Conference Proceedings of The Kabarak University International Conference on Computing and Information Systems, Edited by Christopher M. Maghanga and Moses Thiga. 14th-15th October 2019 Nakuru, Kenya.

Towards a Unique, Secure, and Robust Wireless Local Area Network Device Identifier

John C. Chebor[1], Simeon M. Karume[2] and Nelson B. Masese[3]

[1]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya
Tel: +254 0721416894, Email: jchebor@kabarak.ac.ke

[2]Laikipia University, P.O. Box 1100-20300, Nyahururu, Kenya
Tel: +254 0722499397, Email: smkarume@gmail.com

[3], [1]Kabarak University, P.O. Box Private Bag, Kabarak, 20157, Kenya

Tel: +254 0727171725, Email: NMasese@kabarak.ac.ke

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. This study therefore examined uniqueness, security and robustness characteristics of MAC in relation to a device serial number in order to establish a suitable network device identifier. In order to achieve this, test runs through a proof of concept method by using *Advanced IP Scanner* and *getmac* command line tools. Advanced IP Scanner was used to determine the security, hence robustness of the identifiers while *getmac* was used to determine the uniqueness of the identifiers. The run tests indicated that a MAC address can actually be spoofed and altered rendering the MAC address not unique, insecure and unreliable. On the contrary, a computer's serial number is hard-coded in the hardware only and therefore cannot be spoofed and altered making it unique, secure and reliable. The researcher recommends that a study be conducted on how a device serial number can be used as network device identifier

Key Words: Network device, MAC Address, Serial Number, Identifiers, Wireless Local Area Network

1. Introduction

Wireless LANs (WLAN) also known as Wireless Fidelity (Wi-Fi) or 802.11 standards is a type of a local area network that allows users access network services using mobile devices (wireless stations) such as laptops, personal digital assistants and even smartphones (Dordal, 2018). The wireless stations use a base station usually an access point (AP) as an entry point to the network services. Unlike wired LANs that use cables or wires as transmission media, WLANs uses radio wave frequencies to transmit information over the local area network.

WLAN comes with a number of benefits as compared to wired LANs, notably mobility, rapid deployment, reduction in infrastructure and operational cost, flexibility, and

scalability (Raji, 2014; DHS, 2017; Wallace, 2018). Due to these benefits hotpots are now virtually found everywhere; in enterprises, at homes, and in public places. Wireless devices such as laptops, personal digital assistants and even smartphones come with WiFi features integrated into 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. Singh & Sharma (2017), point 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 (Stallings, 2011; DHS, 2017; Wallace, 2018), describes the reasons for the threats as default configurations, network architecture, encryption weaknesses, and physical security. Garska, (2016), identifies identification, authentication, and authorization as the essential functions in providing the required services in a network.

For authentication and authorization hence accounting 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, and MAC address. But 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, 2013).

Problem Statement

Existing identification methods at the OSI model include the physical address (MAC address) at the data link layer, the logical address (IP address) at Network layer, the Port address at Transport layer and the application specific address at the application layer. 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 while application address is for identifying different instances of the same application (Kurose & Ross, 2013).

Apart from the absence of identifiers at the physical layer of the OSI reference model, MAC addresses, which are used to identify the physical source and destinations addresses, are not universally unique across networks, they are easily spoofed and altered to aid in spoofing attacks. In addition, MAC addresses are coded on the network hardware and a copy is replicated in the operating system when the system starts to facilitate network troubleshooting and configuration. This copy of the MAC address is the one that is usually spoofed. Furthermore, all the identifiers (MAC address, IP address, Port number and application-specific address) are pointers to locations rather than the device itself.

Research Objectives

The main aim of the study was to investigate the suitability of a MAC address in relation to a serial number as a wireless LAN device identifier. The specific objectives are:

i) To establish the characteristics of wireless device identifiers

ii) To analyse the suitability of a MAC address in relation to a computers serial number network device identifier

iii) To recommend a suitable network device identifier

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.* (2012) further cites examples of identifiers as could be a code (identification number, serial number, ISBN) name (domain name) or an address (IP, MAC, Port Number or an application specific address). An attribute should possess uniqueness, universality, collectability, security, data dependence, robustness and mnemonic (Danev *et al.* 2015; Lavassani *et al.* 2010; and Leo, 2004) qualities to be a good identifier. Whereas uniqueness ensures that no two devices have the same identifier value, 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.

Application specific addresses are addresses that are designed for a specific application geared towards user-friendliness. Also referred to as persistent identifiers (Richards *et al.* 2011), the application specifies identifier is permanently assigned to an object. Examples of application specific addresses include e-mail address such as deanset@kabarak.ac.ke and a universal resource locator (URL) such as kabarak.ac.ke. Whereas an e-mail address defines the recipient of an e-mail, a URL is used to find a document on the internet.
Such addresses or locators fundamentally play a crucial role in enabling internet users easily finds information on the internet (Commer, 2013). This is more so as the internet has a huge amount of information which makes it difficult to find. Labelling the files or objects in a way of application-specific addresses, therefore, makes it easy to find a specific object or file. The addresses, however, get changed to the corresponding port and MAC addresses of the sending computer.

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 (Canavan, 2012).

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, (2011). An IPv4, which is currently in use (Kurose & Ross, 2013), 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, 2013). 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, 2013 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, 2013 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.

Methodology

Out of all the characteristics of an identifier, security, robustness and uniqueness characteristics compromised the suitability of a MAC address as an identifier. Security, robustness and uniqueness qualities were therefore analysed using *Advanced IP Scanner* and *wmic* command line tools through test runs. *Advanced IP Scanner* was used to test security and consequently reliability of a computer's serial number and a MAC address. Similarly, *wmic* command line tool was used to test the uniqueness characteristics of the identifiers whose results are presented in the section next.

Results

Characteristics of a Network Device Identifier

The characteristics that define the suitability of an identifier as were established from the related work section of this study were uniqueness, universality, collectability, data dependent, security (availability, integrity, and confidentiality), robustness and mnemonics. As compared to the other identifier characteristics, security, robustness and uniqueness characteristics were established to compromise the suitability of MAC address. The three requirements were examined as follows

Suitability of MAC Address as Physical Layer Network Identifier

Security of a MAC Address

Availability, confidentiality and integrity aspects of security determine the suitability of a MAC address.

Confidentiality of a MAC Address

Confidentiality of an identifier is the degree of how an identifier can be disclosed to an unauthorized entity (Paulsen & Byers, 2019). Although measures have been put in place to protect the confidentiality of a MAC address by coding it into the network hardware, as a network device identifier, attackers would always have a way of getting it unauthorized. *An Advanced IP scanner* tool, for instance, can be used by an intruder to access MAC address

of all devices connected to the network. To demonstrate this, the researcher created a test network of three computers and then the scanner was run from one of the computers. The results are presented in figure 1 below

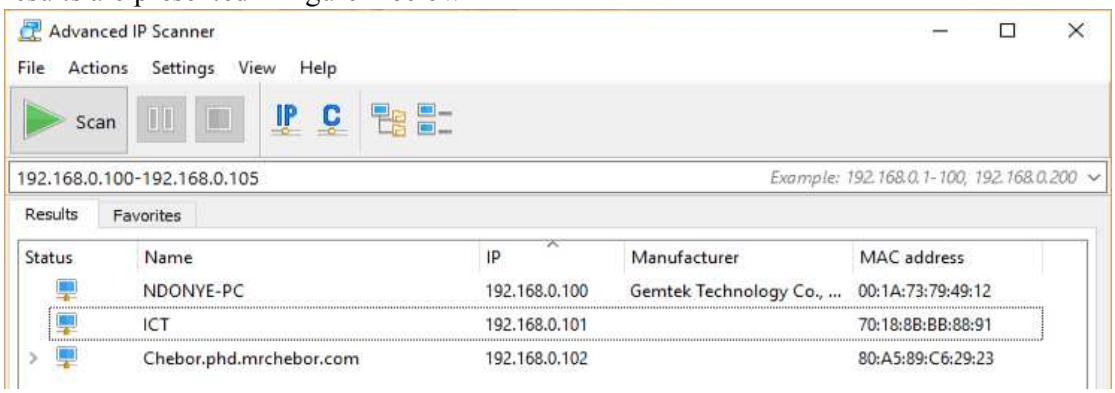

Figure 1: MAC Address Spoofing

As demonstrated in the results in figure 1 above, the scanner collected and displayed all the MAC addresses of the networked computers. This may result in the following flaws

i) If the network is designed to use MAC filters to allow or block network access based on valid existing MAC addresses, then an attacker may use a MAC address spoofed using the advanced IP scanner to gain access to the network
ii) When an attacker knows ones MAC address then they can use it to track a user
iii) If the valid MAC address device and the spoofed MAC address device log onto a network simultaneously, the addresses conflict with each other resulting in miscommunication and inconvenience on the valid device end.

The integrity of a MAC Address

A MAC address is usually hard-coded or 'burned' into the network hardware; therefore, it is difficult to alter it. However, a copy of the MAC address in the system software can easily be modified by an attacker to suit the valid MAC addresses spoofed. To demonstrate this, the following procedure was used to alter the researcher's computer MAC address and results illustrated in figure 2 below:

i) Open System Properties window
ii) Click on Device Manager
iii) Click on the plus sign preceding Network Adaptors list on the dialog that appeared
iv) Select the card whose MAC address is to be altered
v) Right click on the network adaptor and select Properties
vi) Click on the Advanced tab
vii) Click on Network Address option in the list provided
viii) Type the six-digit code in the Value field after selecting the radio button
ix) Click OK

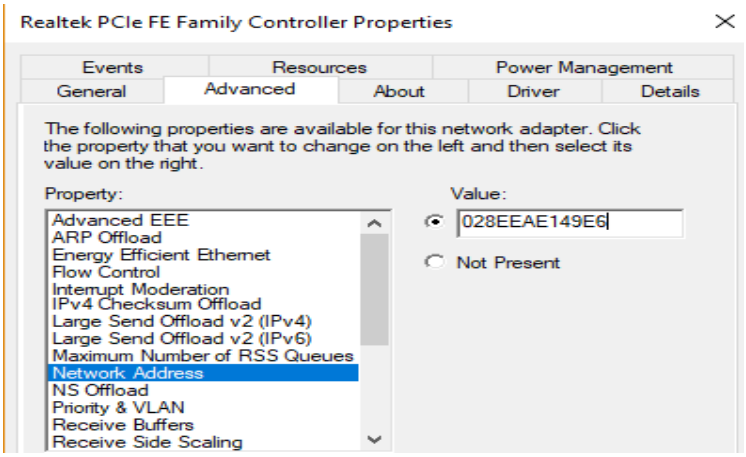

Figure 2: MAC address copy in system software

The altered MAC address is illustrated in figure 3 below. The first part of the figure shows the original MAC address 80-A5-89-C6-29-23 of the researcher's computer before and after it was altered using the procedure described figure 2 above to 02-8E-E4-E1-49-E6.

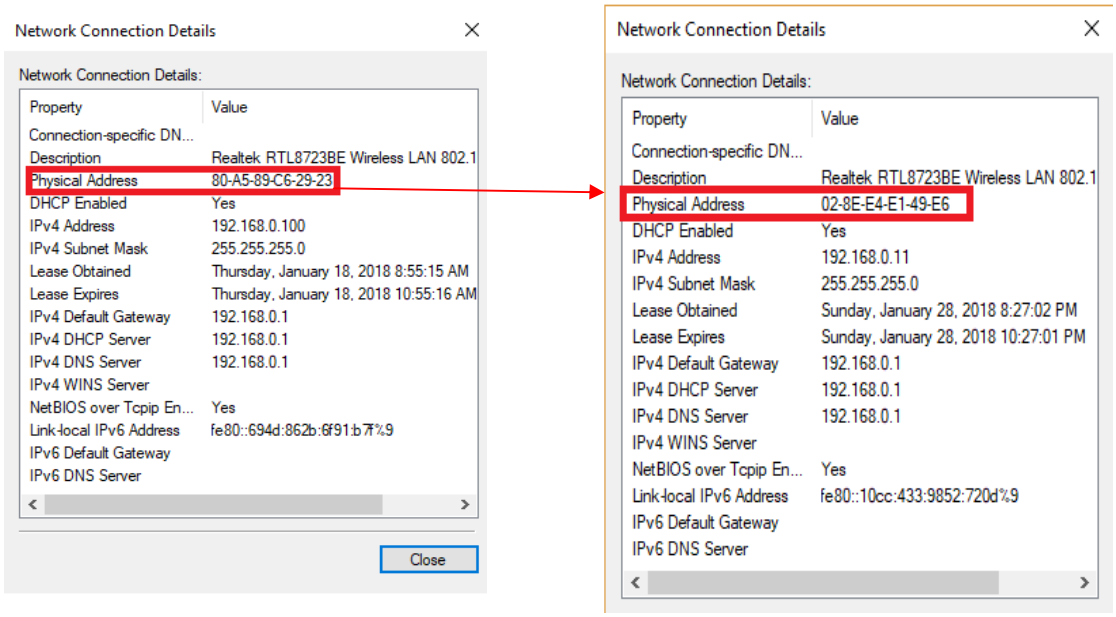

Figure 3: MAC Address before and after alteration

Both results were viewed through the following procedure:

- **a)** Click on Control Panel then Network and Sharing Centre
- **b)** Click on any one of the active networks
- **c)** Click on the Details button on the general tab of the active network window
- **d)** Which leads to Network Connection Details shown in figure 3 above

Availability of a MAC Address

Availability aspect of security as defined earlier on (Paulsen & Byers, 2019), refers to the accessibility and usability of an identifier upon demand by an authorized user. Availability ensures that the identifier works properly and that its service is available to valid users when needed. In ideal scenarios, a MAC address is usually made available by having a

copy in the operating system as illustrated in figure 5 above. However, the effect of the possibility of altering a MAC address compromises the availability of a MAC address.

Robustness of a MAC Address

Robustness characteristic of an identifier refers to the ability of an identifier to function or continue functioning well in unexpected situations (Microsoft Corporation, 2018). Closely related to robustness characteristic of an identifier, are performance and reliability characteristics. Answers to the questions; does the MAC address remain invariant over time? Is a MAC address reliable? is it able to function as intended over a given period time under specified conditions? enable establish the robustness of a MAC address.

The answers to these questions are based on fact that the initial intention of encoding 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). However, due to some valid and invalid reasons, a copy of the MAC dress in the operating system can be altered as shown in figure 6 below. Good reasons for changing a device MAC address include testing out networks for configurations, security applications or new protocols, workarounds and nefarious means. For whichever reasons in changing a MAC address, it leads to the conclusion that a MAC address is not permanent, unreliable and therefore not robust.

The Uniqueness of a MAC Address

The fact that the MAC address is assigned to each network interface controller (NIC) card by the manufacturer makes it unique only to a particular interface. Furthermore, vendors are given a range of MAC addresses that can be assigned to their products by the IEE (Iwaya, 2015). This way, MAC address assignment is controlled such that no different adaptors can have the same address even if they are from different manufacturers. However, a device can have more than one network interface hence even though MAC address can actually uniquely identify a network interface, it doesn't necessary uniquely identify a device.

One case in mind is an instance where a networked computer could contain multiple interfaces for Wi-Fi, Bluetooth and Ethernet adaptors. As illustrated in figure 4 below, a node can contain several MAC addresses. In this particular case, for instance, the node in question contains four interfaces with corresponding four MAC addresses. This was obtained by running the *getmac* command on the command prompt of the computer in question.

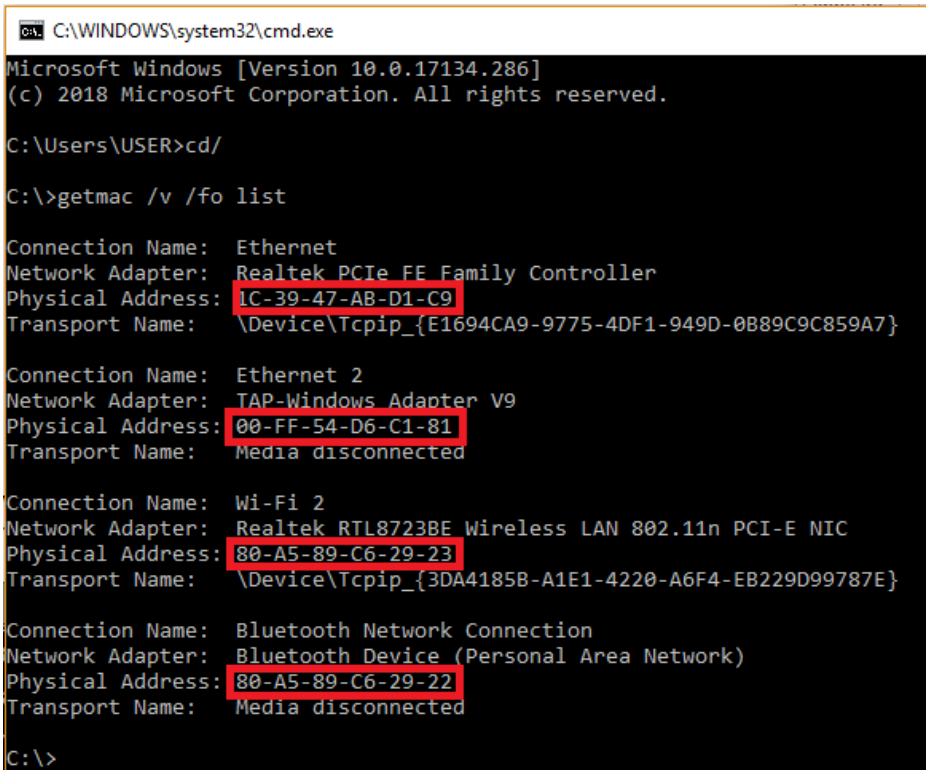

Figure 4: One computer with a number of MAC addresses

The possibility of a MAC address being spoofed is yet another case of a MAC address that makes it not to uniquely identify a device. If a device MAC address is altered for whatever reason, the likelihood of another device having the same address is imminent. As such, it cannot be assumed that a MAC address definitely identifies the device uniquely.

A Computer's Serial Number

- *Computer's Serial Number Location*

Just like in any other product, a computer has its serial number tagged as part of the serialization of the product. Perhaps the only extraordinary thing is that the number is placed strategically on the computer to simply frustrate snoopers from finding it. One would, therefore, more than often find it usually tagged beneath the computer or staged somewhere beside it. Figure 5 below shows an illustration of a laptop model details that include the serial number in a tag.

Figure 5: Serial Number tag on a laptop model

Although tagging of computer serial number is the norm to serializing computers, it is a practice common to products including computers. This way, identifiers that use scanners such as bar code readers can be used to capture their identification details.

Alternatively, modern laptop models have their serial numbers coded into their basic input-output (BIOS) chips. This makes it possible for the identifier to internally be accessed and so, it can be processed for a given desired function. The first line of accessing a computers serial number is generally by running the command *wmic bios get serial number* at the systems command line interface. The serial number for the author's laptop, for instance, can be obtained as shown in figure 6 below;

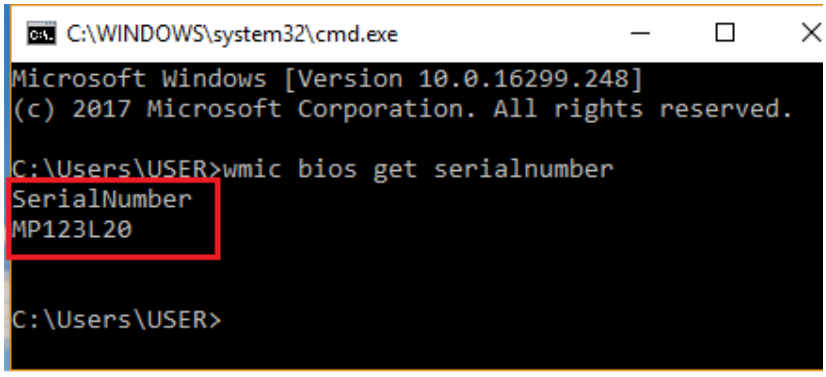

Figure 6: Serial number of a laptop obtained from system BIOS using the wmic command

The encoding of a serial number in a computer's hardware rather than just tagging it on a surface makes it possible to manipulate the serial number. This way, a model that can access the serial number internally and use it to identify the device is made possible.

- *Characteristics of a Computer's Serial Number*

The mere fact that a computer's serial number is hard-coded on the hardware without a copy in the system software alone renders it hard to be spoofed. It then implies that the serial number in normal circumstances cannot be altered and therefore unique, secure and reliable. It is only in some rare cases that the serial number can be altered. But this requires that a computer system has to turned off, any power lines disconnected, any static electricity discharged, computer case opened, disconnect the CMOS battery, wait for roughly 30 seconds (to completely ensure that the CMOS power is completely drained) then the process is done in reverse to revert back to original state (Derekyoung, 2017). This way, all original CMOS settings such as custom CMOS settings, BIOS password, time and

date, as well as the motherboard serial number are lost. The system then generates a new system data that includes a serial number when booted.

Conclusions and Recommendations

The mere fact that MAC address can be spoofed and altered affects robustness and uniqueness attributes of a MAC address due to the fact that apart from it being hard-coded in the hardware, it has a copy of the MAC address in the system software. Uniqueness factor problem 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. On the hand, a computer's serial number is hard-coded in the hardware only and therefore cannot be spoofed and altered making it unique, secure and reliable.

This study then recommends for a further research on how a serial number may be used for identifying a device in a wireless network. One way of realising this recommendation could be by conducting a study towards an algorithm, a model and a prototype that can access a computer's number remotely and use it as an identifier. Progressive systems can as well be developed that would consequently use the computer's serial number as an identifier for authentication, authorization and accounting (AAA) to the network resources.

REFERENCES

Canavan, J.E. (2012). *Fundamentals of Network Security,* Artech House, Boston, London.

Cardenas, D.E., (2018), MAC Spoofing: An Introduction, *GIAC Security Essentials Certification (GSEC),* https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315, Accessed on 07/07/2019

Comer, E.D., (2013), *Internetworking with TCP/IP Volume One,6th Edition*, Pearson, USA

Coulouris, G., Dollimore, J., Kindberg, T. and Blair, G., (2012), *Distributed Systems, 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.

Derekyoung, (2017), How to Change a BIOS Serial Number, *Itstillworks,* https://itstillworks.com/how-to-change-a-bios-serial-number-10394.html, Accessed on 20/06/2019

DHS, (2017), A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family), *Department of Homeland Security (DHS),* Version 1.0 First Release, https://www.us-cert.gov/sites/default/files/publications/A_Guide_to_Securing_Networks_for_Wi-Fi.pdf, Accessed on 20/07/2019

Dordal, P.L., (2018), An introduction to Computer Networks, *Loyola University Chicago,* http://intronetworks.cs.luc.edu/current/ComputerNetworks.pdf, Accessed on 03/08/2019

Garska, K., (2016), Higher Education's Unique Identity and Access Management Challenges, *Identity Automation*, https://blog.identityautomation.com/higher-educations-unique-identity-and-access-management-challenges, Accessed on 10/04/2019

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

Kurose, J.K. and Ross K.W., (2013), Computer *Networking: A Top_down Approach Featuring the Internet*, *6th Edition*, Addison Wesley

Lavassani, K.M., Movahedi, B. and Kumar, V., (2010), Identification in Electronic Networks: Characteristics of e-Identifiers, *Eight International Conference on Electronic Commerce (ICEC)*, 2006, Fredericton, New Brunswick, Canada

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

Microsoft Corporation, (2018). *Microsoft Computer Dictionary*, 6th Edition. Microsoft Press, USA

Paulsen, C. and Byers, R., (2019), Glossary of Key Information Security Terms, National Institute of Standard and Technology (NIST), NISTIR 7298 Revision 3

Raji, M.O., (2014), Design and Implementation of Wireless Network, *Research Gate*, https://www.researchgate.net/publication/269295509_DESIGN_AND_IMPLEMENTATION_OF_WIRELESS_NETWORK, Accessed on 13/04/2019

Richards, K., White, R., Nicoleson, N. and Pyle, R., (2011), A Beginner's Guide to Persistent, Identifiers, *Global Biodiversity Information Facility,* http://links.gbif.org/persistent_identifiers_guide_en_v1.pdf, Accessed on 1/7/2015

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

Singh, R. and Sharma, P.T., (2017), On the IEEE 802.11i security: a denial-of-service perspective, *Security Comm. Networks*; 8:1378–1407, DOI: 10.1002/sec.1079

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

Tanenbaum, A. S., (2011), *Computer Networks, 4th Edition*, Pearson Education, 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

Wallace, K., (2018), Wireless LAN Security, *Kevin Wallace Training*, https://www.kwtrain.com/blog/wlan-security, Accessed on 13/04/19