ENGINEERING IN ADVANCED RESEARCH SCIENCE AND TECHNOLOGY

ISSN 2278-2566
Vol.01, Issue.04
September -2017
Pages: 455-459

BEHAVOIR RULE BASED ON MEDICAL CYBER PHYSICAL SYSTEMS

#1 M.Kishore kumar, #2K.Venkateswara Rao, #3 J.V.Krishna,
[1]M-Tech Dept. of CSE Sree Vahini Institute of Science and Technology, Tiruvuru, Andhra Pradesh
[2]Assit.Professor Dept. of CSE Sree Vahini Institute of Science and Technology, Tiruvuru, Andhra Pradesh
[3]Assoc.Professor & H.O.D Dept. of CSE Sree Vahini Institute of Science and Technology Tiruvuru, Andhra Pradesh

Abstract:
We propose and analyze a behavior-rule specification-based technique for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) in which the patient's safety is of the utmost importance. We propose a methodology to transform behavior rules to a state machine, so that a device that is being monitored for its behavior can easily be checked against the transformed state machine for deviation from its behavior specification. Using vital sign monitor medical devices as an example, we demonstrate that our intrusion detection technique can effectively trade false positives off for a high detection probability to cope with more sophisticated and hidden attackers to support ultra safe and secure MCPS applications. Moreover, through a comparative analysis, we demonstrate that our behavior-rule specification-based IDS technique outperforms two existing anomaly-based techniques for detecting abnormal patient behaviors in pervasive healthcare applications.

1. INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

2. LITERATURE SURVEY

AUTHORS: H. Al-Hamadi and I. R. Chen

In this paper we propose redundancy management of heterogeneous wireless sensor networks (HWSNs), utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of our redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Furthermore, we consider this optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN. We develop a novel probability model to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of voters and the intrusion invocation interval under which the lifetime of a HWSN is maximized. We then apply the analysis results obtained to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes, to maximize the HWSN lifetime.

We propose a trust-based intrusion detection scheme utilizing a highly scalable hierarchical trust management protocol for clustered wireless sensor networks. Unlike existing work, we consider a trust metric considering both quality of service (QoS) trust and social trust for detecting malicious nodes. By statistically analyzing peer-to-peer trust evaluation results collected from sensor nodes, each cluster

head applies trust-based intrusion detection to assess thehere may also be distributed retailers where scores will also be submitted, or every participant with ease files the opinion about each and every experience with different We propose a highly scalable cluster-based hierarchical trust management protocol for wireless sensor networks (WSNs) to effectively deal with selfish or malicious nodes. Unlike prior work, we consider multidimensional trust attributes derived from communication and social networks to evaluate the overall trust of a sensor node. By means of a novel probability model, we describe a heterogeneous WSN comprising a large number of sensor nodes with vastly different social and quality of service (QoS) behaviors with the objective to yield "ground truth" node status. This serves as a basis for validating our protocol design by comparing subjective trust generated as a result of protocol execution at runtime against objective trust obtained from actual node status. To demonstrate the utility of our hierarchical trust management protocol, we apply it to trust-based geographic routing and trust-based intrusion detection. For each application, we identify the best trust composition and formation to maximize application performance. Our results indicate that trust-based geographic routing approaches the ideal performance level achievable by flooding-based routing in message delivery ratio and message delay without incurring substantial message overhead. For trust-based intrusion detection, we discover that there exists an optimal trust threshold for minimizing false positives and false negatives. Furthermore, trust-based intrusion detection outperforms traditional anomaly-based intrusion detection approaches in both the detection probability and the false positive probability.

3. Effect of intrusion detection and response on reliability of cyber physical systems

In this paper we analyze the effect of intrusion detection and response on the reliability of a cyber physical system (CPS) comprising sensors, actuators, control units, and physical objects for controlling and protecting a physical infrastructure. We develop a probability model based on stochastic Petri nets to describe the behavior of the CPS in the presence of both malicious nodes exhibiting a range of attacker behaviors, and an intrusion detection and response system (IDRS) for detecting and responding to malicious events at runtime. Our results indicate that adjusting detection and response strength in response to attacker strength and behavior detected can significantly improve the reliability of the CPS. We report numerical data for a CPS subject to persistent, random and insidious attacks with physical interpretations given.

A relatively new trend in Critical Infrastructures (e.g., power plants, nuclear plants, energy grids, etc.) is the massive migration from the classic model of isolated systems, to a system-of-systems model, where these infrastructures are intensifying their interconnections through Information and Communications Technology (ICT) means. The ICT core of these industrial installations is known as Supervisory Control And Data Acquisition Systems (SCADA). Traditional ICT security countermeasures (e.g., classic firewalls, anti-viruses and IDSs) fail in providing a complete protection to these systems since their needs are different from those of traditional ICT. This paper presents an innovative approach to Intrusion Detection in SCADA systems based on the concept of Critical State Analysis and State Proximity. The theoretical framework is supported by tests conducted with an Intrusion Detection System prototype implementing the proposed detection approach.

4.A multidimensional critical state analysis for detecting intrusions in SCADA systems

A relatively new trend in Critical Infrastructures (e.g., power plants, nuclear plants, energy grids, etc.) is the massive migration from the classic model of isolated systems, to a system-of-systems model, where these infrastructures are intensifying their interconnections through Information and Communications Technology (ICT) means. The ICT core of these industrial installations is known as Supervisory Control And Data Acquisition Systems (SCADA). Traditional ICT security countermeasures (e.g., classic firewalls, anti-viruses and IDSs) fail in providing a complete protection to these systems since their needs are different from those of traditional ICT. This paper presents an innovative approach to Intrusion Detection in SCADA systems based on the concept of Critical State Analysis and State Proximity. The theoretical framework is supported by tests conducted with an Intrusion Detection System prototype implementing the proposed detection approach.

5.Existing system

Intrusion detection techniques in general can be classified into four types: signature, anomaly, trust, and specification-based techniques. In the literature, ISML and T-Rex are also specification-based approaches for intrusion detection in CPSs. However, none of them considered MCPSs. In the field of intrusion detection for MCPSs or healthcare systems, Asfaw et al. studied anomaly based IDS for MCPSs.

The authors focus on attacks that violate privacy of an MCPS; in contrast, our investigation focuses on attacks that violate the integrity of an MCPS. They use an anomaly-based approach while we use a specification based approach. Asfaw et al. do not provide numerical results in the form of false negatives or positives which are the critical metrics for this research area; our investigation does provide these results shoppers are usually not mindful of provider or resource Supplier's reliability, the latter may just act deceitfully via delivering false or

deceptive know-how involving service pleasant stages [11]. Apparently, the crisis of offering safety has reversed, and we must safeguard cloud customers instead than resource providers. On this state of affairs, soft safety mechanisms like trust and fame can provide security towards such threats [37]. Trust is a socio-cognitive phenomenon which has a wide variety of definitions proposed by way of different researchers. It is a subjective view of a customer on a supplier which is most commonly gained from individual experiences got through direct interactions, taken location prior to now. We expect reliability of a provider supplier to be context or situation sensitive.That is because, a provider may just behave otherwise underneath varying contexts, and such behavior is basically impartial of one a different.

6. REPUTATION ESTIMATION

Popularity model comes into outcomes when client cj has now not interacted with provider pk on current context in the previous. Beneath this hindrance, cj has to consider in feedbacks/ referrals from different buyers who've directly interacted with pk. We denote a patron delivering suggestions as a "witness" from cj's viewpoint. Feedbacks from more than a few witnesses are to be mixed to acquire a worldwide fame ranking for any supplier. Such referrals from extraordinary sources may not crisply outline a provider's fame as "depended on" or "distrusted" following any Boolean function. As a result, aside from an speculation (e.g., provider is trusted) being genuine or false, there could exist an detail of uncertainty or lack of expertise, often called common hypothesis. Classical probability conception are not able to realize the detail of uncertainty related to an event [40]. We have chosen Dempster-Shafer (DS) thought of proof [41], [42] to deal with this uncertainty issue. It allows an express representation of lack of knowledge and combination of proof [43]. Motivation behind utilizing this model is that it is well-understood, mathematically sound, supplies a proper framework for combining sources of evidences, and captures the uncertainty or common hypothesis, which is basically normal even as computing repute of an entity.

7. 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 behavior-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 deviceapproaches one (that is, we can always catch the attacker without false negatives) while bounding the false alarm probability to below 5 percent for reckless attackers and below 25 percent for random and opportunistic attackers over a wide range of environment noise levels. Through a comparative analysis, we demonstrated that our behaviorrule specification-based IDS technique outperforms existing techniques [28], [32] based on anomaly intrusion detection. 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 modeling research based on stochastic Petri net techniques [13], [14], [23], [26], as well as intrusion defense modeling research based on accumulation of deviation from good states [6], [9],

[10] such that the system can dynamically adjust CT to maximize intrusion detection performance in response to changing attacker behaviors at runtime.

8.REFERENCES

[1] 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. 189–203, Jun. 2013.

[2] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Security challenges in next generation cyber physical systems," Beyond SCADA: Netw.
Embedded Control for Cyber Phys. Syst., Pittsburgh, PA, USA, Nov. 2006.

[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., Oct. 2010, pp. 1–8. [4] F. Bao, I. Chen, M. Chang, and J.H. Cho, "Trust-based intrusion detection in wireless sensor networks," in Proc. nt. Conf. Commun., Jun. 2011, pp. 1–6.

[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. 169– 183, Jun. 2012.

[6] F. B. Bastani, I. R. Chen, and T. W. Tsao, "Reliability of systems with fuzzy-failure criterion," in Proc. Annu. Rel. Maintainability Symp., Anaheim, CA, USA, Jan. 1994, pp. 442–448.

[7] 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 Trans. Ind. Inf., vol. 7, no. 2, pp. 179–186, May 2011.

[8] A. Cardenas, S. Amin, B. Sinopoli, A. Giani, A. Perrig, and S. Sastry, "Challenges for securing cyber physical systems," in Proc. 1st Workshop Cyber-Phys. Syst. Security DHS, 2009, pp. 1–4.

[9] L. Freeman, "Centrality on social networks," Social Netw., vol. 1, pp. 215–239, 1979.

[10] T. Grandison and M. Sloman, "A survey of trust in internet

Applications," IEEE Commun. Surv. Tutorials, vol. 3, no. 4, pp. 2–

Authors Profiles

M.Kishore kumar, M.Tech dept of cse sree vahini instiute of scienceand technology tiruvuru Andhra pradesh

K.Venkateswara Rao , Assistant Professor SreeVahini Institute of Science and Technology Tiruvuru Andhra Pradesh. "B.TECH (CSE), M.TECH (CSE)"

J.V Krishna, Associate Professor& HOD SreeVahini Institute of science and Technology, Tiruvuru, AndhraPradesh, B.Tech(CSE), M.Tech(CSE), Pursuing Ph.D