Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical Systems : A Review

Arjun Raj
PG Scholar,
Department of Computer Science And Information Technology
College Of Engineering, Perumon

Suja Rani M.S.
Assistant professor
Department of Computer Science And Information Technology
College of Engineering, Perumon

ABSTRACT

Medical cyber physical systems(MCPS)are getting popular now a days. Every advanced healthcare hospitals use the help of MCPS to ease otherwise complicated tasks.These systems analyze the patient status using physical sensors and employ corresponding reaction using actuators. An array of sensor devices are attached to the patient which reads real time data and analyses it. Actuators provide corresponding action with respect to the values sensed. Nowadays these cyber physical systems(CPS) are used as tool for cyber attacks.This can relatively harm the patient or may even cause a direct or indirect threat to life. Since the CPS work based on sophisticated and more complex algorithms, intrusion detection in such system can be really complicated task. Since this area is developing in a peak rate, new attacks are being modeled and deployed. Here, intrusion detection system uses behavioral rule specification which is efficient enough to detect unknown attack/attacker patterns. The methodology is to transform behavior rules to corresponding state machines so that the Intrusion detection system can analyze whether its moving towards a safe state(normal behavior) or an unsafe state(deviation from its normal behavior)that compromises the security of the system. This technique also uses a peer to peer approach in which each nodes monitor its neighboring nodes so that to reduce the chance of failure.

Keywords

intrusion detection, sensor ,actuator, medical cyber physical systems, healthcare, safety, security

1. INTRODUCTION

Security researchers had proved that critical medical devices connected to a patient is highly vulnerable to cyber attacks. Cyber criminals may targets these devices and may initiate an attack. Hospitals were unaware that those devices that they trust is being infiltrated by the cyber attackers and is currently working as a part of an attack. Detecting an attacker in MCPS is further complicated task. The device uses complicated algorithms, sophisticated patient treatment procedures executed within a blink of an eye[1]. Of course those systems demands high execution rate without compromising precision, zero tolerance when it comes to tolerance. To see and perfect every gap in each and every module by a security professional in such a device is a mundane task[2]. From such a standpoint intrusion detection[3] in such systems are necessary to protect the integrity of MCPS because of the unmatched consequences of its failure.

To embed an intrusion detection system in MCPS sensor/actuator networks brings further challenges[4]. These sensor/actuator networks are highly resource constrained. Adding an intrusion detection system should bypass these challenges. With all these in mind a new methodology for intrusion detection is put-forward which uses behavioral rule specification-based Intrusion detection (BSID) which utilizes behavioral rules for defining normal behavioral patterns for a medical device. These behavioral patterns represent acceptable behaviors of that particular CPS[5]. Further, these behavioral rules are then transformed into a state machine, so that any deviation from normal state to an unsafe state can be easily monitored.

The impact of various attackers are also investigated to benchmark the effectiveness of MCPS Intrusion Detection System. This methodology has also been proved to display a higher true positives for a reduced false negative as well as false positive rate. This can further help to identify more complex and invisible attackers[6]. A peer to peer architecture provides an additional uninterrupted operation of Intrusion Detection System.

The main difference between building an IDSs for healthcare devices and other systems is that the attack happens on the physical component rather than in the network or communication protocols. so IDS should be closely coupled with the physical equipment of the Cyber Physical System[7].

2. OVERVIEW OF INTRUSION DETECTION

Before moving on to IDS, lets look at what actually an intrusion is, it is nothing but an unauthorized access in the network or devices though which an intruder or a hacker can alter or grab sensitive information which would directly or indirectly affects the confidentiality, integrity and security of the system or its users[8]. As the cyber physical systems are growing at a fast rate, network security is a serious issue that should be considered[9].

IDS is commonly employed in second stage security after firewall protection. Many IDS exist nowadays which uses different techniques for intrusion detection and are discussed below.

2.1 Categories of Intrusion Detection Systems

2.1.1 Host based intrusion detection. Host based intrusion detection system is employed on the device that is being monitored. It consist of agents which is responsible to identify intrusions by verifying the logs,system calls or any modifications to the file systems[10].

2.1.2 Network Based Intrusion Detection. This technique monitors the ongoing traffic on the network to detect any live disturbances or penetration attempts[11]. This requires a NIC card to capture and monitor all traffic that passes through the network. It inturn contains a sensor module capable of analyzing a positive match with any threat patterns within its database

2.1.3 Signature Based Detection Systems. Signature based intrusion detection works on predefined signatures. This technique is efficient for attacks that's previously been known and further depends on continuous updation of its signature databases[12]. The disadvantage of this system is that it deliberately fails when it comes to unknown attacks.

2.1.4 Behavior Based Detection System. Behavior or Anomaly based intrusion detection system is capable of detecting unknown attacks and attacker patterns. This technique analyses for any deviation from its expected behavior. The normal activity profile is maintained through out and is device specific. The major disadvantage of such systems is defining its device specific rule set.

2.1.5 Hybrid Intrusion Detection System. Hybrid approach uses a combination of both signature based and behavior based intrusion detection. This method can help us to detect both known as well as unknown attacks and further reduces the false alerts currently generated by behavioral based intrusion detection design[13]. The categories of IDS are shown below in Fig 1.

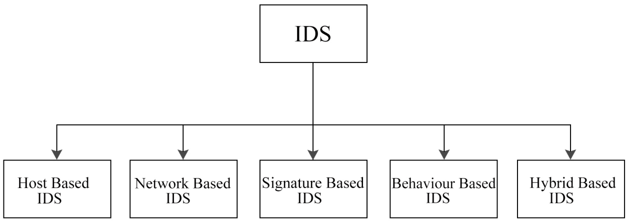

Fig. 1. Categories of IDS

3. MCPS INTRUSION DETECTION DESIGN

The IDS design for MCPS model[14] is based on the use of specification based behavioral rules for each sensor/actuator devices. They are designed to identify an inside attacker attached to these devices which may be sensors or actuators. Monitoring[15] is done using trusted neighbor which continuously monitors for any abnormal behavior. The IDS module is completely isolated from the MCPS functional modules in-order to minimize the risk of exploiting the design methodology and implementation details.

3.1 Behavior Rules

For each device, its behavioral rules are predefined during the design and testing phase. This method takes in behavioral rules for specific devices and analyze whether if that device is being deviated from expected behavior specified by behavioral rule set. Isolated from the functional modules of MCPS, modification of behavioral rules are posible during its normal functioning without interrupting its operation[16].

Since the sensor and actuators are resource constrained, this method uses a lightweight specification based behavior rules for each and every component. The method uses a peer to peer approach such that each and every device performs monitoring of their neighboring nodes. That means a sensor/actuator might be monitoring other dissimilar sensor/actuator nodes. Thus failure of IDS can be reduced to a greater extend. While specifying behavior rules, the acceptable numerical parameters for IDS may vary for different patients.

3.2 Transforming Rules to State Machines

A state is identified as an attack state when a behavior rule is being deviated from an expected one. Each behavioral rule may not point to only a single state, but a collection of states that may include safe or unsafe states. Unsafe states are those in which violation of behavior is being observed. Hence this rule have plenty of state variables together with a range of values that indicates that the node is in safe state or in unsafe state.

The steps described below converts a behavioral rule specification into a state machine. At first an attack behavior indicator is identified as a result of a violation of behavior rule. This attack behavior indicator is then transformed to conjunctive normal form predicate and the state components are identified from the state machine. Then the attack behavior indicators are combined into a Boolean expression in disjunctive normal form. This is then transformed as union of all predicate variables into state components of a state machine followed by marginalizing the range values. The states are then managed by state collapsing and finding out illegitimate combination of values. This is the underlying idea of specification based behavioral rule IDS.

Below shows how a behavior specification based rules are used to derive a state machine for the MCPS.

3.2.1 Identify Attack States. A compromised sensor undergoing an attack embedded in MCPS will often drive MCPS to attack behavior indicators. There are normally four attack states for the device Patient Controlled Analgesia(PCA) as a result of violating four behavioral rules[17]. For example, the first attack state of PCA is that patient gives additional request for analgesic but has a pulse below a specified threshold. This could bring an overdose of analgesic to blood stream using PCA and can bring severe harm to the patient. It can be clearly noted that if the PCA receives additional request, then an intruder is involved in it.In this manner all attack states for every device involved in MCPS are identified.

3.2.2 Express Attack state indicators in Conjunctive Normal Form. The attack state indicators of MCPS system is expressed in conjunctive normal form. Each attack state indicator may consist of different state variables.

3.2.3 Consolidate Predicates in Disjunctive Normal Form. For each sensor/actuator device, it combine the attack states using a boolean expression into disjunctive normal form.

3.2.4 Identify State Components and Component Ranges. Next step is to transform the union of all predicate variables into the state components of state machine. Finally, their corresponding ranges are also established[18].

3.2.5 Manage State Space. The number of states thus formed from the previous step will be too large for an automaton to handle. So the number of states should be managed which is done by state collapsing. This can be done by identifying and tagging values that comes under one name that have a literal meaning to it. For eg values from 80 to 100 can be tagged under keyword ”high”.

So the main idea behind is that the Medical Cyber Physical System will only enter an unsafe state (common for all attacks) only when it is seen to deviate from the normal behaviour specified by the behaviour rules

4. CONCLUSION

From the comparative analysis on the various Intrusion detection techniques in cyber physical systems, it is concluded that the specification based intrusion detection is a highly viable method for the detection of intrusion attack, most commonly unknown attacks. Since the area of cyber physical systems are being developed in a high rate, security professional often meets new attacks very often. It is also established that the probabilities of finding an attacker in the system is higher than what is achieved by using other intrusion detection methods. The comparison between various intrusion detection methods will allow security professionals to effectively and efficiently find best technique that suits a particular system or organization . It can also assist in making acceptable tradeoffs among sometimes conflicting goals such as True Positives, True Negatives, False positives and False negatives and to allocate valuable sensor/actuator energy resource based on the security requirements.

5. REFERENCES

[1] K. Park, Y. Lin, V. Metsis, Z. Le, and F. Makedon. Abnormal human behavioral pattern detection in assisted living environments. In 3rd ACM International Conference on Pervasive Technologies Related to Assistive Environments, pages 9:19:8, 2010.

[2] E. Tapia, S. Intille, and K. Larson. Activity recognition in the home using simple and ubiquitous sensors. In A. Ferscha and F. Mattern, editors, Pervasive Computing, volume 3001 of Lecture Notes in Computer Science, pages 158175. Springer Berlin / Heidelberg, 2004.

[3] C.-H. Tsang and S. Kwong. Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction. In IEEE International Conference on Industrial Technology, 2005., pages 5156, December 2005.

[4] A. Carcano, A. Coletta, M. Guglielmi, M. Masera, I. Fovino, and A. Trombetta. A multidimensional critical state analysis for detecting intrusions in scada systems. IEEE Transactions on Industrial Informatics, 7(2):179 186, May 2011.

[5] H. Al-Hamadi and I. R. Chen. Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks. IEEE Transactions on Network and Service Management, 10(2):189203, 2013.

[6] I. Lee and O. Sokolsky. Medical cyber physical systems. In 47th ACM Design Automation Conference, pages 743748, 2010.

[7] R. Mitchell and I. R. Chen. Effect of Intrusion Detection and Response on Reliability of Cyber Physical Systems. IEEE Transactions on Reliability, 62(1):199210, March 2013.

[8] S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, and A. Valdes. Using model-based intrusion detection for SCADA networks. In SCADA Security Scientific Symposium, pages 127134, Miami, FL, USA, January 2007.

[9] B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam. Host-based anomaly detection for pervasive medical systems. In Fifth International Conference on Risks and Security of Internet and Systems, pages 18, October 2010.

[10] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee. Security challenges in next generation cyber physical systems. Beyond SCADA: Networked Embedded Control for Cyber Physical Systems, 2006.

[11] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sast ry. Challenges for securing cyber physical systems. In First Workshop on Cyber-physical Systems Security, DHS, 2009.

[12] I. R. Chen and D. C. Wang. Analysis of replicated data with repair dependency. The Computer Journal, 39(9):767779, 1996.

[13] M. Aldebert, M. Ivaldi, and C. Roucolle. Telecommunications Demand and Pricing Structure: An Econometric Analysis. Telecommunication Systems, 25:89115, 2004.

[14] S. M. Ross. Introduction to Probability Models, 10th Edition. Academic Press, 2009.

[15] P. Porras and P. Neumann. EMERALD: Event monitoring enabling responses to anomalous live disturbances. In 20th National Information Systems Security Conference, pages 353365, 1997.

[16] F. Bao, I. R. Chen, M. Chang, and J. H. Cho. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to TrustBased Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, 9(2):169183, 2012.

[17] I. R. Chen and D. C. Wang. Analyzing Dynamic Voting using Petri Nets. In 15th IEEE Symposium on Reliable Distributed Systems, pages 4453, Niagara Falls, Canada, October 1996.

[18] C. Hsu. Many popular medical devices may be vulnerable to cyber attacks. http://www.medicaldaily.com/news/20120410/9486/medical-implants-pacemaker-hackers-cyber-attack-fda.htm, April 2012.