Journal of Advances and Scholarly Researches in Allied Education
Vol. 16, Issue No. 5, April-2019, ISSN 2230-7540

Model Detection for Software Security in Medical Cyber Physical Systems

Sakshi Rai[1]* Dr. Sunil Pholre[2]

[1] Research Scholar

[2] Supervisor

Abstract – Some of the major issues that these cyber infrastructures must deal with include issues like privacy, trust, and security. With these smart gadgets, an automated environment may be created in fields such as military, manufacturing, e-healthcare, and so on. These technologies helped to create the Medical Cyber Physical System in e-healthcare (MCPS). CPS are varied and can incorporate a wide range of technologies. However, the security issues found in the upper levels of this taxonomy are more closely linked to those found in other KAs that deal with more traditional security issues. Because of this, the emphasis of this paper is on elements of CPS that are more directly linked to the detection, control and actuation of these systems.

Keywords – Security, Trust, Detection, Medical, Cyber

----------X----------

INTRODUCTION

A cyber-physical system (CPS) or intelligent system is a computer system that uses computer-based algorithms to operate or monitor a mechanism. Physical and software components are intimately interwoven in cyber-physical systems, allowing them to function on various spatial and temporal dimensions, show numerous and unique behavioral modalities, and interact with one another in context-dependent ways. CPS combines cybernetics, mechatronics, design, and process science in a transdisciplinary approach. Embedded systems are a term used to describe process control. The focus of embedded systems tends to be on the computational components, rather than a strong connection between the computational and physical aspects.

In recent years, cyber-physical systems (CPS) have received a lot of attention and are being regarded as an emerging technology. It integrates computing and communication with the physical environment. The US National Science Foundation (NSF) identified CPS as a key research area in 2008, and the US President's Council of Advisors on Science and Technology listed it as the number one research priority. Sensing, processing, and networking are all used in CPS. CPS is a strong candidate for healthcare applications such as in-hospital and in-home patient care, thanks to recent advances in wireless sensor networks (WSN), medical sensors, and Cloud Computing. These advancements promise to give CPS the ability to remotely monitor patient conditions and take action regardless of where the patient is. Medical sensors are the subject of much study. These sensors can collect vital patient information such as health information.

LITERATURE REVIEW

Nilanjan Dey (2018) Medical cyber-physical systems (MCPS) are a network of medical devices that are essential to healthcare. These systems are gradually being used in hospitals in order to provide consistent high-quality treatment. In addition to interoperability, security/privacy, and high confidence in the system software, the MCPS architecture confronts a number of difficulties. The infrastructure of cyber-physical systems (CPS) is examined and addressed in this paper. This paper contributed to the advancement of networked Medical Device (MD) system research in order to improve healthcare efficiency and safety. It may also help medical device experts solve critical problems with medical devices and the obstacles that arise with network architecture for medical

devices. The idea of social networking and its security is discussed, as well as the concept of wireless sensor networks (WSNs). Following that, CPS systems and platforms were developed, with a greater emphasis on CPS-based healthcare. CPSs' big data framework is provided as well.

Darren Seifert (2016) This article examines the various cyber-physical system designs that are currently available. A set of important characteristics for cyber-physical systems in healthcare are used to evaluate a number of potential designs. Then, in two of the designs, schematics describing the anticipated functioning of infusion pumps are examined. The STRIDE Threat Model is then used to deconstruct each one in order to identify potential security problems and how to solve them. Finally, a comparison of the main security problems in each design is given to aid in determining which architecture is the most adaptive to fulfil the security requirements of healthcare cyber-physical systems.

Ajeet Singh (2018) Cyber-Physical Systems (CPS) are systems that combine cyber and physical world components to improve physical performance. Because more cyber and physical equipment are linked to offer state-of-the-art technology, the utilisation of cyber-physical systems (CPS) is increasing, and cyber risks and assaults are occurring and being reported at an exponential rate. CPS security problems and challenges have become a worldwide issue, and a suitable CPS mechanism is urgently needed. An study of the connection between the CPS and IoT, as well as its definitions and some of its domains, is addressed in this article. In the context of CPS, security problems and issues are researched and addressed. This article discusses several CPS vulnerabilities, cyber threats, and cyber-attacks on the cyber-physical system. Finally, security techniques, methods, and procedures for reducing the cyber danger or cyber-physical system assaults are proposed

Saurabh Singh (2017) Because it is particularly adapted to the information age, blockchain technology is becoming more appealing to the next generation. The Internet of Things can also benefit from blockchain technology (IoT). In distributed systems, the development of IoT technology in many areas has resulted in significant progress. For storing and exchanging data and transactions on the network, the blockchain idea necessitates a decentralised data management system. This article goes through the blockchain idea and other important aspects, as well as a thorough examination of possible security threats and current solutions that may be used as defences. This article also discusses ways to improve blockchain security by outlining important aspects that may be used to create different blockchain systems and security tools that address security flaws. Finally, the study addresses outstanding problems with blockchain-IoT systems as well as future research possibilities.

Social Attack and Defense Models

Attack/forged communications in social networks may be detected using techniques created by identifying characteristics. Individual users and network operators may categorize messages using these methods. On the basis of the discovery that malicious accounts have consistent characteristics over time, such as the time of day, source, message content, subject, links in messages and direct user engagement and proximity Egele et al. found malicious accounts in OSNs that are harmful. When profiling fraudulent accounts, Ruan et al. looked at both extroversive and introversive behavioral characteristics (such as browsing preference and visit length) as well as request latency and browsing sequence. For example, the number of retweets, an evolutionary classification system developed by Chen et al. may identify time-varying statistical characteristics of spam. A study by Yang et al. showed that spammers on Twitter had low local clustering coefficients, high betweenness centrality and low bidirectional link ratios. In order to enhance the identification of fraudulent accounts, we used neighbor characteristics such as the followers of our neighbors, the tweets of our average neighbors, and the followers of our average neighbors. The quantity of first-person pronouns and the ratio of exclamation sentences were suggested by Shehnepoor et al. in addition to user-based characteristics to evaluate evaluations in OSNs based on reviews, such as early time frame, rate deviation, and number of exclamation phrases (e.g., feedback on a topic or a product). Another characteristic that was utilized to detect spammers was the amount of views and comments the post had gotten. The use of linguistic characteristics like sentence structure and modifiers to evaluate reviews was also suggested. Tangram split spams into segments and extracted templates for accurate and quick spam detections based on the discovery that the bulk of collected spams are produced using underlying templates.

OSN interactions have been modeled using game theory. Spam communications may be

sent by publishers to earn a larger payoff in a game between publishers and administrators, which in turn enhances the success of spam messages being detected by administrators. Publishers who have been identified as spreading malware should be blocked and quarantined. In order to capture viral product design and customer happiness in OSNs and maximize product uptake, a Stackelberg-type game was built up in. A study by Abbass et al. examined the trustworthiness of OSN players using game theory and found that a society free of dishonest members produced the most income. This thesis discusses a situation where different kinds of users have differing perspectives on (fabricated) communications and messages may even be mistakenly misclassified, but game theory has not been utilized to describe and evaluate such a complex scenario. There are no current game-theoretic studies that can capture the increasingly popular OSN risk warning method, to the best of our knowledge. of the The design and configuration of the method will benefit from knowing the technique's long-term impact on publication behavior control.

Misclassification-free Infinitely Repeated Game

When playing a game with no misclassifications, the real messages are always properly categorized, thus p2 = 1 is the first thing we think about. Only while posting fake communications does P employ bots. Table 1 provides the payoff matrix for each message, with the rewards for P listed under the various approach combinations. Only when fraudulent communications are released are bots recruited at a cost of C3Nt.

Table 1: The payoff matrix to *P* per round in the case of misclassification-free game/situations

		A	
		Trust	*Distrust*
P	*Benign*	$C_1(N_r + N_n)$	C_1N_n
	Malicious	$C_2(N_r + N_n) - C_3N_t$	$C_2N_n - C_3N_t$

There are (Nr + Nn + Nt) possible bits of feedback from a fake message, p1Nr + Nn being positive. As a consequence, it is possible that a fake communication may be seen as real.

$$q_1 = \frac{p_1N_r + N_n + N_t}{N_r + N_n + N_t},$$

and correctly detected to be forged with probability (1 − q_1).

ANALYSIS TO DETECT MALWARE

New malware is being discovered on a daily basis. When a computer user visits a malicious website hosting a drive-by download attack, clicks on a malicious link in an email, or inserts a malware-infected USB flash drive into their computer, they unwittingly download malware to their machine. Depending on the virus, there may be breaches of private data, disruptions in operations, or infrastructure damage after it has entered the company (Security and Report, 2017). The vast quantity and diversity of attack strategies, both known and undiscovered, contribute to the difficulty of detecting a cyber-strike.

Signature-based, Behaviour/anomaly-based, and Heuristic/specification methods are the most common ways to detect an assault and classify it. Table 4.1 summarizes the benefits and drawbacks of each technique, and Figure 4.2 shows examples of methods from each category.

At this stage, detecting new variants of well-known malware families is a problem. However, a growing number of hackers are now using polymorphic or encrypted code portions, making it almost impossible to detect their activity. As a result, malware writers have the option of making signature detection obsolete. As a result, behavior-based scanning was created by observing a certain pattern or aberrant behavior (Ding et al., 2014). Putting malware in a sandbox, for example, makes it easier for it to keep track of its victims. However, employing behavioural analysis to find malware requires extensively instrumenting the OS. Apart from that, stopping harmful or suspicious behavior in running applications requires a lot of time and effort (Mohammed, Mohammed, and Saraee, 2016). Furthermore, many behavior solutions are only available on the cloud, which may be problematic for certain businesses. Figure 1, based on knowledge of current works, illustrates the plan of each method once it has all been put together.

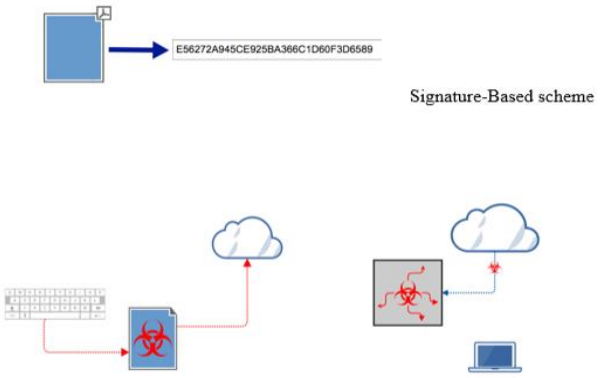

Figure 1: Malware Analysis Scheme

Malware that looks for a particular registry key associated with a virtual environment may elude detection by an automated sandbox and an analyst running a suspected malware code dynamically in a virtual machine, respectively (Mehra and Pandey, 2016). Malware detection methods based on signatures and behavior have their uses and benefits. These methods, although useful, consume resources and are inaccurate due to the assumption that malware and its behavior will not change. It is possible that behavior and signature-based techniques have potential, but they may not deliver on that promise when seen as pure technology (Das et al., 2016). As a result, a specification-based hybrid analysis is presented that makes use of both methods.

Security

"Security engineering is about designing systems to stay reliable in the face of malice, mistake, or mischance," writes one of the book's most famous writers, Ross Anderson.

Software must be reliable in the face of malice: the desire to cause damage, misery, or injury to another due to an aggressive urge or a deep-seated selfishness. Error: a departure from accuracy or correctness; a blunder, whether in action or speech, should not be a problem for the program. Mischance: an accident or misfortune: the program must be reliable in the face of this situation.

Software cryptography and hardware temperature resistance are only two examples of the types of knowledge needed in security engineering. Additionally, it includes the use of tools, procedures, and techniques of the trade. Anderson asserts that for a security system to be effective, four factors must be in place: policy, incentives, mechanism, and assurance. This is an illustration of an organizational chart in Figure 2.

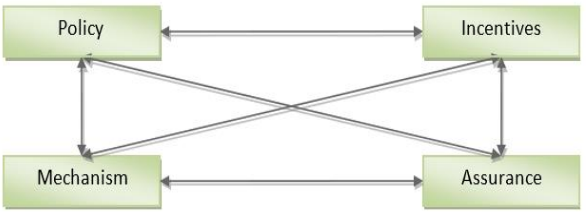

Figure 2 Security Engineering Analysis Framework > Adapted from (Anderson, 2001)

Software Security (7 Touch points)

7 points of contact STP refers to a method for developing security systems that focuses on a certain set of standards. the software security series published in 2006 by addison-wesley To enhance software security, there are seven contact points that offer seven new functionalities.

There are seven processes shown in Figure 3, and unlike SDL, these processes have artifacts listed above them. We will use these artifacts in this research project to collect needs, much as we did with SDL in the past.

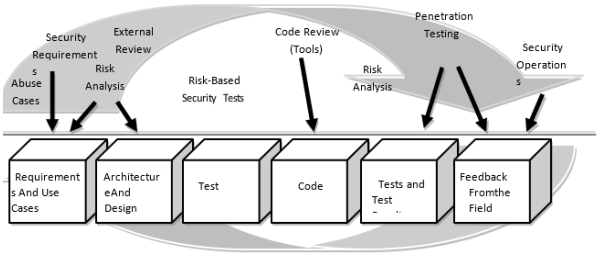

Figure 3 Software Security 7 Touch Points > Adapted from (Addison-Wesley Software Security Series, 2006)

In order to bring security considerations into the software development lifecycle as early as feasible, the CLASP offers a well-organized and structured methodology (OWASP, 2014). Each of the five CLASP views is divided into activities, each of which has process components. must be familiar with the CLASP procedure As shown from the View > Activity > Process component, Figure 4 depicts how this process works from inside.

CLAPS views are organized so that engineers may see things from a variety of angles depending on the view they are in. To begin, there is a concept view that walks you through the process's fundamentals. It is easier to comprehend authentication management using a role-based approach. Understanding the risks,

costs, and applicability of inactivity from an activity-assessment perspective.

Security-related actions may be analyzed using an activity implementation perspective. Finally, there is a vulnerability perspective on stating risks, issues, outcomes, and so on.

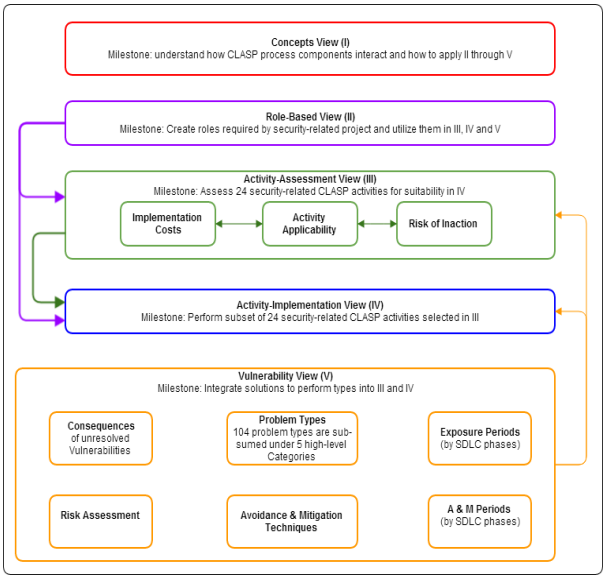

Figure 4 CLASP Views and their interactions > Adapted from

A malevolent user's anti-requirement subverts an already existent requirement. Security requirement engineers may generate anti-requirements using misuse/abuse scenarios or other elicitation techniques, but malevolent users are more likely to do so..

CONCLUSION

Targeted Cyber Attacks and Advanced Persistent Threats were the focus of this study. Furthermore, a thorough understanding of APT, APT attack types, attack routes, and malware evasion methods was provided. In order to identify and evaluate APTs, this study suggested a Hybrid analytic method that integrates static, dynamic, memory, and system state analysis. Advanced malware was detected using a hybrid analytic method that used a Behaviour-based Sandboxing (BbS) approach. No extra OS or application requirements are needed with the BbS method; thus, it may be implemented on any operating system. Compared to the Cuckoo analysis, the Hybrid analysis method was more effective and yielded higher detection accuracy.

Targeted ransomware assaults may be detected using an Intrusion Detection Honeypot (IDH), which is suggested in this thesis. With this approach, data is gathered from multiple sources (Honeyfolder, SDN network and hosts (Audit Watch), Firewall), converted into event streams, and processed (complex) using CEP engine by applying aggregation rules in order to determine ransomware behavior and pattern in order to mitigate the attack with no data loss. Additionally, a software-defined network (SDN) architecture has been implemented, which enhances network security by applying control rules to categorize network traffic. According to the results of the experiments, the suggested IDH beats the current state-of-the-art Honeypot by 98 percent when it comes to ransomware detection. There is also evidence to suggest that the IDH deployment 167, as now suggested, is both cheap and successful in drawing attention to ransomware threats. A proof-of-concept implementation shows how attackers utilize drones to launch assaults and compromise their targets from a distance. It was shown via testing that drone-based assaults are possible, simple to deploy, and the target may be remotely hacked in this way.

REFERENCES

1. Nilanjan Dey (2018). “Medical cyber-physical systems: A survey,” J Med Syst 2018 Mar

2. Darren Seifert (2016). “A Security Analysis of Cyber-Physical Systems Architecture for Healthcare,” Computers 2016, 5, 27; doi:10.3390/computers5040027 www.mdpi.com/journal/computers

3. Ajeet Singh (2018). “Study of Cyber Attacks on Cyber-Physical System,” 3rd International Conference on Advances in Internet of Things and Connected Technologies (ICIoTCT).

4. Saurabh Singh (2017). “Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network,” Received January 4, 2017, accepted January 9, 2017, date of publication January 14, 2017, date of current version January 26, 2017. Digital Object Identifier 10.1109/ACCESS.2017.3051602

5. Dong Chen, Sandeep Kalra, David Irwin, Prashant Shenoy, and Jeannie Albrecht (2015). Preventing occupancy detection

from smart meters. IEEE Transactions on Smart Grid, 6(5): pp. 2426–2434.

6. Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, and Victor C Leung (2011). Body area networks: A survey. Mobile Networks and Applications, 16(2): pp. 171–193.

7. Thomas M Chen and Saeed Abu-Nimeh (2011). Lessons from stuxnet. Computer, 44(4): pp. 91–93.

8. Eric Chien, Liam OMurchu, and Nicolas Falliere (2012). W32.duqu: The precursor to the next stuxnet. In Presented as part of the 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, Berkeley, CA, 2012. USENIX.

9. Kyong-Tak Cho and Kang G Shin (2016). Error handling of in-vehicle networks makes them vulnerable. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 1044–1055. ACM.

10. Kyong-Tak Cho and Kang G Shin (2016). Fingerprinting electronic control units for vehicle intrusion detection.

Corresponding Author

Sakshi Rai*

Research Scholar