ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Survey on Secure Medical Cyber Physical System Based on Behavior Rule Specification

Manasi Kadam, Bhagyashree Patle

Department of Computer Engineering, SKNSITS, Lonavala, India

Asst. Professor, Department of Computer Engineering, SKNSITS, Lonavala, India

ABSTRACT: Behavior-rule specification-based technique is analyzed for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) where patient's safety is of the utmost importance. Medical cyber physical system(MCPS) are used as tool for cyber attacks.This can relatively harm the patient or may even cause a direct or indirect threat to life. Intrusion detection technique helps to detect secret attackers to support safe and secure MCPS applications. Along with this using comparative analysis, we demonstrate that our behavior-rule specification-based IDS technique performs two existing anomaly-based techniques for detection of abnormal patient behaviors in medical applications

KEYWORDS: Intrusion detection, Sensors, Actuators, Medical cyber physical systems, Security

I. INTRODUCTION

Medical Cyber Physical System is used in advanced healthcare hospitals to do any complicated tasks.This system can analyze the patient status using physical sensors and perform corresponding action 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. Medical Cyber Physical System becomes a tool for cyber attacks.

IDS is used to detect unknown attack/attacker patterns. IDS Uses behavioral rule specification for this purpose. MCPS sensor/actuator networks are highly resource constrained. Therefore To enclose an intrusion detection system in MCPS sensor/actuator networks is difficult.To overcome this problem a new methodology for intrusion detection is introduced which is based on behavioral rule specifications which utilizes behavioral rules for defining normal behavioral patterns for a medical device. These behavioral patterns represent acceptable behaviors of that particular CPS. 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 Basic difference between creating an IDSs for medical devices and other systems is that the attacker may attack the physical component rather than the network or communication protocols. Thus IDS should be closely coupled with the physical equipment of the Cyber Physical System. IDSs for MCPSs may test medical sensor measurements and actuator settings to detect misbehavior of physical properties visible because of attacks.

II. RELATED WORK

The mixture of embedded software controlling the devices, networking capabilities, and complicated physical dynamics that patient bodies reveal makes modern medical device systems a distinct class of cyber-physical systems, which is referred as medical CPS(MCPS)[2]. In the context of intrusion detection for MCPSs or healthcare systems, Asfaw et al. studied an anomaly-based IDS for MCPSs. The authors studied attacks that violate privacy of an MCPS[3]. a trust-based IDS scheme giving a hierarchical trust management protocol for Wireless Sensor Networks is used. A composite trust metric deriving from both social trust (honesty) and QoS trust (energy and coop-erativeness) as an indicator of maliciousness is considered. A probability model based on stochastic Petri nets techniques to describe the behaviors of Sensor Networks or Cluster Heads for trust evaluation and intrusion detection, as well as a statistical method to predict the false alarm probabilities of the trust-based IDS scheme. The experimental results shows that a node with high compromising rate can be easily detected, thus supporting the idea of using trust to implement IDS

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

functionality[4]. trust-based IDS algorithm contains traditional anomaly-based IDS techniques for the detection while maintaining sufficiently low false positives[5].A probability model is developed to analyze the reliability of a cyber physical system (CPS) containing harmful nodes showing attacker behaviors and an intrusion detection and response system for identifying and giving response to malicious events at runtime. For each attacker behavior,The best detection strength, and the best response strength is identified under which the reliability of the system may be maximized[6].

III.SYSTEM ARCHITECTURE

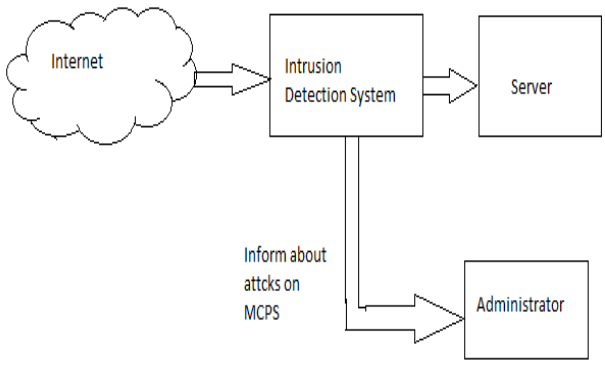

Fig 1. Architecture of system

Fig.above shows architecture of the system.In this system, there is intrusion detection system which is based on behavior rules. This system will prevent medical cyber physical system from any unauthorised access. If there is any unauthorised access then it will inform about this attack to the administrator. Medical cyber physical system is the main system which may be attacked by unknown attacker.

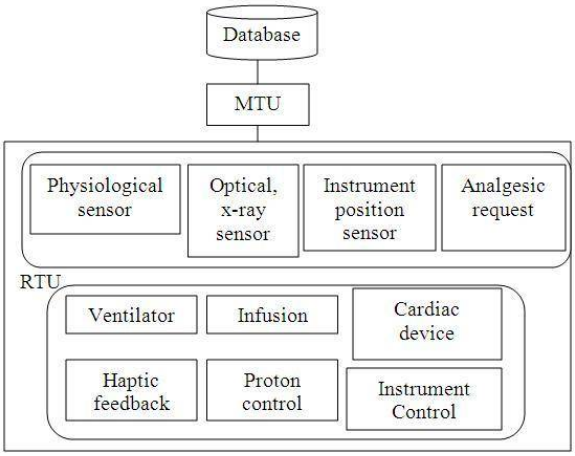

FIG.2 MEDICAL CYBER PHYSICAL SYSTEM

Medical cyber physical system has three types of sensor/actuator devices.vital sign monitor, patient controlled analgesia and cardiac device . Vital sign monitor is a device which is used to monitor vital signs i.e. signs of life specifically the pulse rate, body temperature and blood pressure. Patient controlled analgesia is a method which allows a person in pain to manage their own pain relief. The infusion is programmable by the prescriber. Cardiac device is an electronic device that constantly checcks the patients heart rhythm. The attacker can attack any of these three devices.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

Specifically, insulin pumps and cardiac devices are more vulnerable. The attacks on MCPS can be done by third party software providers.

BEHAVIOR RULE BASED IDS

Behavior rule	Trustee	Monitor
Pulse above threshold during analgesic request	PCA	VSM
Respiration above threshold during analgesic request	PCA	VSM
Pulse matches pacemaker frequency	CD	VSM
Patient is unstable before defibrillation	CD	VSM
Trustee pulse matches Monitor	VSM	Peer VSM
Trustee temperature matches Monitor	VSM	Peer VSM

Table 1:Behavior Rules

Behavior rules are specified for all three devices of MCPS namely PCA,CD,VSM. Behavior rules are specified during the design and testing phase of an MCPS. The intrusion detection protocol takes a set of behavior rules for a device as input and detects whether a device's behavior differs from the expected behavior specified by the set of behavior rules.The behavior rule set gives expected normal behaviors for each device and can detect deviation of normal behaviors regardless of the attacker's patterns.

For the PCA device, there are two attack states as a result of violating the two PCA behavior rules listed in Table 1.The first PCA attack state is that a patient requesting analgesic has a pulse below some threshold. One way an attacker could exploit this is to cause an overdose of analgesic delivered by a PCA system. A patient will lose consciousness after receiving a sufficient amount of analgesic, if the PCA receives additional requests for analgesic, then an intruder is involved.The second PCA attack state is that a patient requesting analgesic has a respiration rate below some threshold. A compromised PCA device performing this attack will drive the MCPS into this state. One way an attacker could exploit this is to cause an overdose of analgesic delivered by a PCA system. A patient will lose consciousness after receiving a sufficient amount of analgesic; if the PCA receives additional requests for analgesic, then an intruder is involved.For the CD device, there are two attack states. The first CD attack state is that pulse average is not equal to CD frequency when acting as a pacemaker. One way an attacker could exploit this is to change the pacemaker frequency. If the CD frequency when acting as a pacemaker is substantially different from the patient's heart rate, then an intruder is involved.The second CD attack state is that pulse average is within a normal range when the CD enters defibrillator mode. One way an attacker could exploit this is to defibrillate a stable patient. If the CD enters defibrillator mode unnecessarily, then an intruder is involved.For the VSM device, there are five attack states in which a trustee sensor reading (blood pressure, oxygen saturation, pulse, respiration, or temperature) is beyond 100 percent of the corresponding monitor sensor reading.

IV. ALGORITHM

Naive Baysian Classification Algorithm

1. Let D=Training data set i.e. data taken by user.
2. x=Each tuple in data set
3. Let c1,c2 are classes where c1=Patient,c2=attacker
4. The naïve base classifier will predict that x belongs to the class having highest posterior probability conditioned on x.
5. The naïve bayesian classifier predicts that tuple x belongs to the class Ci if and only if

$$P(Ci|x)>P(Cj|x) \quad \text{for } 1<=j<=m,\ j=i$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2016

6. Maximize P(Ci|x). The class Ci for which P(Ci|x) is maximized is called maximum posterior hypothesis. By Bayes theroem,

$$P(Ci|x)=\frac{P(x|Ci).\ P(Ci)}{P(x)}$$

V. CONCLUSION AND FUTURE WORK

For safety-critical MCPSs a behavior-rule specification-based IDS technique is used for intrusion detection of medical devices contained in a MCPS.In future, plan is to analyze the overheads of current detection techniques by using comparison with contemporary approaches.

REFERENCES

1. Robert Mitchell and Ing-Ray Chen, Member, IEEE, "Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems", IEEE transactions on dependable and secure computing, vol. 12, no. 1,pp.16-30, january/february 2015.
2. I. Lee and O. Sokolsky, "Medical cyber physical systems", in Proc. 47th ACM Des. Autom. Conf, pp. 743-748, 2010.
3. B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam, " Host-based anomaly detection for pervasive medical systems" , in Proc. 5th Int. Conf. Risks Security Internet Syst., pp.1-8, Oct. 2010.
4. F. Bao, I. Chen, M. Chang, and J.H. Cho, " Trust-based intrusion detection in wireless sensor networks", in Proc. IEEE Int. Conf. Commun, pp. 16, Jun. 2011.
5. F. Bao, I. R. Chen, M. Chang, and J. H. Cho, " Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", IEEE Trans. Netw. Service Manage., vol. 9, no. 2, pp. 169183, Jun. 2012.
6. Ms. Simrandeep Kaur chana, Prof S.J.Karale, " Analysis of Intrusion Detection Response System (IDRS) In Cyber Physical Systems (Cps) Using Regular Expression (Regexp) ", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, PP 120-125, Ver. XI (Mar-Apr. 2014).

BIOGRAPHY

Manasi Kadam have completed Bachelors in Information Technology Engineering(BE) from Finolex Academy of Management and Technology, Mumbai university and currently pursuing ME in computers from SKNSITS, Lonavala. My research interests are Cyber Security, Data mining,Database technologies, Software Project Manage-ment, Software Testing and Software Engi-neering.

Bhagyashree Patle working as an assistant professor at SKNSITS,Lonavala My research interests are Data mining and information retrieval, Software Architecture and Software Engineering.