ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Detection of Intrusions by Using Behaviour Rule Specification Based Technique for Providing Security to MCPSs

Jameela Jahan
M.Tech,CN,
Shadan Women's College of Engineering & Technology, Khairatabad.

Ms. Shilpa Karre
Assosicate Professor,
Department of CSE,
Shadan Women's College of Engineering & Technology, Khairatabad.

Ms. Saleha Farha
HOD,
Department of CSE,
Shadan Women's College of Engineering & Technology, Khairatabad.

ABSTRACT:

In this dissertation research we aim to design and validate intrusion detection system (IDS) protocols for a medical cyber physical system (MCPS) comprising sensors, actuators, control units, and physical objects for controlling and protecting physical infrastructures. The design part includes host IDS, system IDS and IDS response designs. The validation part includes a novel model-based analysis methodology with simulation validation. Our objective is to maximize the MCPS reliability or lifetime in the presence of malicious nodes performing attacks which can cause security failures. Our host IDS design results in a lightweight, accurate, autonomous and adaptive protocol that runs on every node in the CPS to detect misbehavior of neighbor nodes based on state-based behavior specifications. Our system IDS design results in a robust and resilient protocol that can cope with malicious, erroneous, partly trusted, uncertain and incomplete information in a MCPS. Our IDS response design results in a highly adaptive and dynamic control protocol that can adjust detection strength in response to environment changes in attacker strength and behavior. The end result is an energy-aware and adaptive IDS that can maximize the MCPS lifetime in the presence of malicious attacks, as well as malicious, erroneous, partly trusted, uncertain and incomplete information.We develop a probability model based on stochastic Petri nets to describe the behavior of a MCPS incorporating our proposed intrusion detection and response designs, subject to attacks by malicious nodes exhibiting a range of attacker behaviors, including reckless, random, insidious and opportunistic attacker models. We identify optimal intrusion detection settings under which the MCPS reliability or lifetime is maximized for each attacker model.

Adaptive control for maximizing IDS performance is achieved by dynamically adjusting detection and response strength in response to attacker strength and behavior detected at runtime. We conduct extensive analysis of our designs with four case studies, namely, a mobile group CPS, a medical CPS, a smart grid MCPS and an unmanned aircraft MCPS. The results show that our adaptive intrusion and response designs operating at optimizing conditions significantly outperform existing anomaly-based IDS techniques for MCPS.

keywords:

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

INTRODUCTION:

The most prominent characteristic of a medical cyber physical system (MCPS) is its feedback loop that acts on the physical environment[3][4]. In other words, the physical environment provides data to the MCPS sensors whose data feed the MCPS control algorithms that drive the actuators which change the physical environment. MCPSs are often characterized by sophisticated patient treatment algorithms interacting with the physical environment including the patient. In this paper, we are concerned with intrusion detection mechanisms for detecting compromised sensors or actuators embedded in an MCPS for supporting safe and secure MCPS applications upon which patients and healthcare personnel can depend with high confidence. Intrusion detection system (IDS) design for cyber physical systems (CPSs)[13][14] has attracted considerable attention because of the dire consequence of [3]CPS failure.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

However, IDS techniques for MCPSs is still in its infancy with very little work reported. Intrusion detection techniques in general can be classified into four types: signature, anomaly, trust, and specification-based techniques. In this paper, we consider specification rather than signature-based detection to deal with unknown attacker patterns. We consider specification rather than anomaly based techniques to avoid using resource constrained sensors or actuators in an [3]MCPS for profiling anomaly patterns (e.g., through learning) and to avoid high false positives. We consider specification rather than trust based techniques to avoid delay due to trust aggregation and propagation to promptly react to malicious behaviors in safety critical MCPSs.

To accommodate resource-constrained sensors and actuators in an MCPS, we propose behavior-rule specification-based [13]intrusion detection (BSID) which uses the notion of behavior rules for specifying acceptable behaviors of[3] medical devices in an MCPS. Rule-based intrusion detection thus far has been applied only in the context of communication networks which have no concern of physical environments and the closed-loop control structure as in an [13]MCPS. For example, propose an IDS that applies seven types of traffic-based rules to detect intruders[1]: interval, retransmission, integrity, delay, repetition, radio transmission range and jamming. propose a multitrust[3] IDS with traffic-based collection that audits the forwarding behavior of suspects to detect black hole and keyhole attacks launched by captured devices based on the rate of specification violations.

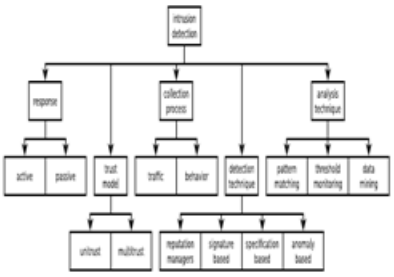


Fig:- Classification Tree for CPS Intrusion Detection Techniques.

We classify the intrusion detection literature based on four criteria (or dimensions):

1. Detection Technique: this criterion distinguishes IDSs based on their basic approach to detection analysis;[3]

2. Collection Process: this criterion contrasts behavior-based IDSs from traffic-based IDSs;

3. Trust Model: this criterion differentiates IDSs that share raw data or analysis results from standalone IDSs;[6]

4. Response Technique: this criterion contrasts active from passive and static from dynamic approaches to repelling an attack[1].

Our intrusion detection is characterized by false negative and positive probabilities, denoted by pfn and pfp, respectively. A false negative occurs when a bad medical [4]device is missed as good, while a false positive occurs when a good medical device is misdiagnosed as bad. While neither is desirable, a false negative in an MCPS is especially impactful to the patient's well being. Because the key motivation in MCPS is safety, we searched for a configuration yielding a high detection rate without compromising the false positive probability. In this paper we consider a threshold criterion.

RELATED WORK:

Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

We have to analysis the Secure Computing Survey:

Secure Computing:

Secure Computing Corporation, or SCC, was a public company (NASDAQ: SCUR) that developed and sold computer security[14] appliances and hosted services to protect users and data. McAfee acquired the company in 2008. Computer security[14] is the effort to create a secure computing platform, designed so that agents (users or programs) cannot perform actions that they are not allowed to perform, but can perform the actions that they are allowed to. This involves specifying and implementing a security policy.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The actions in question can be reduced to operations of access, modification and deletion. Computer security can be seen as a subfield of security engineering, which looks at broader security issues in addition to computer security.It is important to understand that in a secure system, the legitimate users of that system are still able to do what they should be able to do. It has been said pejoratively that the only truly secure computer is one locked in a vault without any means of power or communication; however, this would not be regarded as a useful secure system because of the above requirement.It is also important to distinguish the techniques employed to increase a system's security from the issue of that system's security[14] status. In particular, systems which contain fundamental flaws in their security designs cannot be made secure without compromising their utility. Consequently, most computer systems cannot be made secure even after the application of extensive "computer security" measures.

Techniques for creating secure systems:

1. Cryptographic techniques can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.

2. Strong authentication techniques can be used to ensure that communication end-points are who they say they are.

3. Secure crypto processors can be used to leverage physical security techniques into protecting the security of the computer system.

4. Chain of trust techniques can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.

Next Generation Secure Computing Base:

(Next Generation Secure Computing Base) A Windows security platform from Microsoft introduced in 2002, and originally called "Palladium." First used in Windows Vista in 2007, applications that support NGSCB can be isolated within the computer; their data can be sealed and made unavailable to other applications, and data can be digitally signed to ensure they were created by a trusted application. Viruses may still enter and reside within the computer, but NGSCB-aware applications are far less vulnerable to their damage.

EXISTING SYSTEM:

Existing work only considered specification-based state machines for intrusion detection of communication protocol misbehaving patterns. Before that not using trust based techniques to avoid delay due to trust aggregation and propagation to promptly react to malicious behaviors in safety critical MCPSs.

PROPOSED SYSTEM:

We propose a methodology to transform behaviour rules to a state machine, so that a device that is being monitored for its behaviour can easily be checked against the transformed state machine for deviation from its behaviour specification. We also investigate the impact of attacker behaviors on the effectiveness of MCPS intrusion detection. We demonstrate that our specification based IDS technique can effectively trade higher false positives off for lower false negatives to cope with more sophisticated and hidden attackers. We show results for a range of configurations to illustrate this trade. Because the key motivation in MCPS is safety, our solution is deployed in a configuration yielding a high detection rate without compromising the false positive probability. Our approach is monitoring-based relying on the use of peer devices to monitor and measure the compliance degree of a trustee device connected to the monitoring node by the CPS network. The rules comparing monitor and trustee physiology (blood pressure, oxygen saturation, pulse, respiration and temperature) exceeds protection possible by considering devices in isolation.

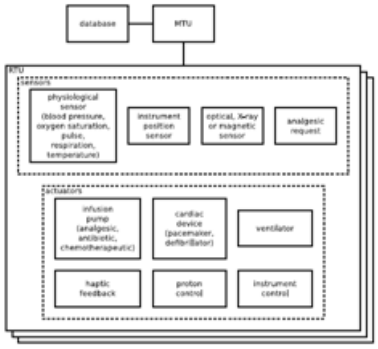
Algorithm:
IDS techniques:

We demonstrate that our behaviour-rule specification based IDS technique outperforms two existing anomaly-based techniques for detecting abnormal patient behaviors in pervasive healthcare applications.

Anomaly-based techniques using statistical analysis: one studies user sessions (to detect live intruders), and the other studies the runtime behaviour of programs (to detect malicious code). We propose semi-supervised anomaly-based IDS targeted for assisted living environments. Their design is behaviour-based and audits series of events which they call episodes. The authors' events are 3-tuples comprising sensor ID, start time and duration.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SYSTEM ARCHITECTURE:



IMPLEMENTATION:

1.Threat Model:

We focus on defeating inside attackers that violate the integrity of the MCPS with the objective to disable the MCPS functionality. Our design is also effective against attacks such as subtle manipulations that change medical doses slightly to cause long term harm to patients or medical or billing record exhilarations which violate privacy[4]. There are two distinct stages in an attack: before a node is compromised and after a node is compromised. Before a node is compromised, the adversary focuses on the tactical goal of achieving a foothold on the target system.

2. Attacker Archetypes:

We differentiate two attacker archetypes: reckless, random and opportunistic. A reckless attacker performs attacks whenever it has a chance to impair the MCPS functionality as soon as possible. A random attacker, on the other hand, performs attacks only randomly to avoid detection. It is thus insidious and hidden with the objective to cripple the MCPS functionality. We model the attacker behaviour by a random attack probability pa. When pa = 1 the attacker is a reckless adversary. Random attacks are typically implemented with on off attacks in real-world scenarios, so pa is not a random variable drawn from uniform distribution U(0, 1) but rather a probability that a malicious node is performing attacks at any time with this on-off attack behaviour. An opportunistic attacker is the third archetype. An opportunistic attacker exploits ambient noise modelled by per (probability of miss-monitoring)to perform attacks.

3. Behavior Rules:

Behavior rules for a device are specified during the design and testing phase of an MCPS. Our intrusion detection protocol takes a set of behaviour rules for a device as input and detects if a device's behaviour deviates from the expected behaviour specified by the set of behaviour rules. Since the intrusion detection activity is performed in the background, it allows behaviour rules to be changed if incomplete or imprecise specifications are discovered during the operational phaseWithout disrupting the MCPS operation. Our IDS design for the reference MCPS model relies on The use of lightweight specification-based behaviour rules for each sensor or actuator medical device.

4. Intrusion detection system:

Intrusion detection system (IDS) design for cyber physical systems (CPSs) has attracted considerable because of the dire consequence of CPS failure. In this paper, we consider specification rather than signature-based detection to deal with unknown attacker patterns. We consider specification rather than anomaly based techniques to avoid using resource constrained Sensors or actuators in an MCPS for profiling anomaly patterns (e.g., through learning) and to avoid high false positives. We consider specification rather than trust based techniques to avoid delay due to trust aggregation and propagation to promptly react to malicious behaviours in Safety critical MCPSs.

CONCLUSION:

For safety-critical MCPSs, being able to detect attackers while limiting the false alarm probability to protect the welfare of patients is of utmost importance. In this paper we proposed a behaviour-rule specification-based IDS technique for intrusion detection of medical devices embedded in a MCPS. We exemplified the utility with VSMs and demonstrated that the detection probability of the medical device approaches one (that is, we can always catch the attacker without false negatives) while bounding the false alarm probability to below 5% for reckless attackers and below 25% for random and opportunistic attackers over a wide range of environment noise levels. Through a comparative analysis, we demonstrated that our behaviour-rule specification-based IDS technique outperforms existing techniques based on anomaly intrusion detection.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

FUTURE WORK:

In future work, we plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches. We also plan to deepen adversary modelling research based on stochastic Petri net techniques such that the system can dynamically adjust CT to maximize intrusion detection performance in response to changing attacker behaviours at runtime.

REFERENCES:

[1] H. Al-Hamadi and I. R. Chen. Redundancy management of multipath routing for intrusion tolerance in heterogeneous wireless sensornetworks. IEEE Transactions on Network and Service Management, 10(2):189–203, 2013.

[2] M. Aldebert, M. Ivaldi, and C. Roucolle. Telecommunications Demand and Pricing Structure: An Econometric Analysis. Telecommunication Systems, 25:89–115, 2004.

[3] 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.

[4] 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 1–8, October 2010.

[5] F. Bao, I. R. Chen, M. Chang, and J. H. Cho. Hierarchical Trust Management forWireless Sensor Networks and its Applications to Trust- Based Routing and Intrusion Detection. IEEE Transactions on Network and Service Management, 9(2):169–183, 2012.

[6] 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.

[7] A. C´ardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry. Challenges for securing cyber physical systems. In First Workshop on Cyber-physical Systems Security, DHS, 2009.

[8] I. R. Chen and T. H. Hsi. Performance analysis of admission control algorithms based on reward optimization for real-time multimedia servers. Performance Evaluation, 33(2):89–112, 1998.

[9] I. R. Chen, A. P. Speer, and M. Eltoweissy. Adaptive fault tolerant qos control algorithms for maximizing system lifetime of query-based wireless sensor networks. IEEE Transactions on Dependable and Secure Computing, 8(2):161–176, 2011.

[10] I. R. Chen and D. C. Wang. Analysis of replicated data with repair dependency. The Computer Journal, 39(9):767–779, 1996.

[11] I. R. Chen and D. C. Wang. Analyzing Dynamic Voting using Petri Nets. In 15th IEEE Symposium on Reliable Distributed Systems, pages 44–53, Niagara Falls, Canada, October 1996.

[12] S.-T. Cheng, C.-M. Chen, and I. R. Chen. Dynamic quota-based admission control with sub-rating in multimedia servers. MultimediaSystems, 8(2):83–91, 2000.

[13] 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 127–134, Miami, FL, USA, January 2007.

[14] A. daSilva et al. Decentralized intrusion detection in wireless sensor networks. In 1st ACM inter. workshop on quality of service & security in wireless and mobile networks, pages 16–23, 2005.

[15] B. Dutertre. Formal modeling and analysis of the modbus protocol. Critical Infrastructure Protection, pages 189–204, 2007.

AUTHOR DETAILS:

Author 1:

Ms.jameela jahan has completed her DIPLOMA in electronics and communication engineering , she has completed her B.Tech. in electronics and communication engineering from swami vivekannda institute of engineering , JNTU University, Hyderabad. Presently, she is pursuing her Masters in Computer Networks from Shadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, T.S, India.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Author 2:

Ms. SHILPA KARRE, has completed her BTECH FROM JNTU,and MTECH FROM OSMANIA UNIVERSITY(I.E MAIN CAMPUS), Currently. She has 7 years of experience in teaching field she is working as ASSOSICATE PROFESSOR, Department of CSE, in Shadan Women's College of Engineering and Technology.

Author 3:

Ms. Saleha Farha has completed her B.Ttech (Computer Science & Engineering) and M.Tech (Software Engineering) from JNTUH University, hyderabad. She has five years of experience in teaching field. Currently, she is working as the Head of CSE Department in Shadan Women's College of Engineering and Technology, Hyderabad, T.S, India.