Security for Medical Cyber Physical System

Manasi R. Kadam[1] , Vikas Thombre [2]

[1]Computer Engineering Department, SKNSITS, Lonavala, India

[2]Professor, Computer Engineering Department, SKNSITS, Lonavala, India

ABSTRACT

Nowadays Medical Cyber Physical System is available in almost every advanced hospital to make complicated tasks easy. These systems has physical sensors to check the patient status and actuators to respond accordingly. 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.These systems are used as a tool for cyber attacks. These attacks may harm the patient. In existing system,behavioral rule specification based Intrusion detection system is used to detect unknown attacker. This system can only detect the attacks on Medical Cyber Physical system. There is no any technique to prevent the attack on the system. This problem is overcome in proposed system. In Proposed system, additional forms of security is provided to protect Medical Cyber Physical System and their customers from unauthorized access.In the event that unauthorized individuals gain access to sensitive data, system turns towards data encryption to safeguard the data itself. Encryption is a way of disarranging data in such a way that without a key to rearrange it (or decrypt it), the data is unreadable. Encryption is used to reversibly randomize the data to make it unreadable to unauthorized individuals. With the help of encryption key, attacks on Medical Cyber Physical System are successfully prevented.

Keywords*-Medical cyber physical systems,Intrusion Detection System, Security, Encryption.*

---

1. INTRODUCTION:

Medical device industry has quick transformation, including the potential of embedded software and network connectivity.Medical Cyber Physical System(MCPS) is a special class of modern medical device systems that contains the embedded software controlling the devices, networking capabilities..There are particularly three types of sensor/actuator devices present in this MCPS. 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. Cardiac device is an electronic device that constantly monitors the patients heart rhythm. The attacker can attack any of these three devices. Specifically, insulin pumps and cardiac devices are more vulnerable. Critical medical devices connected to a patient is highly vulnerable to cyber attacks.Cyber criminals may targets these devices and may initiate an attack. Detecting an attacker in MCPS is very difficult job. Therefore intrusion detection is required to protect the integrity of MCPS.A new methodology that is behavioral rule specification based Intrusion detection is used which contains behavioral rules that gives normal behavioral patterns for a medical device.These behavioral patterns represent acceptable behaviors of that particular CPS. These behavioral rules are then converted to state machines so that any changes from normal state to an unsafe state can be easily recognised. This ids is also very useful to identify more complex and invisible attackers.

Along with the detection of attacks on system, prevention of attacks is also important. Attack prevention provides additional forms of security to protect the system and their customers from unauthorized access.Encryption is useful to reversibly randomize the data to make it unreadable to unauthorized individuals.Encryption is a type of security that converts data, programs, images or other information into unreadable cipher. This is done by using a collection of complex algorithms to the original content meant for encryption.An encryption key is a random string of bits created explicitly for

scrambling and unscrambling data. Encryption keys are designed with an algorithm to ensure that each & every key is unpredictable and unique.

An encryption key is used to encrypt as well as to decrypt, or to perform both functions, based on the encryption software used. In Symmetric forms of encryption, single password is used for both decryptor and encryptor. Symmetric types use algorithms that are very safe. Public asymmetric encryption systems use more secured algorithms,and it uses different techniques for encryption and decryption. The asymmetric encryption method uses two keys.One is a public key, and the other one is a private key. The public key is used for encryption and it can be freely shared among various users whereas the private key is not shared, and is used for decryption.

2.LITERATURE REVIEW

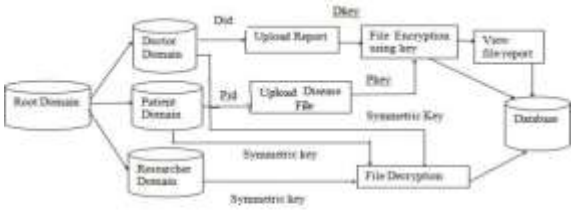
In the base paper.i.e. Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems, the author has proposed the idea about attack detection based on behavior rule specification method for medical devices embedded in a medical cyber physical system (MCPS) in which the patients safety is of the utmost importance.Author has proposed a methodology to transform behavior rules to a state machine, so that behavior of a device being monitored can easily be checked against the transformed state machine for variation from its behavior specification.[1]In the paper of Medical Cyber Physical Systems,author has given the detail information about MCPS which is the main system in the proposed work.The Author has discussed current trends in the development and use of high-confidence medical cyber-physical systems(MCPS).[2] In the paper of Host-Based Anomaly Detection for Pervasive Medical Systems,the author has proposed a contribution to provide a host-based, anomaly modeling and detection approach based on data mining techniques for pervasive healthcare systems. The technique maintains normal usage profile of pervasive healthcare applications and inspects current workflow against normal usage profile so as to classify it as anomalous or normal.[3]In the paper of Security Issues and Challenges for

Cyber Physical System,the author has represented the abstract the general workflow of cyber physical systems, identified the possible vulnerabilities, attack issues, adversaries characteristics and a set of challenges that need to be Addressed and then proposed a context-aware security framework for general cyber-physical systems and suggest some potential research areas and problems.[4]The paper of Cyber Physical Systems Security: A Brief Survey, mainly focuses on the security requirements of CPS systems , security objectives and threats , major attacks on CPS and finally the discussion of the key areas where security of these systems are required and survey of the main security work that has been carried out in this domain.[5].In the paper of DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis,the author has provided a fair comparison between three most common symmetric key cryptography algorithms: DES, AES, and Blowfish. Since main objective is to check working of algorithms under different settings, the comparison is done regarding the behavior and the performance of the algorithm when different data loads are used. The comparison is made using the parameters namely speed, block size, and key size. [6] In the paper of Secure Control: Towards Survivable Cyber-Physical Systems,the author has identified the problem of secure control,investigated the defenses that information security and control theory can provide, and proposed a set of challenges that need to be addressed to improve the survivability of cyber-physical systems.[7]

3. MOTIVATION

Critical medical devices connected to a patient are highly vulnerable to cyber attacks. Cyber criminals may target 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.Intrusion detection in such systems is necessary to protect the integrity of MCPS.Behavioral rule specification-based method is useful to embed Intrusion detection system in MCPS sensors/actuators.IDSs for MCPSs may test medical sensor measurements and actuator settings for misbehavior detection of physical properties manifested because of attacks.Along with the detection of attacks on system, prevention of attacks is also important. Attack prevention provides additional forms of security to protect the system and their customers from unauthorized access.Encryption is useful to reversibly randomize the data to make it unreadable to unauthorized individuals.

4. PROPOSED APPROACH



The Medical Cyber Physical System is a special class of cyber physical system that contains embedded software controlling the devices, networking capabilities. There are three types of sensor/actuator devices present in this MCPS. 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 monitors the patients heart rhythm. The attacker can attack any of these three devices. Specifically, insulin pumps and cardiac devices are more vulnerable. The attacks on MCPS can occur through the air software updates, stack buffer overflow exploits or logic bombs planted by third party software providers.Critical medical devices connected to a patient is highly vulnerable to cyber attacks.Cyber criminals may targets these devices and may initiate an attack. Detecting an attacker in MCPS is very difficult job. Therefore intrusion detection is required to protect the integrity of MCPS. Along with the detection of attacks on system, prevention of attacks is also important. Attack prevention provides additional forms of security to protect the system and their customers from unauthorized access.Encryption is useful to reversibly randomize the data to make it unreadable to unauthorized individuals.Encryption is a type of security that converts data, programs, images or other information into unreadable cipher. This is done by using a collection of complex algorithms to the original content meant for encryption.An encryption key is a random string of bits created explicitly for scrambling and unscrambling data. An encryption key is used to encrypt, decrypt, or carry out both function.An encryption is provided to patient files as well as reports to prevent the attacks on them.

4.1 ALGORITHM

1) Browse file and write file details.
2) K=create encryptor

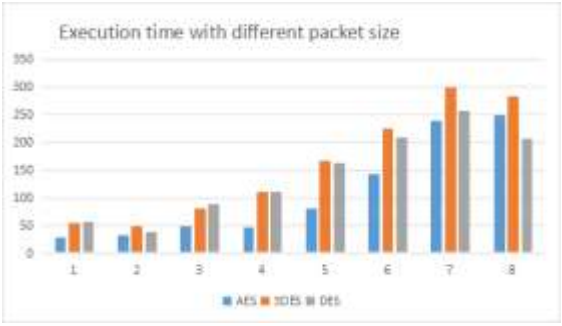
   Generate key=create encryptor(key,key)
3) Open file mode

   Filestream=filemode.open

   While((data=FsIn.ReadByte())!=-1)

   FsIn=filestream
4) Write databyte
5) Close file.
6) File encrypted.

5. RESULT ANALYSIS



6. CONCLUSION AND FUTURE WORK

For safety of critical Medical Cyber Physical System, being able to prevent attackers from attacking the system to protect the welfare of patients is of utmost importance. The proposed system provides encryption to the patients files as well as report generated by doctor. So. Attackers or any unauthorized person cannot access these files or reports. As a result, the medical cyber physical system gets fully secured.

In future, we intend to focus on making the algorithm simpler and more efficient along with making it even more suitable for access control.

ACKNOWLEGMENT

It gives me great pleasure to deliver sincere thanks to my project guide Prof. V.D.Thombre for his valuable guidance, constant encouragement and support. I appeal thanks to all the authors of the referenced papers as they help me and motivate me to work on this emerged area. Last but not least, I would like to deliver thanks to my family members, my colleague, and the people who directly or indirectly support me in this project work.

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, January/February 2015

2.Insup Lee, Oleg Sokolsky, Medical Cyber Physical Systems, 47th Design Automation Conference (DAC '10) , 743-748. June 2010.

3.B. Asfaw, D. Bekele, B. Eshete, A. Villafiorita, and K. Weldemariam, Host-based anomaly detection for pervasive medical systems, Proc.5th Int. Conf. Risks Security Internet Syst.,Oct.2010, pp. 18.

4.Eric Ke Wang,Yunming Ye, Xiaofei Xu, Security Issues and Challenges for Cyber Physical System, 2010 IEEE/ACM International Conference on Cyber, Physical and Social Computing.

5.Qaisar Shafi, Cyber Physical Systems Security: A Brief Survey , 2th International Conference on Computational Science and Its Applications,2012.

6.Jawahar Thakur, Nagesh Kumar ,DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis, International Journal of Emerging Technology andAdvanced Engineering,(ISSN 2250-2459, Volume 1, Issue 2, December 2011).

7.Alvaro A. C´ardenas Saurabh Amin Shankar Sastry University of California, Berkeley, Secure Control: Towards Survivable Cyber-Physical Systems in The 28th International Conference on Distributed Computing Systems Workshops.

8.H. Al-Hamadi and I. R. Chen, Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensor networks, IEEE Trans. Netw. Service Manage., vol. 10, no. 2, pp. 189203, June. 2013

9.F. Bao, I. Chen, M. Chang, and J.H. Cho,Trust-based intrusion detection in wireless sensor networks, in Proc. IEEE Int. Conf. Commun,Jun. 2011, pp.1-6

10.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.

BIOGRAPHY

Vikas Thombre, I have completed Bachelors in Computer Engineering (BE) from Government College Of Engineering, Aurangabad and masters (MTECH) in computer engg., from Dr. Babasaheb Ambedkar Technological University, Lonere. Currently, I am working as an assistant professor and HOD at SKNSITS, Lonavala with total experience of 11 years. My research interests are Data mining and information retrieval, Software Architecture and Software Engineering.

Manasi Rajendra Kadam.

I have completed Bachelors in Information Technology from Finolex Academy of Management &Technology College, Ratnagiri affiliated by Mumbai University and currently pursuing ME in computers from SKNSITS, Lonavala. My research interests are Cyber Security, Database technologies, Software Project Management and Software Engineering.