International Journal of Computer Applications (0975 - 8887)
Volume 167 - No.8, June 2017

Combating Malware with Whitelisting in IoT-based Medical Devices

Raghu Nallani Chakravartula
Security Architect, Philips Healthcare
Bengaluru, India

V. Naga Lakshmi, PhD
HOD, GITAM Institute of Computer Science
Visakhapatnam, India

ABSTRACT

With the rapid advancements in the mobile, Internet and wireless technologies, the computing environment is seamlessly getting integrated into the physical world and being connected to the Internet leading to Internet of Things (IoT). In this environment, heterogeneous devices can communicate with one another, leading to innovative applications in healthcare. Malware in IoT environment possesses a great challenge due to interconnected and interoperated systems. Traditional signature based anti-malware solutions will not suffice to healthcare based IoT devices. The paper presents a novel approach of using whitelisting in IoT-based healthcare medical devices and illustrate the performance improvements over traditional solutions.

General Terms

Security, Internet of Things (IoT)

Keywords

Internet of Things (IoT), Whitelisting approach, Medical devices, Signature based Anti-Virus (AV), Malware

1. INTRODUCTION

'Malware' is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, spyware, ransomware, Trojan horses, worms, adware and other malicious programs.

As more and more medical devices are interconnected, they are increasingly exposed to malware and security risks. Malicious programs could not only impair the medical devices functionality but potentially adversely effect on patient safety. Malware running on a medical device can negatively impact the confidentiality, integrity, availability and performance of the system.

Traditionally, Anti-Virus solutions are used as a golden standard to detect & prevent malware intrusions[1]. However, these solutions proved ineffective on IoT-based medical devices. The paper addresses combating malware using whitelisting approach.

Having given an initial introduction and motivation of the work, the rest of this paper is structured as follows. Section 2 talks about limitations of signature-based AV's in medical IoT-based devices. Recent security incidents and the use of white-listing approach are captured in Section 3 & 4. Section 5 describes the background & related work. Methodology, workflow and assessment details are presented in the respective sections 6,7 and 8. The conclusion of this paper is in section 9.

2. LIMITATIONS OF SIGNATURE BASED ANTI-VIRUS

Most traditional anti-virus (AV) software's are based on signatures to detect malicious programs. Signature-based anti-virus software works by scanning every executable in the end-point and triggers an alert when the signature of the binary matched with that of the database in the AV. Signature based AV's are ineffective on IoT-based medical devices for following reasons.

2.1 Signature based AV solution cannot protect against 0-day attacks

Next generation malware or zero-day malware is a previously unknown computer malware for which specific antivirus software signatures are not yet available. Hence, these malicious programs go undetected and cannot be triggered with signature based AV programs[2].

2.2 Signature based AV solutions behavior impacts integrity of the product

Signature based AV solutions are based on blacklisting approach. Black listing solution will block all known malicious activity and permit the rest. Hence, constant upgrade of signatures is important to ensure that the solution can defend against the known malware[3]. This might have negative impact on the integrity of the product.

2.3 New variants of malware

Advances in malware capabilities allow same malware to have different signatures adopting polymorphism or metamorphism techniques[4,5,6]. New signatures are needed in AV software to detect the variant of the existing malware.

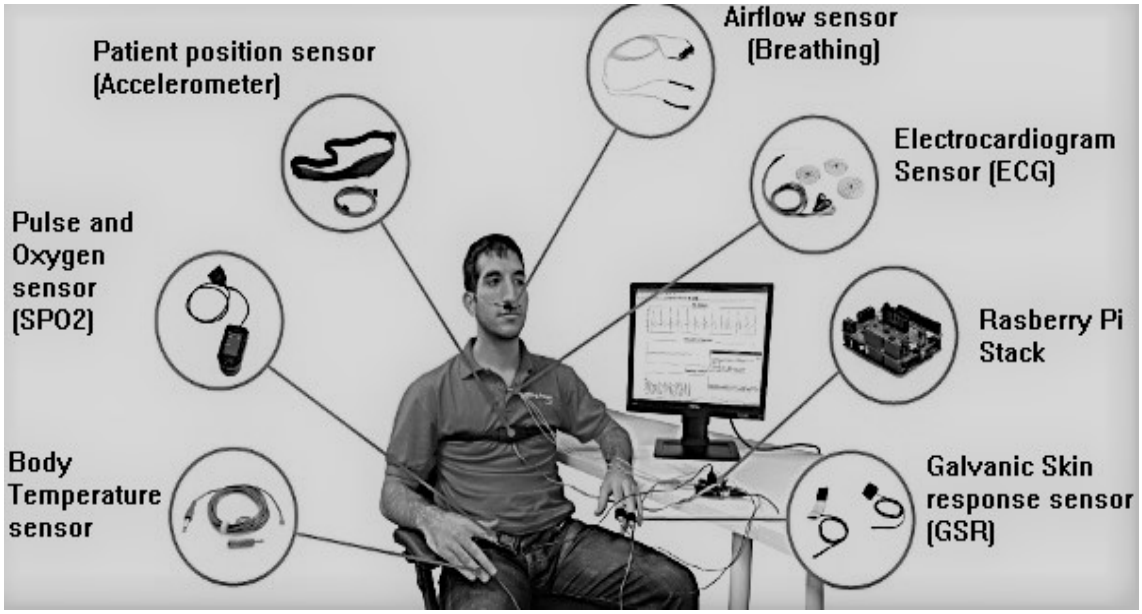

Fig. 1. High level architecture of Patient monitoring

2.4 Signature based AV solutions lead to risk of false positives and false negatives

Signature based AV's triggers false alerts. These false positives or false negatives might have diverse impact on the reliability and safety of the product.

2.5 Signature based AV solutions are less suited in resource constraint devices

IoT-based Medical devices are resource constraint in processing, memory, hard disk and network bandwidth[7]. Increase in malware signature affects the performance. For example, in April 2005, ClamAV has less than 100,000 signatures. As on Feb 2017, ClamAV contains more than 5,760,000 virus signatures[8].

2.6 Regression testing critical after signature update

The clinical software has to be tested after every major signature update to ensure the new signatures does not break the functionality and quality of the software. considering the cost and effort, it would not be feasible to perform the same.

2.7 Signature based AV's need Internet connectivity

Most of the medical devices are deployed within dedicated hospital private subnets. External connectivity to internal network is generally discouraged as any malware outbreak may lead to patient safety concerns and loosing critical Protected Health Information (PHI). Whitelisting does not need signature update and it works based on the existing policies.

Considering the above, Application whitelisting is the recommended approach for IoT-based medical devices.

3. RECENT SECURITY INCIDENTS

Hollywood Medical Center computer system was infected with malware on Feb 2016 and hacker encrypted all files on the system. The hospital paid $17,000 USD in Bitcoin to gain access to the filesystem [9]. The recent outbreak of Wannacry ransomware attacked more than 230000 computers across in over 150 countries. Britain National Health Service Hospital and Barts Health network of hospitals are few examples where the entire IT systems were shut down to contain the malware leading to a huge loss [10]. Medical device company Bayer Medrad radiology device was infected with the malware. It was used to improve the imaging for MRI. These incidents show the need for application whitelisting approach [11].

4. APPLICATION WHITELISTING APPROACH

Application Whitelisting approach [12,13,14,15] is designed to permit known good activity and block all other. It takes a snapshot of the existing system, and any deviation from the original operation is not allowed.

According to NIST, An application whitelist [16,17] is a list of applications and application components (libraries, configuration files, etc.) that are authorized to be present or active on a host according to a well-defined baseline. The technologies used to apply application whitelists to control which applications are permitted to install or execute on a host are called whitelisting programs, application control programs, or application whitelisting technologies. Thereby, Application whitelisting technologies intends to stop the execution of malware and other unauthorized software.

5. BACKGROUND & RELATED WORK

Various concepts are proposed towards the development of behavior based anti-malware. References [18,19,20,21] use control-flow graphing to create signatures for detecting malware. However, the

mechanism does not work when the malware is encrypted to identify the control flow.

Reference [22] uses behavior identification for classifying malware into families and create a methodology to identify the signatures but suffer from same limitations that exist in signature based AV.

Reference [23,24] created a system that works based on traffic analysis. The proposed system does not work on resource constraint devices.

The above literature is confined to various aspects of whitelisting but none of the them addressed the needs of the IoT based medical device

6. IMPLEMENTATION METHODOLOGY

The proposed architecture depicts the use of various sensors in patient monitoring by measuring the below patient vital parameters as shown in the figure 1:

(1) Pulse oximetry often referred as SpO2 used to determine the measurement of the saturated percentage of oxygen in the blood.

(2) Hemo dynamic monitor is used to monitor the blood pressure and blood flow within the circulatory system. It involves non-invasive with an inflatable blood pressure cuff.

(3) Respiratory rate monitoring through a thoracic transducer belt via ECG channel

(4) Body temperature sensor is used to monitor the temperature of the patient

(5) Capnography monitoring is used to measure the concentration or partial pressure of carbon dioxide (CO2) in the respiratory gases.

(6) Patient position accelerometer sensor helps to determine the patient body movements and positions with respect to the diseases.

(7) Galvanic skin response sensor is a method of measuring the electrical conductance of the skin, which varies with its moisture level. It helps to understand the patient emotions as it represents the sympathetic nervous system

Patient data on vital parameters is captured by these sensors and transmitted to the base station. The base stations captures the traffic to transmit over cloud for further processing and analytics. The proposed whitelisting approach is implemented in raspberry pi hardware.

Linux operating system is deployed in raspberry pi and McAfee Application control is used for whitelisting the base station as illustrated in the fig 3.

7. APPLICATION CONTROL DEPLOYMENT WORKFLOW

This section provides an overview of the Application whitelisting deployment workflow as depicted in fig 2.

(1) Install the medical application

(2) Take snapshot of the system by running solidify command

(3) Perform regression testing to learn existing flows

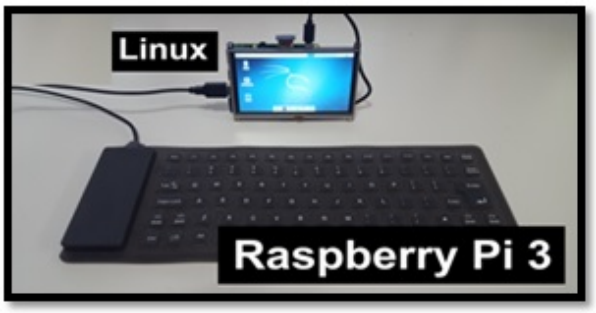

Fig. 3. Base station deployed in Raspberry Pi

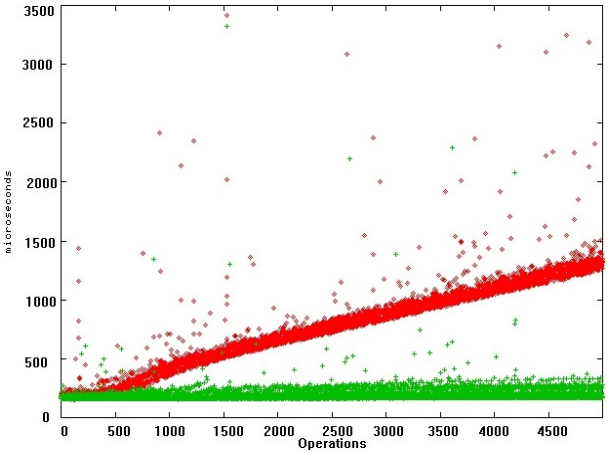

Fig. 4. Performance assessment with signature based AV Vs Whitelisting approach

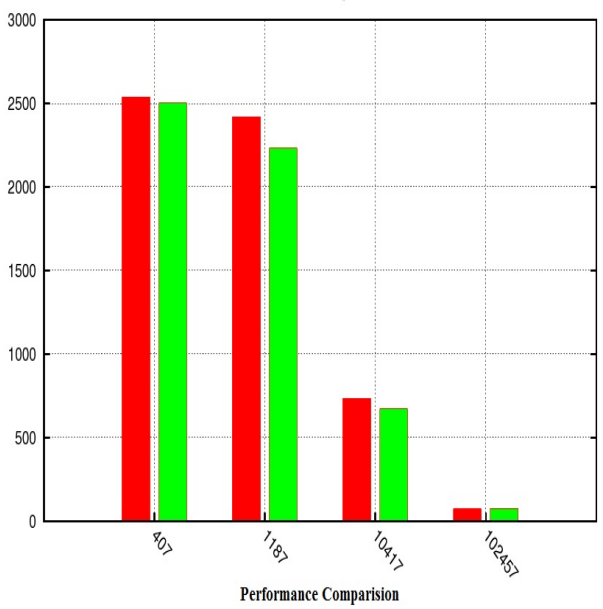

Fig. 5. Performance assessment with and without whitelisting solution

8. ASSESSMENT

Performance assessment of signature-based malware solution is compared with the whitelisting approach as shown in fig 4. It is benchmarked against CPU, File IO, and memory utilization. Signature based AV solution is indicated in red color and green is used to represent the whitelisting approach.

Performance assessment of with and without whitelisting solution is captured by enabling and disabling the whitelisting solution.

The performance graph in fig 5. shows minimal impact on CPU, File IO, and memory utilization with & without whitelisting solution. The same is indicated in red and green color respectively.

9. CONCLUSION

The paper presents the limitation of signature based Anti-virus approach against IoT-based medical devices. Thereby, It illustrates the application whitelisting approach and implementation details in an IoT Based patient monitoring environment. The paper concludes by capturing the performance and availability improvements against the signature-based system. The future research work includes implementing the whitelisting to various sensors in Patient monitoring system and measuring the performance against the baseline.

10. REFERENCES

[1] O. Sukwong, H. S. Kim, J. C. Hoe, "Commercial Antivirus Software Effectiveness: An Empirical Study", Computer, vol. 44, no. 3, pp. 63-70, 2011. "Critical Controls for Effective Cyber Defense" in , vol. 4.1, 2013.

[2] S. Alvarez and T. Zoller "The Death of AV Defense in Depth-revisiting Anti-Virus Software " in CanSecWest Vancouver B.C. Canada 2008.

[3] S. Jana and V. Shmatikov "Abusing File Processing in Malware Detectors for Fun and Profit " in IEEE Symposium on Security and Privacy (S&P) 2012 San Francisco CA USA 2012 pp. 80-94.

[4] B. B. Rad M. Masrom and S. Ibrahim "Camouflage in Malware: from Encryption to Metamorphism " International Journal of Computer Science and Network Security vol. 12 no. 8 pp. 74-83 Aug. 2012.

[5] K. Murad S.-M. Cheng Y. Zikria and N. Ikram "Evading Virus Detection Using Code Obfuscation " Future Generation Information Technology pp. 394-401 2010

[6] P. O'Kane S. Sezer and K. McLaughlin "Obfuscation: The Hidden Malware", Security & Privacy IEEE vol. 9 no. 5 pp. 41-47 2011.

[7] Kelly Hughes and Yanzhen Qu ?Performance Measures of Behavior-based Signatures? 9th International Conference on Availability, Reliability and Security, 2014.

[8] ClamAV (May, 2017). Retrieved from clamav.org

[9]"Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers", [Online Document Feb, 2016] Available at https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center

[10] "Medical Devices Hit By Ransomware For The First Time In US Hospitals", [Online Document May, 17] Available at https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#425cf961425c

[11] A. Beuhring and K. Salous, "Beyond Blacklisting: Cyberdefense in the Era of Advanced Persistent Threats," in IEEE Security & Privacy, vol. 12, no. 5, pp. 90-93, Sept.-Oct. 2014.

[12] S. Dery, "Using Whitelisting to Combat Malware Attacks at Fannie Mae," in IEEE Security & Privacy, vol. 11, no. 4, pp. 90-92, July-Aug. 2013

[13] Patrice Godefroid Michaeal Y. Levin David Molnar SAGE: Whitebox Fuzzing for Security Testing Communications of the ACM March 2012.

[14] P. R. L. Eswari and N. S. C. Babu, "A practical business security framework to combat malware threat," World Congress on Internet Security (WorldCIS-2012)?

[15] S. A. C. DeCato, "Increasing the security on non-networked ground support equipment: Analyzing the implementation of whitelisting protection," 2016 IEEE AUTOTESTCON, Anaheim, CA, 2016, pp. 1-5.

[16] NIST Whitelisting Guide http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

[17] J. Newsome, B. Karp, and D. Song, "Polygraph: Automatically generating signatures for polymorphic worms," presented at the 2005 IEEE Symposium on Security and Privacy, 2005.

[18] Z. Li, M. Sanghi, Y. Chen, M.-Y. Kao, and B.Chavez, "Hamsa: fast signature generation for zeroday polymorphic worms with provable attack resilience," in 2006 IEEE Symposium on Security and Privacy 2006, pp. 15 pp.-47.

[19] W.-C. Sun and Y.-M. Chen, "A rough set approach for automatic key attributes identification of zero-day polymorphic worms," Expert Systems with Applications, vol. 36, pp. 4672-4679, 2009.

[20] Z. Li, L. Wang, Y. Chen, and Z. Fu, "Network-based and attack-resilient length signature generation for zero-day polymorphic worms," in IEEE International Conference on Network Protocols, Beijing, China,2007, pp. 164-173.

[21] M. F. Zolkipli and A. Jantan, "A framework for malware detection using combination technique and signature generation," presented at the Second International Conference on Computer Research and Development, 2010.

[22] "Wannacry", Available online https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_WannaCry_Ransomware.pdf

[23] G. Hu and D. Venugopal, "A malware signature extraction and detection method applied to mobile networks," in Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE International, 2007, pp. 19-26

[24] J. M. Hagen, E. Albrechtsen, and J. Hovden, "Implementation and effectiveness of organizational information security measures," Information Management & Computer Security, vol. 16, pp. 377-397, 2008.

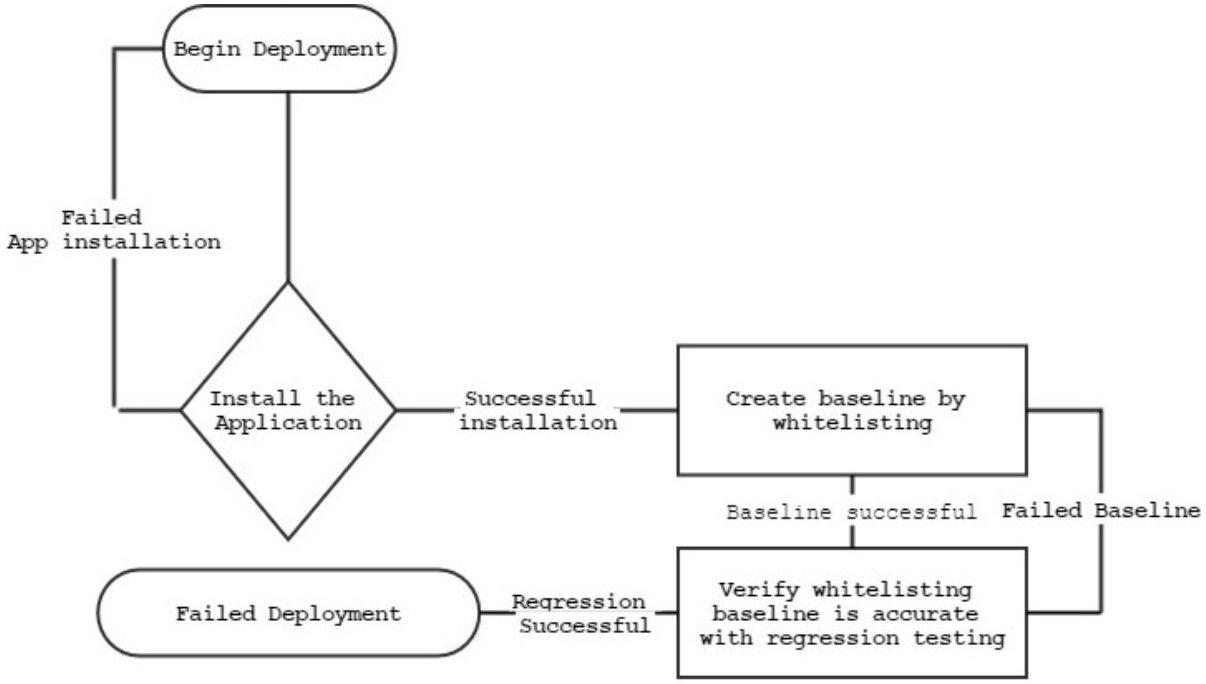

Fig. 2. Application control deployment workflow