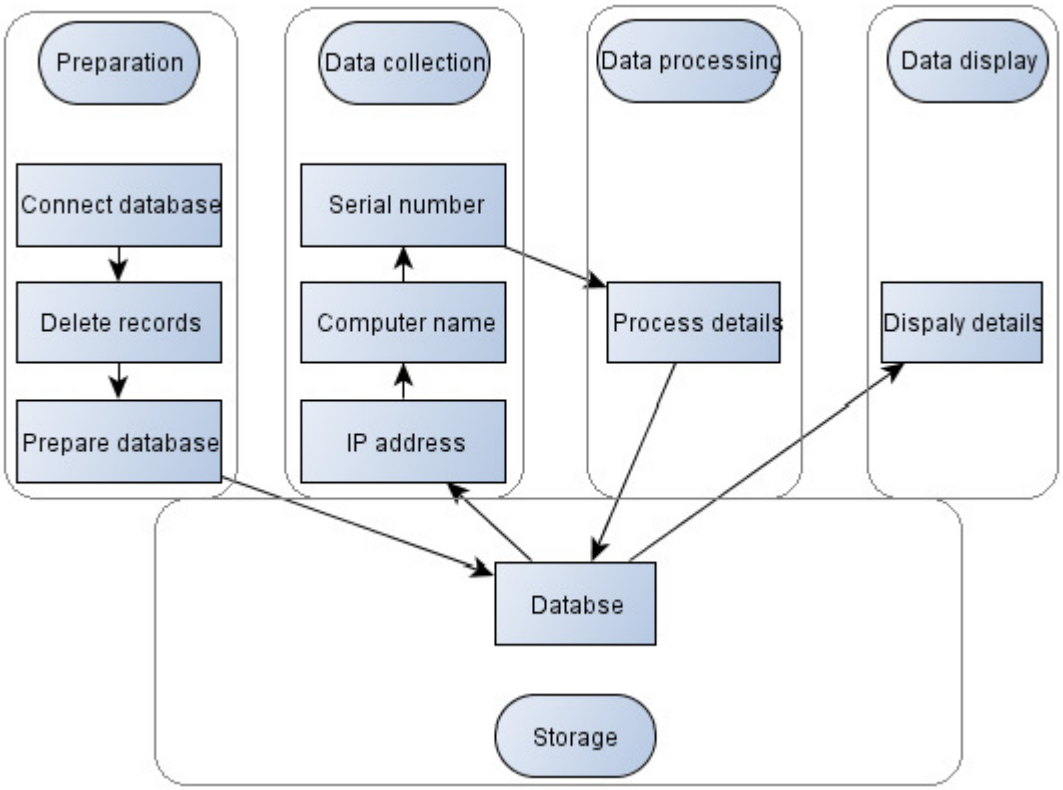

Figure 3: General model for a serial number based identification system

The SNID System Design and Implementation

Processing of the computers serial number is the core component of this study. The system relies on the computers IP address to get the serial number. All these are circumvented in a Java network programming class called the inetAddress. This class is used with other networking java classes to manipulate the computer's hostnames and IP addresses (Harold, 2013).

In this section, the function getCompName() was created to processes the serial number basing on the hostname and IP address of both the local and remote hosts. The class is enabled to throw an UnknownHostException error if an address is not found. The code running on the DNS then starts by connecting to the DNS to resolve local host name from the IP address. This is followed a variable creation for the IP address assignment. After representing the IP address in a byte format, the code gets the local IP address, the connected computer IP addresses, the connected computers serial numbers then posts the details to a database. All these is illustrated in the algorithm and corresponding flow chart below

1. Start
2. Resolve local host name and IP address
3. Assign the IP address a variable
4. For IP address between 70 and 254
   - 4.1 Set byte representation from string representation of the IP address
   - 4.2 Get local IP address
   - 4.3 Get connected computers IP address
   - 4.4 If the address is reachable, then
     - 4.4.1 Set Computer name
     - 4.4.2 Get computer serial number
     - 4.4.3 Post IP address, Computer Name an d serial number to a dataset
5. Else end
6. End

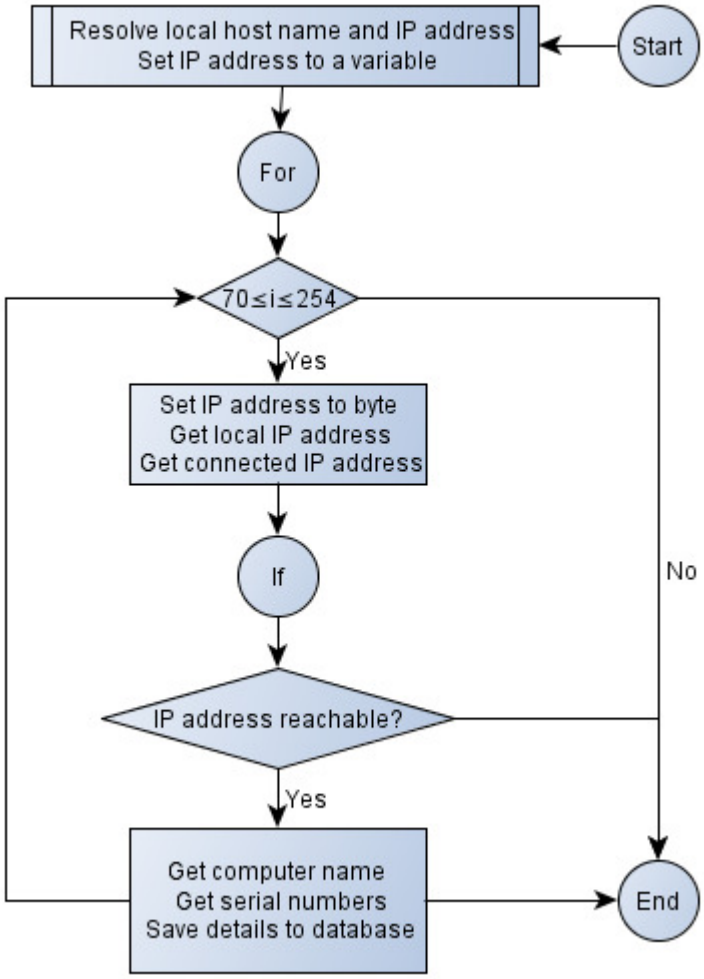

Figure 4: Processing of the computer's serial number chart

The corresponding code is as follows:

```
public void getCompName() throws UnknownHostException {
    InetAddress localhost = InetAddress.getLocalHost();
```

```
        byte[] ip = localhost.getAddress();
        for (int i = 70; i <= 254; i++) {
            try {
                ip[3] = (byte) i;
                InetAddress address = InetAddress.getByAddress(ip);//local ip address(server ip)
                ipoutput = address.toString().substring(1);//get the computer ipaddress
                if (address.isReachable(500)) {
                    Computer_Name = address.getCanonicalHostName();
                    getSerial();
                    System.out.println("COMPUTER NAME: " + Computer_Name);
                    System.out.println("COMPUTER IP: " + ipoutput);
String sqlins = "INSERT INTO condevices
(IpAddress,Computer_Name,Serial_Number)values('" + ipoutput + "','" + Computer_Name +
"','" + serial + "')";
                    pst = con.prepareStatement(sqlins);
                    pst.execute();
                    String sql1 = "SELECT IpAddress,Computer_Name,Serial_Number FROM
condevices";
                    PreparedStatement pst1 = con.prepareStatement(sql1);
                    ResultSet rs1 = pst1.executeQuery();
TblConnectedDevices.setModel(DbUtils.resultSetToTableModel(rs1));
                }
            } catch (Exception er) {
            }
        }
       (rs1));
```

Eventually the identification details are displayed in an interface as in the figure below

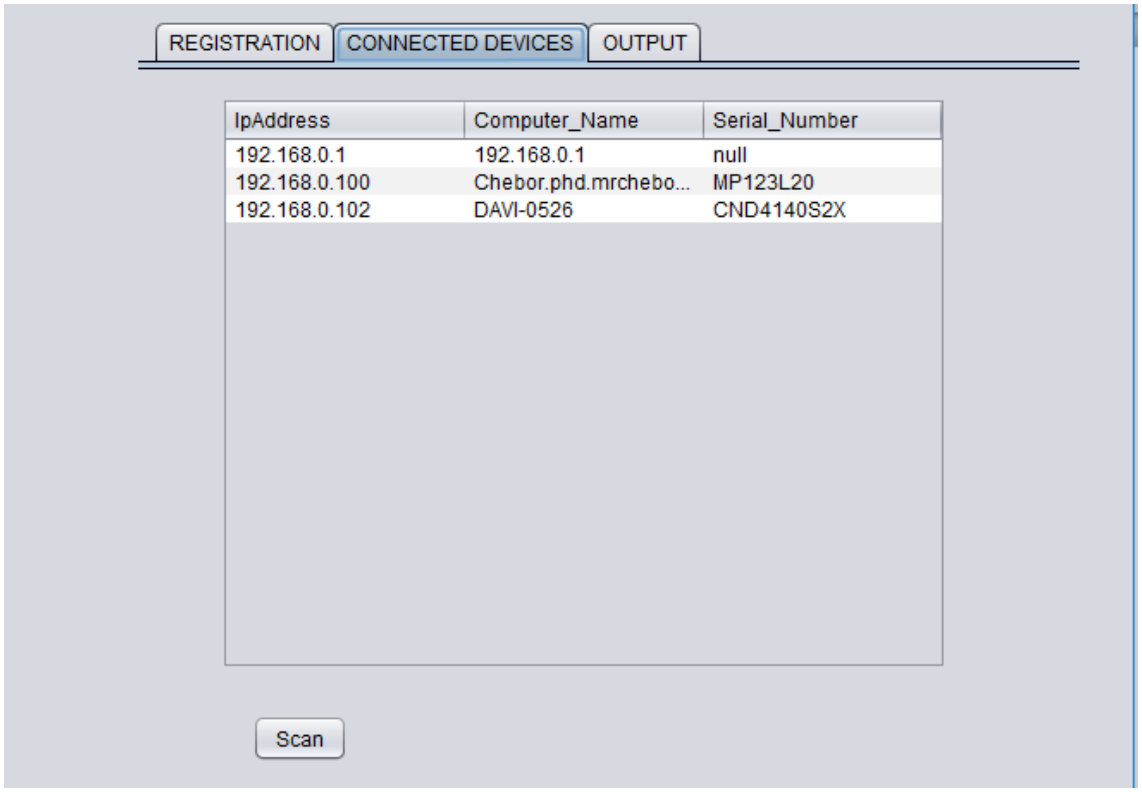

Figure 5: Identification details interface

Research Contributions

This method should not be used as a replacement for device identifiers but primary as an alternative method to MAC address in device identification. It can actually added to the existing MAC address at data link, IP address at the network, and port number at the transport OSI reference layer model of identification especially at the physical layer

Alternative Identification Method

SNID can go a long way in providing alternative identification method to MAC address at the physical TCP/IP reference model layer. As an identifier, a serial number is unique, robust and more secure than a MAC address therefore providing a better alternative device identifier to network devices.

Additional Identification Layer

A notable contribution of the study to research is on the additional layer to existing network device identifiers. The identifiers identified earlier on are an IP address, MAC address and port number. Of course the identifiers are implicit as they are primarily used to identify devices indirectly through their locations rather the actual device.

Due to it's in process communication identification, port number identifiers are transport layer of OSI reference model. IP address identifier, of course, is a network issue as far as OSI layer model is concerned because it identifies devices in the internet. MAC addresses on the other hand identify devices in a particular network, therefore placed at data link layer of the same model.

A serial number is hard coded onto the system board BIOS of a computer by the products manufacturer. Its association with the pure hardware makes it be a physical layer issue in the OSI reference model. In this case, the serial number becomes an additional not only as a mere identifier to the existing port numbers, IP address and MAC address identifiers but more so as an actual identifier to the product (computer).

Modern computer networks are full of complexities as a result of the internet exponential growth (Behringer, 2009). A particular concern is the tremendous growth of computer hardware capacities, software sizes and so their configurations. One way of simplifying this complexity is by layering although it comes with an overhead. This way functions are devolved to each layer relieving other layers some other additional responsibilities that would have otherwise performed.

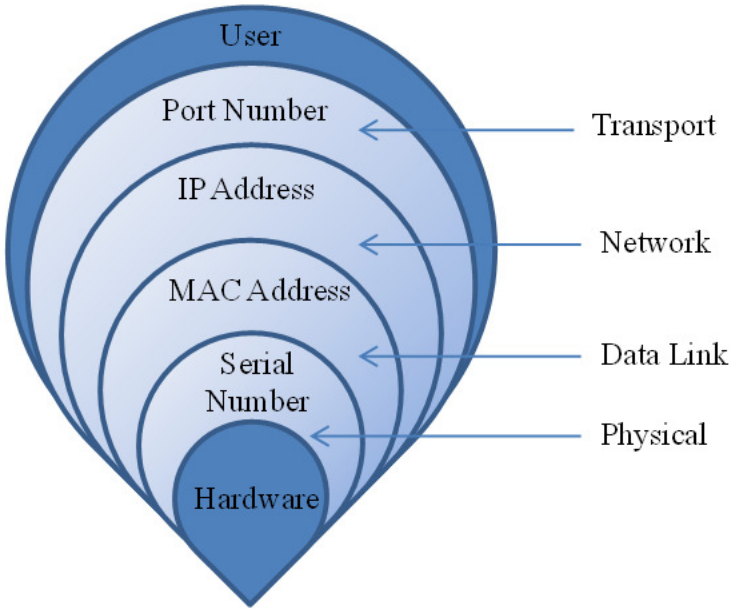

Figure 6: Device identifiers layering

Recommendations

The following three recommendations are proposed

Improvement and Deployment of SNID

The ultimate goal of the study was to demonstrate that a computer's serial number could be used for identification. The prototype was therefore developed with the emphasis on test runs to prove this concept. No much regard was considered for the usability and actual implementation design of the system in an ideal environment. It is with this regard therefore that the system is recommended to undergo through GUI enhancement, user acceptability testing process and eventually deployment of the system

Development of a System that Caters for other Network Device Identifiers

Laptops and computers in general like any other products are serialized for product differentiation. Other wireless network devices such tablets and smart phones use IMEIs rather serial numbers for identification. The study therefore focused on laptops to argue its case that a serial number can be used for identification. Development of an overall model/system that caters for the varieties of identifiers whether it is a serial number or an IMEI or any other related identifier is recommended

Integrating of SNID into an Access Point

The SNID system for the sake of the study was implemented in a server. But due to the functions and nature of servers, it is recommended that the SNID be implemented in an AP. In most cases DNS resolve domain names and IP addresses. In addition, there could be a number of servers communicating through the same AP that might require the SNID system. Access points (AP) on the other hand is an ideal home to SNID. Apart from an AP being the entry point to all devices connecting to the network it also acts as good security control in what is commonly referred to as identification, authentication, authorization and accounting (IAAA).

Areas for Further Research

Using a serial number for identification in isolation is not good enough. But if it results to authentication, authorization and accounting in that order then its mission will be accomplished. Actually, identification, authentication, authorization and accounting (IAAA) are essential in providing the network services required. Therefore, to accomplish the mission of network service provision, the following areas for further research are forwarded:

Using a Serial Number for Network Authentication

The serial number used to identify a network device can as well be used to authenticate the device. Authentication simply establishes of the validly of a logged on device. This can be achieved by creating a look up system that validates a device when logged on.

Using a Serial Number for Network Authorization

The reliability of a serial number puts it in a better position to be used as field to authorize devices to a network. Furthermore, its ability to carry with it aliases like computer name makes it easier to identify who the responsibility of the device lies on therefore authorized to access the appropriate network services. To achieve this, a study on a system that allows/disallows access network services depending on who the user is at authentication stage is proposed.

Using a Serial Number for Network Accounting

The serial number based identification will not be complete without the accounting component of network services provision. Accounting or auditing traces the device actions right from identification, authentication and authorization as well as track the activities performed. Once again a serial due to its reliability can be used as base for accounting.

Conclusions

The mere fact that MAC address can be spoofed and altered affects robustness and uniqueness attributes of a MAC address. Uniqueness factor is more compounded due the possibility of multiple network interfaces attached to a computer results to multiple MAC address for the same computer thus compromising the uniqueness quality of a MAC address as an identifier. Basing on the study objective on whether existing network device identifiers (MAC address) is suitable for network device identification, it can be concluded then that MAC address is not suitable for network device identification.

The study that was carried out with an aim of investigating how a serial number could be used to identify a computer in a WLAN revealed that a serial number can actually be used to identify a computer in a wireless LAN by displaying the identification details on an interface. For the identification details to be displayed then the database has to be created, started, connected and details interface created in that order. At the same time codes to get computer name, get IP address and eventually get and process the computer's serial number had to be developed. The processes were made possible by employing divide and conquer algorithm design

First, the overall system was divided into two sections: the application and the database parts. The application section was further divided into get computer name and IP address that resulted to getting and processing of the computers serial number. On the other hand the

database was split into starting and connecting the database followed by preparing the interface to accept the identification details. Finally the identification details are displayed on the created identification details interface.

To better understand the system as well ensure the inclusion of all possible system components, SNID was put into preparation, details collection, details processing, details display and details storage sub sections. Starting, connecting, and cleaning the database and creation the interface were placed under the preparation section. The details collection section ensures that the fundamental details for identification (IP address, computer name and serial number) are factored in. The serial number has to process from the IP address and computer name that is taken care of by the processing sub section. The display section then is responsible for displaying identification details. All these would only happen with a storage location that stores and manages the details.

To make the model complete, relationships between the processes and the sections were indicated. A diagram that shows the all the components and their relation using analogue model was used to model the system

A prototype had to be developed to demonstrate the fact that a serial number can actually be used as a device identifier. As a prototype, the model had to be simple and be able proof the intended concept. This then called for implementation of the prototype using MySQL database and Java's NeatBeans IDE tools. And from the test runs, it was proofed that a serial number can actually be used as an identifier to identify network devices.

References

Behringer, M.H, (2009), Classifying network Complexity, *Cisco Systems*, conferences.sigcomm.org/co-next/2009/workshops/rearch/papers/Behringer.pdf. Accesed on 09/08/2018

Bruhn, M. Gettes, M. and Ann, W. (2003). Identity and Access Management and Security in Higher Education. *EDUCAUSE QUERTERLY*. https://net.educause.edu/ir/library/pdf/eqm0342.pdf. Accessed on 21/03/2015.

Canvan, J.E. (2000). *Fundamentals of Network Security*. Artech House. Boston, London.

Coulouris, G. Dollimore, J. and Kindberg, T. (2005). *Distributed Sytems, Concepts and Design*. Fourth Edition, Addison Wesley.

Danev, B. Zanetti, D. and Capkun,S. (2015). On physical-layer identification of wireless devices,*Computing Surveys* Volume: 45 Issue: 01.

Frankel, S. Eydt, B. Owens, L. and Scarfone, K. (2007). Establishing Wireless and Robust Security Networks: A Guide to IEE 802.11i. *NIST Special Publication*. 800-97.

Harold, E.R., (2013), *Java Network Programming,* 4th Edition, O'Reilly Media. ISBN: 9781449365936

Idris, N.A. and Kassim, N.M. (2010). *Wireless Local Area Network (LAN) Security Guideline*, http://www.cybersecurity.my/data/content/files/11.649.pdf Accessed on 14/3/2015

IEEE-USA. (2009). Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S. *IEEE-USA White Paper.* https://www.ieeeusa.org. Accessed on 24/11/2015

Jain, A., Hong, L. and Pankanti, S., (2000), Biometric Identification*, Communications of the ACM*, Vol.43, No.2

Kurose, J.K. and Ross K.W. (2006). *Computer Networking: A Top_down Approach Featuring the Internet*. 3rd ed. Addison Wesley.

Lee, T. (2010). Securing your Meru Network. *Meru Networks White Paper*. Accessed on 19/09/2014.

Leo, R.V. (2004). Predicting consumer intentions to use on-line shopping: the case for an augmented technology acceptance model**.** *Information & Management*, 41, 747-762.

Lehtonen, M. Staake, T. and Michahelles, F. (2008). From identification to authentication–a review of RFID product authentication techniques. In *Networked RFID Systems and Lightweight Cryptography* (pp. 169-187). Springer Berlin Heidelberg

Luis-Garzia, R., Albero-Lopez, C., Aughzout, O. and Ruiz-Alzola, J., (2003), Biometric Identification Systems, *Signal Processing* 83, 2539-2557

Mandy, A. (2002). Wireless LAN Security. *Information Systems Security*, 11:3, 29-33

Nicopolitidis, P., Papadimitriou, G. I. and Pomportsis, A. S., (2001), Design alternatives for wireless local area networks, *INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS*, 14:1-42

Shay, W. A. (2004). *Understanding Data Communication and Networks*. Third Edition. Thomson Learning

Skiena, S. S., (2008), *The Algorithm Design Manual*, Second Edition, Springer, London

Stallings, W. (2011). *Network Security Essentials, Applications and Standards*. Fourth Edition. Pearson Education. New Jersey, USA.

Takahashi, D. Xiao, Y. Zhang,Y. Chatzimisios, P. and Chend, H. (2010). IEEE 802.11 user fingerprinting and its applications for intrusion detection. *Computers and Mathematics with Applications*, 60 (2010) 307_318.

Tanenbaum, A. S. (2003b). *Computer Networks,* Fourth Edition, Prentice-Hall, India.

Vollbrecht, J. and Moskowitz, R. (2002). Wireless LAN Access Control and Authentication. *Interlink Networks White Paper*. http://www.interlinknetworks.com/whitepapers/WLAN_Access_Control. Accessed on 10/01/2014.