ISSN No:-2456-2165

Investigating the Effect of Sinkhole Isolation on the Wireless Network Sensor System" Case Study the University of Rwanda

DUSHIMIYIMANA Eric[1] Master's,
Supervisor by Dr. Musoni Wilson Ph.D.
[1] Information communication and Technology (ICT), University of Kigali, Kigali, Rwanda.

Abstract:- This research focused on: understanding the effects of sinkhole isolation or Network Access Control(NAC) isolation on the Wireless sensor Networks System (WSNs).

Investigating cryptography-based strategies to limit network degradation caused by the isolation of sinkhole. The WSNs is a self-configuring network that does not have centralized control. Sensing devices are referred to as nodes.

The main reasons for this research are to look at the effects of isolation of sinkhole in the wireless sensor Network System, and to look at the steps to be taken to prevent malicious attacks. Malicious can also join the network and launch various active and passive attacks, Malicious attacks have a detrimental effect on the Network and on users of the Internet with insufficient security. it is we who must establish reliable protection. For many applications, security (i.e., confidentiality, integrity and availability of information).

The results of this research study was achieved through qualitative technique of primary research. An open-ended interviews are aimed to be conducted with the identified sample population(IT) in which they were given a complete chance to share their opinions and views about asked questions and research problem. Moreover, the sample population of this study includes the individuals from IT industry.

I. INTRODUCTION

A Sinkhole is a server designed to capture malicious traffic or unauthorized access and prevent control of infected computers by the criminals who infected them. Wireless communications is unavoidable in today's technology because of the benefits it provides, such as mobility, portability, freedom from network connection, and so on. Given the advantages, it opens the door for adversaries to eavesdrop on the information is transmitted and also makes active intrusions are less difficult (through the wireless medium). In order to keep unauthorized people out, It is necessary to design highly secured protocols for the network, which provided both The confidentiality of wireless internet connectivity and the reliability of communicating parties.

II. STATEMENT OF THE PROBLEM

Some institution, public and private company didn't used sinkhole in wireless network sensor system. This reduces the security of the wireless network in a particular institution. Because if you don't use the Sinkhole server, it was easier for hacks to access the company's resources using a wireless network because it does not have enough security. Most companies that use a wireless network do not have enough security because they only use passwords and there is a need for reliable security.

Because wireless sensor networks use a broadcast transmission medium, information is more vulnerable than in wired applications. As a result, security mechanisms such as encryption and authentication are required to protect data transfers. Existing network security mechanisms, however, are impractical in this domain due to limited processing power, storage, bandwidth, and energy resources.

Encryption and authentication mechanisms provide adequate defense against low-level outsider attacks. Cryptography, on the other hand, is ineffective at preventing laptop-class and insider attacks. It is still a problem that requires more research and development. Insiders significantly reduce the effectiveness of link layer security mechanisms. This is due to the fact that an insider is permitted to participate in the network and has complete access to all messages routed through the network, with the ability to modify, suppress, or eavesdrop on the contents.

III. THE FUNDAMENTAL SECURITY OF A WIRELESS SENSOR NETWORK

The general objective of this research is to deploy usually WSN in security-sensitive environments and We must protect the wireless network from unauthorized access or unintended uses in order to keep it secure. We discuss the various types of wireless sensor network attacks and how to prevent them.

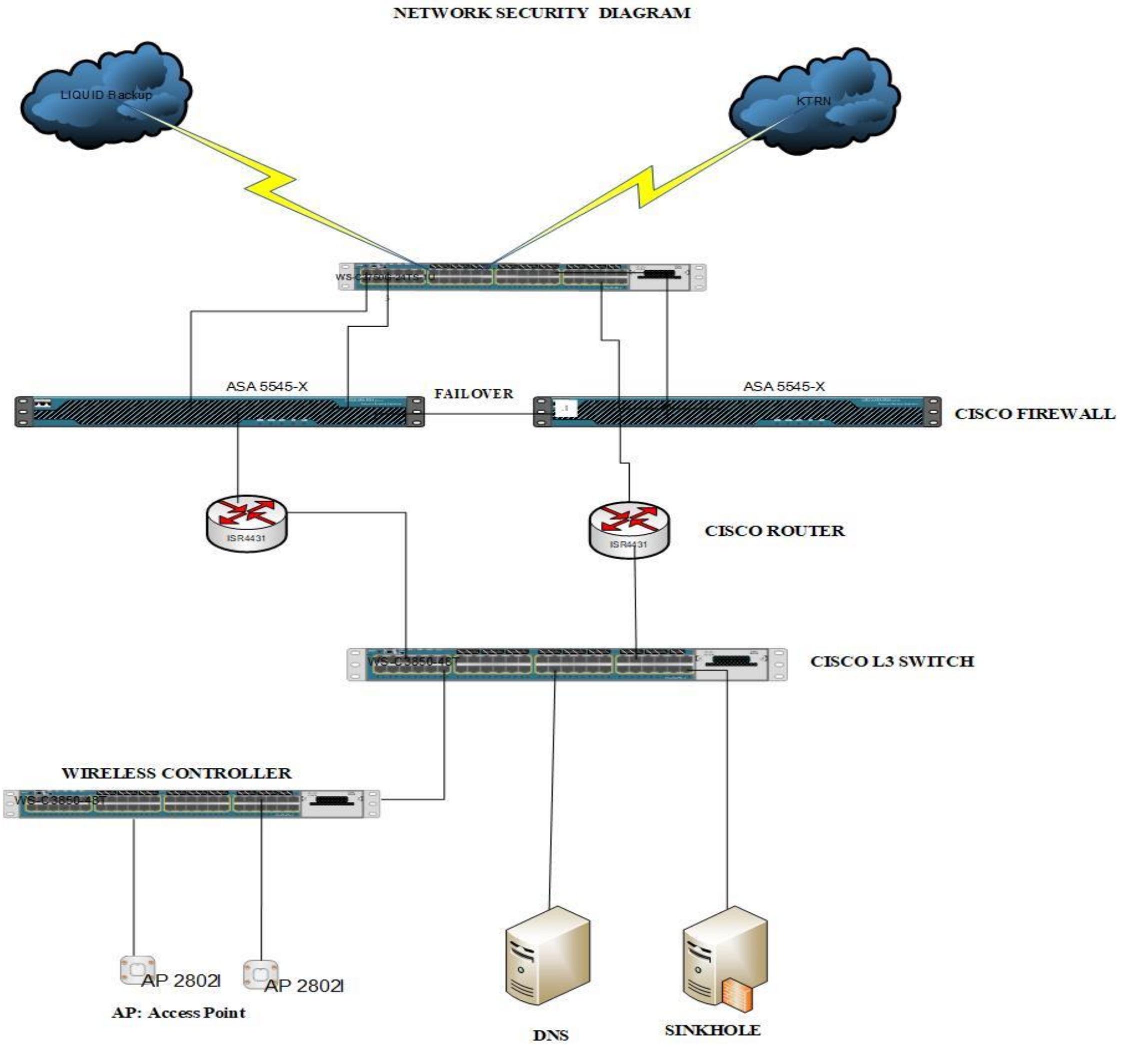

Fig 1. a basic wireless sensor network

- *Some Wireless Sensor Network attacks*

Because of the broadcast nature of the transmission medium, wireless networks are vulnerable to security attacks. Furthermore, because WSNs nodes are unfriendly and unprotected due to their location, security is made more vulnerable. When a sensor network is very large, it is extremely difficult and complicated to supervise and defend each node. The attackers always create various types of security threats in order to make the WSN system unsteady and unstable. To gain a general understanding of the security system of this network, various types of WSN security threats are listed here.

A. *External and Internal Attacks*

Outside attacks are those that originate from outside stations. Insider attacks occur when genuine WSN nodes engage in unintended or unauthorized behavior. To overcome this problem, you must be tough against outsiders . Realistic levels of security must be implemented to prevent insiders from conducting network attacks.

B. *Passive vs. Active Attacks*

A sensor network that wireless made up of hundreds of thousands of sensor nodes connected to one or more base stations that handle all transmission functions for the sensor node stations . Passive attack is eavesdropping or monitoring of data exchanged during transmission. However, active attack includes changing information directly or modifying packets while they are being transmitted.

C. *Host Based Attacks*

Host-based attacks are classified into three types. These are user-compromise, hardware-compromise, and software-compromise. In the user compromising process, WSN user nodes are managed to provide trustworthy information to intruders such as passwords and sensor node keys. Tempering is a process that reveals the program code, data, and keys stored in sensor nodes by compromising the hardware. Software compromise entails disassembling the software code that runs on sensor nodes. Buffer overflows occur when the operating system or application running on the sensor nodes is vulnerable.

D. Network Based Attacks

Layer-based attacks and protocol-based attacks are the two main types of network base attacks .These attacks primarily target information during transmission. These attacks deviate from the protocol as well. Aside from service availability, message confidentiality, network integrity, and authenticity, an insider of the network gains an unreasonable advantage in network usage. The attacker engages in self-centered behavior that disrupts the protocol's dedicated operation.

IV. EMPIRICAL REVIEW

We must protect the wireless network from unauthorized access or unintended uses in order to keep it secure. There are three critical services for there are security mechanisms. The CIA security model defines confidentiality, integrity, and availability. The term "confidentiality" means that any unauthorized access to the network must be prohibited. Only reliable network nodes have access to the resources. The term "integrity" refers to the requirement that a message be delivered from sender to receiver without being changed or modified. Unauthorized individuals must not access or change sensitive information.

Ngai et al. proposed an efficient IDS algorithm with low overhead. This robust algorithm verifies network flow information to ensure data consistency and captures the intruder. In addition, the technique is resistant to the presence of many malicious nodes.

Wireless Sensor Networks is a cooperative network of number of sensor devices that communicate in a short range to share the sensed information. The sensor networks have got a great attention due tolow cost and ad-hoc deployment structure. As a result, wireless sensor networks have piqued academics' curiosity, and numerous researchers have been researching on various aspects of wireless sensor networks i.e. Low processing power, limited communication resources, limited memory, and battery power When designing protocols for wireless sensor networks, different trade-offs must be made in order to effectively utilize these scarce resources. Because of the nature of wireless sensor networks, security is the most important issue. The low processing and memory constraints prevent the implementation of a protocol with security mechanisms.. Wireless sensor networks have limited resources, such as computing power, communication bandwidth, and memory, and are powered by batteries. When creating protocols for wireless sensor networks, different trade-offs must be made in order to make the best use of these limited resources. Because of the nature of wireless sensor networks, security is the most important concern. The lack of processing power and memory prevents the deployment of a protocol with security features. Wireless sensor networks are used in sensitive environments and are prone to sinkhole, wormhole, and greyhole attacks, among other things. Sinkhole attacks are one of the most hazardous types of attacks, in which a phony node promotes a fake routing update, such as the shortest way to a sink node, causing network traffic to fail. A complete literature review is conducted in this study to highlight current sinkhole attacks in wireless networks, as well as prevention methods. The research is based on a set of parameters that are associated to the proposed solutions. The paper also discusses the challenges in detecting the sinkhole attacks (Mubashir Ali, Muhammad Nadeem and al., 2020).

V. METHODOLOGY

The results of this research study achieved through qualitative and descriptive methods. To achieve the best results, we must use both quantitative and descriptive data collection methods. When you combine the two, we get deeper insights.

- *Data Analysis*

The process of cleaning, transforming, and processing raw data in order to extract information is known as data analysis actionable, relevant information that assists businesses in making informed decisions. The procedure reduces the risks associated with decision-making by providing useful insights and statistics, which are frequently presented in charts, images, tables, and graphs.

Kenton, (2019), said that, Descriptive statistics are concise descriptive coefficients that summarize a given data set, which can be a representation of the entire population or a sample of it. Descriptive statistics are divided into measures of central tendency and measures of variability (spread). The mean, median, and mode are examples of measures of central tendency, whereas the standard deviation, variance, minimum and maximum variables, and kurtosis and skewness are examples of measures of variability.

Descriptive statistics or frequencies used to summarize the data. The researcher evaluated the mean by using these equivalences which are found in the table illustrated below. These equivalences of mean help to learn about each group's perception of the sub-variables.

VI. FINDINGS

The diagram below summarizes the gaps identified in software/hardware/tools during the assessment of the university's wireless network security 5 layers in network security infrastructure:

- *Data Layer*

This layer describes the inspection of data packets to detect attempts to compromise network applications

- *Endpoint Layer*

This layer focuses on technologies that protect the IT environment through keeping track of activities, authorization and authentication of client /server devices (end point devices).

- *Network Layer*

This layer contains technologies that restrict and control access to critical network assets

- *Perimeter Layer*

This refers to software/hardware/tools that protect the boundary between the private and locally managed-and-owned side of a network and its public, usually provider-managed side.

- *Security and Monitoring Layer*

The software/hardware/tools in this layer aid in keeping watch against threats to the IT environment. An alert is raised whenever a suspicious activity is detected

➢ *Finds*

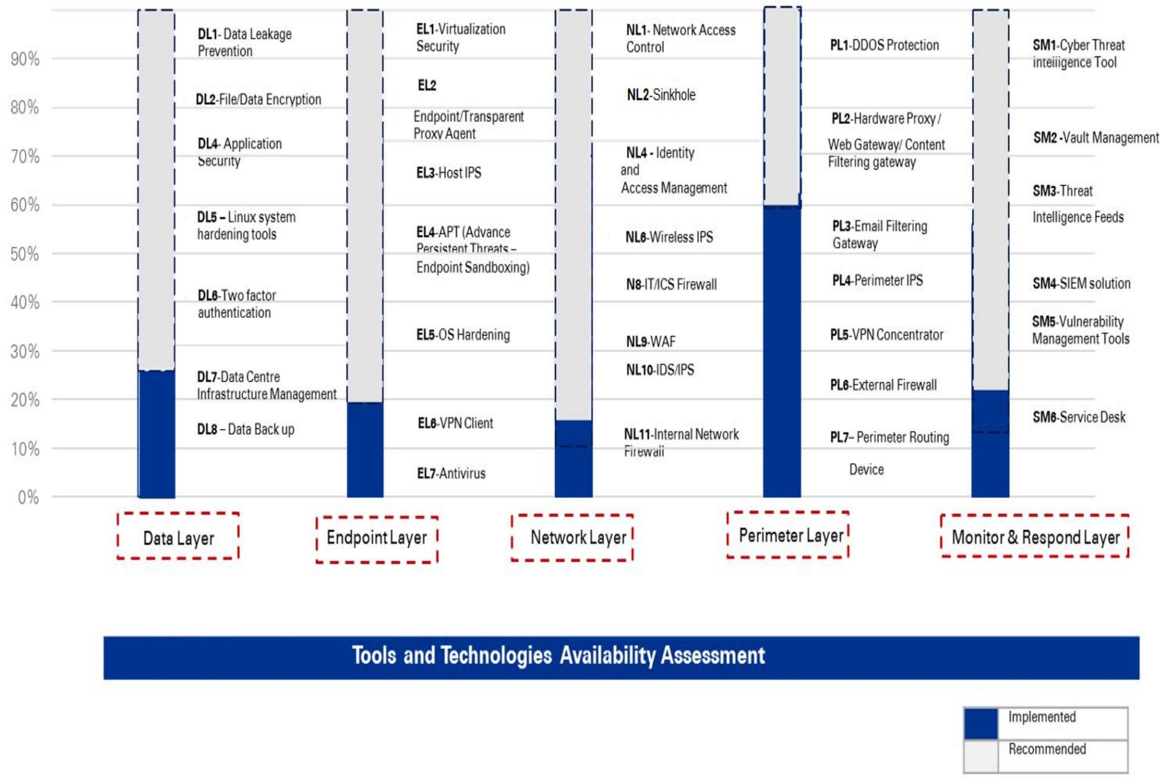

Fig 2: Finds

➢ *Data Layer Findings*

- *Data Leakage Prevention*

UR does not have a data leakage prevention tool in place. Confidential and sensitive data may be leaked to unauthorized personnel who could use the data maliciously.

- *Data Encryption*

UR does not have a data encryption tool. Without data encryption, unauthorized users can gain access to the data.

- *Application Security Testing*

UR does a lot of in-house development especially around Online registration. We recommend UR should consider implementing an application security tool .

- *Two Factor Authentication Software*

UR stores sensitive data and records in its systems. UR also uses a lot of cloud storage in its environment. The university should use two factor authentication to enhance information security in its IT environment.

➢ *End Point Layer Findings*

- *Virtualization Security*

We observed that UR uses virtualization in its IT environment. A virtualization security tool to aid in the protection of virtual infrastructure configured in an environment

- *Host IPS*

UR does have intrusion prevention system (IPS) in its IT environment.

- *Linux System hardening*

UR should harden its operating systems. This involved configuring system and network components properly, deleting unused files and applying the latest patches.

Without OS hardening the university may be susceptible to remote execution attacks from malicious hackers

- *Advanced Volatility Threat Protection*

UR has a dynamic IT environment and it is ever changing. There is need for UR to have an advanced volatility threat protection to protect against malware

Advanced Volatility threat protection offers security against malware that is persistent in its attacks and wipes its trace/steps after stealing sensitive data

➢ *Network Layer Findings*

- *Network Access Control (NAC) and Sinkhole*

We noted that UR does not have a NAC in place. NAC is a method of increasing the security of a proprietary network by restricting network resources to endpoint devices that adhere to a defined security policy.

- *Internal and External Firewalls*

We observed that UR has implemented Cisco routers in its network environment. As UR redesigns its network environment based on best practice, the university should consider the following firewalls and select one based on its needs.

- *Privileged Identity Management (PIM) Solution*

We noted that the university does not have a PIM solution , PIM is the monitoring and protection of superuser accounts in an organization's IT environments in place.

➢ *Perimeter layer Findings*

- *Web Application Firewall (WAF)*

We observed that there is no web application firewall in place. A hacker can use SQL injection and cross site scripting to gain credentials to an application. WAF can protect web applications visible or accessible from the Internet, including outward facing or intranet applications

- *Web Gateway/ Content Filtering*

UR does not have a web gateway/content filtering solution. Users can access sites that contain hidden risks and inadvertently download malware.

A web gateway/content filtering tool gives organizations the ability to prevent web users visiting online destinations that may harbor hidden security risks or unacceptable content.

➢ *Security and Monitoring Layer Findings*

- *Security Incident and Event Monitoring(SIEM) Solution*

We noted that there is no SIEM tool in place. Without a SIEM tool UR may not be able to detect and respond to security threats in a timely manner leaving it exposed ,A SIEM analyzes log and event data in real time to provide threat monitoring, event correlation and incident response.

- *Vault Management Tool*

UR has a number of administrator passwords for its critical software and hardware such as databases, operating systems, firewalls ,network routers and switches .A vault management tool secures, stores, and tightly controls access to API keys, tokens, passwords, certificates, and other confidential information in modern.

- *Security Operations Center (SOC)*

We noted that there is no SOC in place. UR can choose to set up a SOC or outsource the services. SOC is a centralized unit within an entire organisation that detects, analyzes, and responds to cyber security incidents.

- *Vulnerability Management Tools*

We observed that UR does not have in place tools that can aid in vulnerability assessment and penetration testing. Without this tools UR may be unaware of the weaknesses within its IT environment.Vulnerability assessment tools can assist the university in testing and verifying the strength of its security controls. The tools can point out security weaknesses within the IT environments that may expose the University to malicious hackers.

- *Threat Intelligence Feed*

We observed that there is no threat intelligence feed at UR. This may leave the organization susceptible to malware attacks as they may not be up to date on the current cyber security trends. A threat intelligence a feed is a continuous stream of data related to potential or current security threats to an organization

VII. CONCLUSION

UR has implemented various software/hardware and tools such as VPN's,e-learning, Online registration, email gateway tools, data backup tools and service desk across its IT environment.

UR has implemented majority of the software/hardware and tools available across the perimeter layer. However there is need to improve and implement critical software/hardware/tools across all the layers in order to enhance the network security posture of UR cause of Sinkhole isolation.

RECOMMENDATION

➢ *There are weakness today on sinkhole isolation on the wireless network sensor system*

UR does not have a Sinkhole in place, Sinkhole is a method of bolstering the security of a proprietary network by restricting network resource availability to endpoint devices that adhere to a defined security policy. It also detects and prevents potential data breaches/exfiltration transmissions by monitoring, detecting, and blocking sensitive data while it is in use (endpoint actions), in-motion (network traffic), and at-rest (data storage). This tool is used to prevent sensitive data from being lost, mishandled, or accessed by unauthorized users.

REFERENCES

[1]. Roshan Singh Sachan, Mohammad Wazid, Avita Katal, D P Singh, R H Goudar, ”A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN”, International conference on Communication and Signal Processing, April 3-5, 2013, India.

[2]. https://www.researchgate.net/publication/261247977_A_cluster_based_intrusion_detection_and_prevention_technique_for_misdirection_attack_inside_WSN March 11th 2022

[3]. https://www.researchgate.net/publication/347752321_Addressing_Sinkhole_Attacks_In_Wireless_Sensor_Networks_-A_Review March 11th 2022

[4]. https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1506-1 March 12th,2022

[5]. Bhavkanwal Kaur [1] , Puspendra Kumar Pateriya [2] “A Security Framework for Detection and Prevention of Misdirection Attack in Wireless Sensor Networks for IOT” nternational Journal of Engineering Trends and Applications (IJETA) – Volume 5 Issue 5, Sep-Oct 2018

[6]. Shahzad, F., Pasha, M., & Ahmad A. (2017). A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. International Journal of Computer Science and Information Security, Vol. 14, No. 12. arXiv preprint arXiv:1702.07136

[7]. Hossain, M., Muslima, U., & Islam, H. (2015). Security Analysis of Wireless Sensor Network. Journal of Multidisciplinary Engineering Science and Technology (JMEST), Vol. 2 - Issue 1, pp. 393-403, 2015. DOI: 10.1155/2014/303501

[8]. Rung-Ching Chen, Chia-Fen Hsieh and Yung-Fa Huang (March 2010)An Isolation Intrusion Detection System for Hierarchical Wireless Sensor Networks

[9]. avita Tandon (2016), “Sinkhole Attacks in Wireless Sensor Network Routing: A Survey”, Research Journal of Computer and Information Technology Sciences, IEEE, Vol. 4(8), pp. 4-7.