Using Secure Virtual Private Networks for Increasing the Patient Privacy in the case of Telemonitoring Services

Jules Gbedande
Polytechnic of Abomey-Calavi
University of Abomey-Calavi
Cotonou, Bénin

Michel Dossou
Polytechnic of Abomey-Calavi
University of Abomey-Calavi
Cotonou, Bénin
Email: michel.dossou [AT] epac.uac.bj

Antoine Vianou
Polytechnic of Abomey-Calavi
University of Abomey-Calavi
Cotonou, Bénin

Henoc Yatakpo
Polytechnic of Abomey-Calavi
University of Abomey-Calavi
Cotonou, Bénin

Marc Assogba
Polytechnic of Abomey-Calavi
University of Abomey-Calavi
Cotonou, Bénin

Abstract— **Global health care system is facing a crucial personnel shortage issue. Developing countries bear the high shortage burden. This is due to mass brain drain from developing to developed countries. Remote health care systems aim at increasing access to health care for outpatient living at remote areas where access to health care services represents a challenge. Homecare also takes benefit from remote health care. Sharing information in the remote health care system can be done via virtual private networks (VPN). Virtual Private Networks (VPN) permit to share information through secure tunnel on internet. However, VPN faced some security issues such as Distributed Denial of Service (DDoS), identity theft attacks… The goal of this article is to enhance VPN security by providing a firewall-based system and Snort-inline intrusion prevention system.**

Keywords: Intrusion, VPN, Snort-inline, Tunnel, Attacks.

I. INTRODUCTION

Internet of Things (IoT) is a network of dedicated physical objects that integrates technologies and enables objects to interact with their internal states or external environments [1]. The Internet of Things is used in several fields such as: energy, transport, communication, and health. The use of information technology in medicine will improve health care and significantly reduces the costs and interventions inefficiencies.

Hospitals are often short of qualified medical staff or some of them have a small number of doctors. It is necessary to use remote surveillance or Internet of Things technics to strengthen the quality of care in these hospitals.

In the field of health, the Internet of Things is committed to providing information related to patients in health care. For example, medical telemonitoring allows patients to be monitored outside of conventional clinical settings. This reflects lower costs of care and improved health services. In medical telemonitoring, the sharing of information between patients and health centers can be done via the public network (internet). Virtual private networks can be used to reduce the risk of attacks by remote medical monitoring and ensure the integrity and confidentiality of information shared between patients and health centers [2].

VPN make it possible to use the internet network to set up a secure transmission channel (tunnel) between two network entities [3]. This work aims to prevent different attempts to intrude on the VPN.

II. RELATED WORKS

Studies have been done in the field of IoT to ensure the protection of shared information within medical remote monitoring systems. According to Zimu et al's., work [4], access and falsification of IoT devices are blocked by combining the obfuscation approach, PPG (photoplethysmography) and ECG (electrocardiography). Nevertheless, this system has limits since it does not perform the encryption of the transmitted data. Tyson Macaulay in his work[5], proposed data management techniques in IoT systems to ensure the security in the routing of data on the internet. Mamta et al.[6] have also proposed a model of security and privacy protection implemented in METEOR (Methodist Environment for Translational and Outcomes Research) [7]. This model indicates that patient privacy is better protected [8-9] by implementing a systematic combination of technologies and best practices such as technical data misidentification, data access restrictive and security measures technological platforms. Ahmed Dridi et al in their article [10] have proposed the semantic medical IoT platform that allows the semantization of IoT in the field of health. Chanchal Raj et al

proposed in their article [11] a low cost rural health monitoring platform for sharing important patient information. We also have the work of Melisa and Kamath [12] who implement a system of monitoring body fat and heart rate that can save patient information to reduce the frequency of consultation.

III. PROBLEM STATEMENT

Hospitals in rural areas in developing countries sometimes lack a sufficient number of qualified personnel. It is therefore necessary to find a way to remotely monitor patients from these hospitals. Internet of things is a way that responds to this patients monitoring needs. However, information shared on this network is sometimes confronted with hacking problems. It is necessary to strengthen security on the network of connected objects.

IV. RESEARCH OBJECTIVES

This article aims to propose a new security architecture for remote monitoring of patients by physicians from a less expensive but very secure VPN based platform. This architecture does not require the renewal of medical equipment. It is based on existing equipment for remote monitoring. Telemedicine has advanced health care [13] and has allowed physicians to consult patients remotely [14]. Thus, to ensure the sharing of information between patients and doctors, specialized links that are sometimes very expensive are used. This work aims to provide VPN architecture to secure the sharing of patient data on the internet and uses a VPN intrusion prevention system to prevent different intrusion attempts.

V. RESEARCH METHODOLOGY AND MATERIALS

In this work, we configured host-to-site VPN using the IPsec protocol. This VPN makes it possible to secure the sharing of patients' sensitive data through a tunnel. We used the **openswan** tool to implement VPN because IP addressing will be dynamically assigned. In order to validate authentication between the client and the VPN server, we used the IPsec 256 rabbit protocol. The architecture of the health surveillance system is shown in Fig. 1.

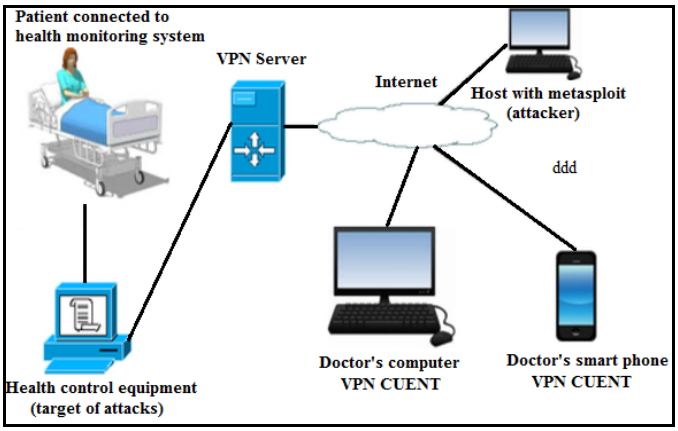

Figure 1. Medical telemonitoring with the host site VPN

To test the vulnerability of the unsecured health surveillance system, we used Metasploit attack generator to generate an attack. We have configured a firewall and finally installed on the VPN server an intrusion prevention system (SNORT-INLINE). To compare the vulnerability of the secure VPN to the unsecured VPN, we generated the same attacks as those generated on the unsecure VPN. The structure of the secure VPN is shown in Figure 2.

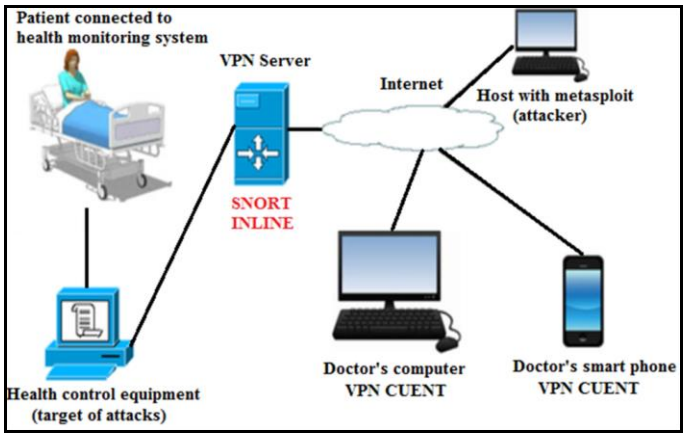

Figure 2. Medical telemonitoring with the host to site VPN and SNORT INLINE

VI. EXPERIMENT

We performed a connection test to verify the proper functioning of the set up network. Figure 3 shows the result of the test.

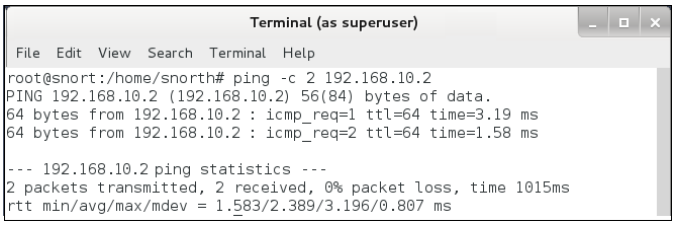

Figure 3. Connection test

VII. RESULTS AND DISCUSSION

A. Attacks generation test in health monitoring architecture based on simple VPN

Before generating an attack on a remote host, we need to know the open Transmission Control Protocol (TCP) ports on the host. With the **Nmap** tool (Network Mapper), we tested and verified the open TCP ports on the target machine. The result of the test is shown in Figure 4.

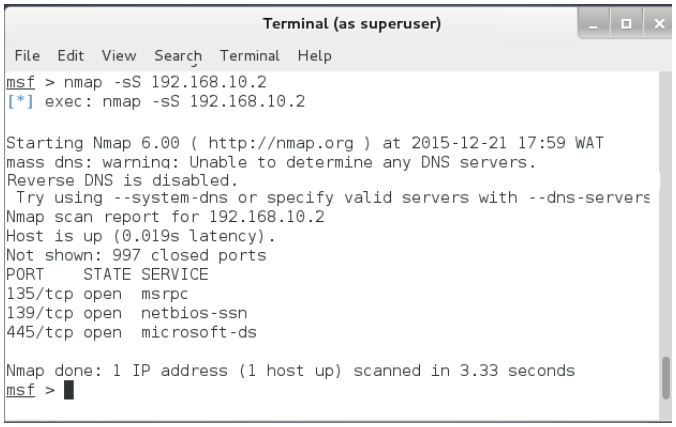

Figure 4. Attacks generation test in health monitoring architecture based on simple VPN

B. MS08 067 attack generation

This attack allows remote code execution if an affected system receives a specially crafted RPC request. **MS08 067** attack works on Windows XP and Windows Server 2003. In developing countries, most computers continue to use the Windows XP system. We therefore consider to pay particular attention to this type of attack. To generate this attack, we loaded it into the Metasploit attack generator. After loading the attack, we sent the TCP reverse payload.

Figure 5 shows the result of this attack.

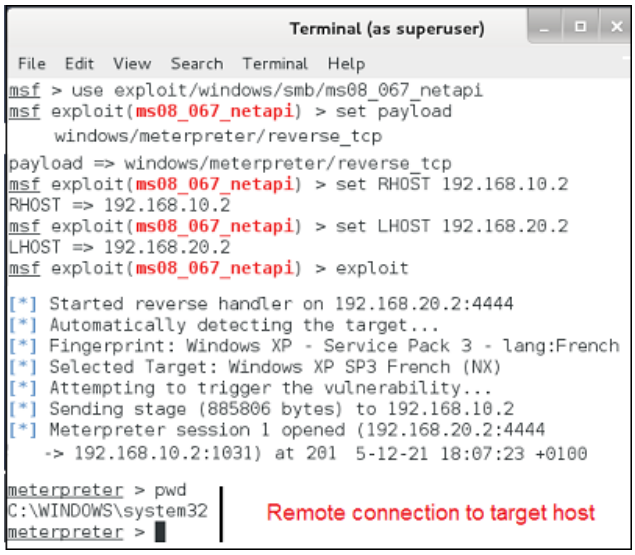

Figure 5. Remote connection to target host

C. Attacks generation test in health monitoring architecture based on secure VPN

In order to secure the VPN and test its vulnerability, we installed on the VPN server an intrusion prevention system. Then we generated the same attack as before. The attack on the secure VPN was blocked by the intrusion prevention system. Figure 6 and Figure 7 show the results of the test.

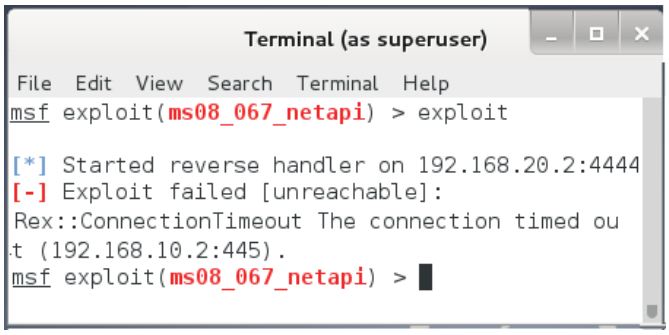

Figure 6. Intrusion prevention system blocks the MS08 067 attack

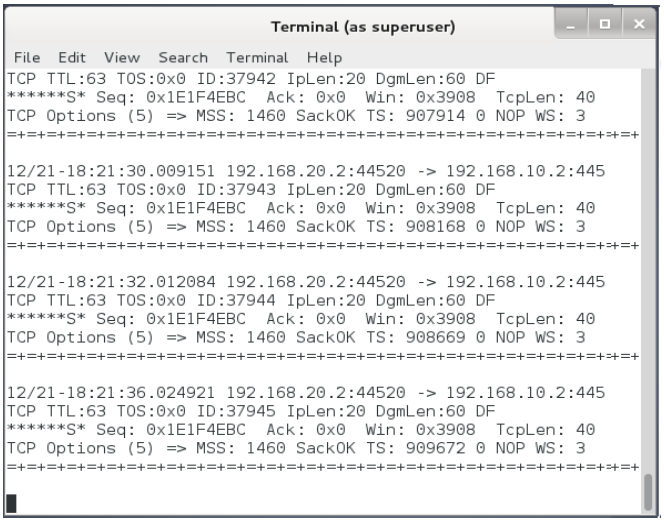

Figure 7. Contents of intrusion prevention system log file

VIII. CONCLUSION

This study allowed us to improve the security, confidentiality and confidentiality of data exchanged through a proposed new network architecture. This study has also made it possible to prevent various intrusions into a surveillance system in the field of health on virtual private networks. The proposed network architecture is based on intrusion prevention systems and firewalls. It can detect different intrusions into health surveillance systems.

But what are the new types of attacks on VPN and what is the impact of the insertion of the intrusion prevention system on the quality of service (QoS) within the health surveillance systems?

[1] B. N. C. A. V. L. Z. M. Zanella A, «Internet of things for smart cities», *IEEE Internet Things J.*, 2014.

[2] O. M. A. A. Mohammed Basheer Al-Somaidai, «Remote monitoring and controlling of gas sensors using VPN connection», *International Conference on Future Communication Networks*, 2012.

[3] M. N. Ogbu, G. N. Onoh and K. C. Okafor, «Cloud based virtual private networks using IP tunneling for remote site interfaces», *IEEE 3rd International Conference on Electro-Technology for National*

Development (NIGERCON), 2017.

[4] Zimu GUO et al., «Hardware Security Meets Biometrics for the Age of IoT», *IEEE International Symposium on Circuits and Systems (ISCAS)*, 2016.

[5] T. MACAULAY, «RIoT Control Understanding and Managing Risks and the Internet of Things», *Elsevier*, 2016.

[6] T. H. X. Y. S. C. R. O. a. S. W. Mamta PUPPALA, «Data Security and Privacy Management in Healthcare Applications and Clinical Data Warehouse Environment», *International Conference on Biomedical and Health Informatics (BHI)*, 2016.

[7] B. W. X. P. Lejiang GUO, «The real-time wireless infrastructure for family medical care base on wearable technology», *International Conference on Future BioMedical Information Engineering (FBIE)*, 2009.

[8] N. VERMA, «Cyber Security In 21st Century», *Global Vision Publishing House*, 2013.

[9] S. M. a. P. P. S. Kale, «IOT based Wearable Biomedical Monitoring System», *International Conference on Trends in Electronics and Informatics*, 2017.

[10] A. Dridi, S. Sassi and S. Faiz, «Towards a Semantic Medical Internet of Things», *IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)*, 2017.

[11] C. Raj, C. Jain and W. Arif, «HEMAN: Health monitoring and nous: An IoT based e-health care system for remote telemedicine», *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 2017.

[12] M. Pereira and K. K. Nagapriya, «A novel IoT based health monitoring system using LPC2129», *2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, 2017.

[13] C. J. W. A. Raj Chanchal, «An IoT based e-Health Care System for Remote Telemedicine», *IEEE WiSPNET conference*, 2017.

[14] N. K. T. P. K. Priyanka Kakria, «A Real-Time Health Monitoring System for Remote Cardiac Patients Using Smart-phone and Wearable Sensors», *International Journal of Telemedicine and Applications*, 2015.