International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

An Enhanced and Dynamic Network Hardware Devices Security Using MAC Address

Emmilly Mbichi Mwangi[1]

[1]Jomo Kenyatta University of Agriculture and Technology, Institute of Computer Science and Information Technology, P.o. Box 62000 - 00200, Nairobi Kenya

Abstract: ***Network hardware devices are currently becoming very expensive due to high market demand. As a result, they are at a great risk of theft. Securing or recovering a stolen or lost device is a great challenge in the modern world .Every networked computer device has a Network Interface Card (NIC). An NIC has a unique identifier code prominently known as the (media access control) MAC address that uniquely identifies the device under use over the network. It is therefore possible to use a MAC address as a security measure for devices that can operate within a network. Using a database system, users (network security managers) can identify the computer owners using their computer MAC and in case of a reported theft occurrence, it is possible to identify and locate the device. This work therefore, specifically focuses on how to track lost network devices that are still under operation using their MAC addresses.***

Keywords: MAC, address, NIC and network.

1. Introduction

Adoption of the use of network hardware devices especially laptops has been on the rise globally in recent years. These devices have become so crucial in storage of information, communication and even leisure. The loss of these devices from theft or other means usually leave their owners exposed to malice activities of the criminals. Various techniques are currently used to deal with the loss of devices whether in inhibition of information access or physical recovery [1]. These techniques include physical means of tracking the burglar down, using biometric systems for user authentication etc. Most of these techniques are however plagued by difficulties such as high costs and no guaranteed success in physical recovery of the devices.

Every computer device with networking capabilities has a network interface Card (NIC). Every NIC has a unique identity programmed on it, known as the media access control (MAC) address which identifies the device once connected to networks. [5] The MAC address is a 48 bit binary number that is contained in a plaintext frame that is broadcasted in a probe upon sensing network connectivity [2, 4]. MAC addresses thus provide a simple way of tracking devices used in a certain network since every connected device can be monitored uniquely.

1.1 Introduction to MAC address concept

A MAC address is a 48bits number used to uniquely identify a network adapter of hardware in a network. MAC addresses are endorsed to interface vendors by block of 2*24. As a result the 24 leftmost bits of a MAC address are used to identify the producer of the NIC. In any frame, the source address header fields contain the MAC address of the sender interface. The frame headers are never encrypted; hence the source MAC address is available in plaintext in all the frames send by a device. Therefore, the MAC address of a device constitutes an ideal unique identifier of hardware devices. Knowing the MAC address of a device can be used to collect information from systems storing MAC address along with other information.

2. Current Techniques in Tracking and Recovery

2.1 GPS tracking

Some laptops are GPS-enabled and capable of sending their geographical location to a monitoring center. GPS is a navigation system that relies on satellites to determine the precise location of a GPS receiver [3]. However, these systems can be tampered with by resetting the basic input output system (BIOS) of a device. Including this technology in laptops, also significantly increases the cost due the extra GPS receiver hardware needed.

2.2 Physical recovery

Victims of device theft can also report their loss to authorities who can embark on legal processes of tracing them. Chances of finding them are usually very slim adding to the fact that it can be a costly process.

2.3 Biometrics authentication

Biometrics scanning hardware have also been installed on devices to ensure only authentic users can log in. These devices range from finger print readers, iris scanners, voice recognition and face recognition using web cams. Flashing the BIOS may interfere with the hardware of the biometric authentication making it being overridden. Facial recognition using webcams is also prone to hacks by altering of common facial features like say putting on glasses or shaving.

3. Research Problem

Hardware devices especially the highly portable ones like laptops are prone to theft. Currently the most used technique is to track the lost devices is by use of physical means. This

physical means involves reporting to security and a search is carried out. By use of this method the chances of finding these devices are very slim and owners are not guaranteed of finding them. A lot of people use physical mechanisms like locking their devices in a safe to safeguard them, thus increasing malice activities of the criminals. Other techniques such as biometrics and Geographic positions systems (GPS) are not affordable to many middle income earners. Thus developing a system which uses readily available resources such as MAC address will be of advantage**.**

4. Research goals and objectives

1) To conduct a research on the current techniques used to track network devices.
2) To find out whether there exist dynamic methods of tracking network devices.
3) To prove through data analysis how powerful and feasible a hardware devices security is, by use of a database system that can dynamically track network devices using MAC address.

5. Proposed Method

This research contributed a lot to the field of hardware security in that it advances the work done by others in tracking lost network devices as well as giving the owners guarantee of recovering their devices. This will be achieved by enhancing the current physical tracking methods of devices to the use of network oriented technique of using MAC addresses to identify devices and their location. Therefore, the proposed method is more reliable and takes fewer resources in terms of time and energy lost.

6. Dynamic device tracking and recovery

Tracing lost network hardware devices is very crucial in protecting vital information as well as retaining the asset. A cheap and effective way to track a network hardware connected to the network is to use the MAC address. Since the MAC address is unique for every device, a system can be developed to determine the location of the device. The system has a web based application with an online database which has all the MAC addresses of devices and owners information. Upon connection to the internet, geo latitude is used to get the location of the device. An application with a Graphical User Interface (GUI) will be installed in the device as a measure to conceal the tracking technology. If a device is flagged as lost in the database, a prompt alert is send to the user via Short Messaging Service (SMS). Tracking is also eased by the fact that the IP address is sent together with the geo- latitude information to the owner of the device. This technique is effective in the sense that users are given a portal or a web base application where they register. Currently used systems are installed in the hard disk and when these devices are lost or misplaced the malice may format it. Some techniques can be tempered with since one can identify their presence thus we can use the stealth and scare tactic by using the web based system. Such systems don't offer a guarantee to the owner. The dynamic technique (MAC address) of a given device can be used to set off an action when a device is connected. By monitoring the Wi-Fi channel and by examining the source MAC address of the captured frames, it is possible to detect when a device comes in range. Moreover, by considering the signal strength of the received signals, it is possible to approximate the distance between the receiver and the device or even to estimate its position by triangulation if several receivers are deployed [6].

7. Data Collection Analysis and Experimentation

A data was collected using questionnaire and results were summarized as show in the table below. The aim of this was: to find out how many network devices can fit the technologies available. It is clear that each network device in a network has a unique physical address. When you compare with other techniques it out compete them all. Secondly I found out on the availability of the technology the same case is observed since the MAC address is readily available and the research is about network devices. The third was on affordability, in this I tried to find out the cost of acquiring the technology and the maintenance cost. By this the cost of MAC address is zero since it is available in every device. The fourth was the tampering resistance of the method this was in term of the malice person damaging the technology and lastly the survival of the technology in case of hard disk swap or wipe.

Table 1: Techniques and their effectiveness measure

Technique/measure	*Biometric /100*	*GPS/ 100*	*MAC/ 100*
How many devices fits the technology fits	20	5	100
Availability of the technology(regionally)	30	10	95
How many user can afford the technology	40	20	96
What is the tampering resistance of the technology	10	60	99
Potential to survive after hard disk swap/wipe	80	15	90
Total score(%)	36	22	96

8. Conclusion and Recommendations

This paper describes about tracking network hardware devices by use of MAC address. Here I researched on the current techniques applied in tracking network devices in the event of theft. An analysis of the techniques proofs that the most suitable method of tracking lost devices is by use of MAC addresses since it is cost effective, readily available, highly acceptable and very much reliable in terms of permanence. With this we can recover the lost or stolen laptop automatically and at an affordable cost and with an assurance of finding it whenever is connected in a network.

9. Acknowledgement

I would like to thank the almighty God, myself, friends and relatives for helping me to undertake this research from start to completion. May all of you be blessed so much.

References

[1] Christian Roy, "An Alternative Approach to Identifying Stolen Network Clients Using DHCP., school of computer science,ChristianRoycGilluniversity, http://scholar.google.co.in/scholar
[2] Kenneth Vernon Westin, Portland, "MOBILE DEVICE OR COMPUTER THEFT classification, http://scholar.google.co.in/schor.
[3] Google Books,. (2015). *Patent US20050149752 - System and method for tracking laptop computers*. Retrieved 19 February 2015, from https://www.google.com/patents/US20050149752
[4] Mathieu Cunche, Mohamed-Ali Kaafar, and Roksana Boreli. Linking wireless devices using information contained in Wi-Fi probe requests. Pervasive and Mobile Computing, (0):–, 2013.
[5] Ben Greenstein, Ramakrishna Gummadi, Jeffrey Pang, Mike Y. Chen, Tadayoshi Kohno, Srinivasan Seshan, and David Wetherall. Can Ferris Bueller still have his day off? Protecting privacy in the wireless era. In Proceedings of the 11th USENIX nworkshop on Hot topics in operating systems, pages 10:1–10:6, Berkeley, CA, USA, 2007. USENIX Associatio
[6] P. Bahl and V.N. Padmanabhan. RADAR: an in-building RF-based user location and tracking system. In INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, volume 2, pages 775–784 vol.2, 2000.

Author Profile

Emmilly Mbichi Mwangi is a competent and experienced guru the field of computing and Information Technology. She specializes in networking management systems research and development. She is an expert in the area of developing strategies for innovation and creativity. She has always provided commendable leadership and pursues strategies for engagements with the senior executives on Innovation in Business and Information Technology. **She** is pursuing the B.S. degree in Information Technology from Jomo Kenyatta University of Agriculture and Technology since 2011. During 2011- 2014, she stayed in I.T. Research and network management in various universities and organizations in Africa. She is now amongst the best adored Information technology specialist not only in Africa, but also globally.