IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

# Cyber Victimization: Healthcare Cyber-Physical Systems (H-CPSs) Vulnerability Issues and Challenges

**Mahesh Devarshi,**
PhD Scholar, MS University, Tamilnadu

***Abstract:*** *Computers, Mobile Phones and the Internet persist to spread throughout human life's' in everything from automobiles to kitchen appliances. The rapid rise of computers and computer networks in present life has formed new opportunities for criminal activity. The healthcare industry is undergoing a major transformation. Using computer intelligence and machine learning, the sector is revolutionizing care and convenience. This new ecosystem, which is called Cyber Physical Systems, was built by IoTs. Cyber-physical system (CPS) is an integration of physical processes with computation and communication. It has the ability to add more intelligence to social life. In the last decade, there has been a lot of work done on cyber physical systems that we didn't expect. There have been a lot of threats, challenges, and important issues in the last decade. Today, Healthcare Cyber-physical Systems (HCPS) is considered to be an area with huge potential in the medical field. Healthcare Cyber-Physical Systems (HCPS) attempts to provide intelligent information about a patient's treatment to caregivers. The Functioning of HCPS is comparable to other systems involving automated decisions that impact human life. This makes the safety and security requirements of HCPS extremely important. Currently, the biggest threat to HCPS would be the numerous security and privacy challenges that it shares with classical distribution systems and some unique to HCPS as a result of connected components and system requirements. For example, there is no doubt that HCPS must maintain patient's privacy information, avoiding leakage through direct exposure to unauthorized parties, side-channel information, or poor system implementation practices.*

*This article investigates the security and safety of HCPS through the understanding of threat modeling in HCPS as a step towards patient security and privacy. This is achieved through examining the roles of stakeholders and system components and sketching and abstract architecture of HCPS to demonstrate various threat modeling options. The article also comments on the role of major security techniques that have been well-established state-of-the-art and investigate their applicability and utility for the design of HCPS.*

***Key Words:*** *Cyber-Physical System, Healthcare Cyber-Physical System, Threat Modelling, Trust Modelling, Anomaly Detection, Crypto-graphic Measures, System Hardening, Impact of human life.*

## 1. INTRODUCTION:

The healthcare industry is undergoing a major transformation. Using computer intelligence and machine learning, the sector is revolutionizing care and convenience. This is mainly due to developments in the field of Cyber-Physical Technology. Cyber-Physical Technology is the confluence of intelligent software and capable hardware. Where computer-based algorithms are used to control and monitor mechanical components. Today, Healthcare Cyber-Physical Systems (HCPS) is considered to be an area with huge potential in the medical field. Healthcare Cyber-Physical Systems (HCPS) attempts to provide intelligent information about a patient's treatment to caregivers. The system prioritizes patient care and safety by computing usage scenarios considering a broad spectrum of the patient's health. Its ability to compute such data at an unprecedented level makes it uniquely suited for this type of work. For Example, health-monitoring systems continuously monitor patients' various body parameters in real-time to improve patient treatment effectiveness. Robotic surgical systems aid surgical procedures by performing actions with smooth and feedback-controlled motions. HCPS are increasingly used in hospitals to provide high-quality healthcare and have emerged as promising platforms for monitoring and controlling multiple aspects of patient health.

The Functioning of HCPS is comparable to other systems involving automated decisions that impact human life. This makes the safety and security requirements of HCPS extremely important. Currently, the biggest threat to HCPS would be the numerous security and privacy challenges that it shares with classical distribution systems and some unique to HCPS as a result of connected components and system requirements. For example, there is no doubt that HCPS must maintain patient's privacy information, avoiding leakage through direct exposure to unauthorized parties, side-channel information, or poor system implementation practices. Some of the interoperability requirements with components are not always suited for usage with untrustworthy parties. Limited knowledge in system security and privacy makes operators of HCPS particularly vulnerable from a cyber-security standpoint. As a result, a sequence of unstudied consequent executions demanded from the system may jeopardise the patient's privacy or safety.

(Manuscript received January 20, 2022)

## 2. LITERATURE REVIEW:

There is a great deal of literature investigating the factors that motivate healthcare cyber physical systems and its security challenges, the management of cyber security in medical devices (https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidancecedocuments/ucm356190.pdf, [On-line; accessed 20-December-2021], Javaid, Y., Sun, W., Devabhaktuni, V. K., Alam, M. (2012).“Cyber security threat analysis and modelling of an unmanned aerial vehicle system, H. Yun, L. Sha, and T. F. Abdelzaher, “A framework for the safe interoperability of medical devices in the presence of network failures,” in ICCPS ’10, 2010, S. Johansson, K. H. (2015). “Cyber physical security in networked control systems: An introduction to the issue,” IEEE Control Systems, vol. 35, no. 1, pp. 20–23, Lin, J., Li, F. Luo, B. (2017). “Cyber-physical systems security a survey,” IEEE Internet of Things Journal.

## 3. ISSUES AND CHALLENGES IN CYBER PHYSICAL SYSTEMS:

Currently Cyber-Physical Systems (CPS) is widely used in many applications, the security considerations of these systems should be of very high significance. Co-operation of these systems through several security vulnerabilities, attacks in serious infrastructure will cause serious consequences. We need efficient security countermeasures into cyber-physical systems to overcome such attacks and also, patching and frequent updates are not implemented or updated correctly in cyber physical systems / control systems. Some new research Challenges in CPS are High assurance software, Interoperability, Context awareness, Security and privacy, and Certifiability. The efficient CPS architecture with good styles and designs is a big issue. We require a multi-view, multi-stakeholder, extensible framework for designing and validating early design decisions taken when architecting CPS. Some challenges towards CPS (in general) are in terms of Modifiability, Performance, Dependability, Flexibility, Portability, Reliability, Maintainability, Verifiability and Compatibility. Hence, this section discusses several critical issues and challenges in CPS.

## 4. THREAT MODELLING IN H-CPS:

Threat modelling is an approach used to analyse a system's potential threats at the design level. It is traditionally used in CPS to identify threats. It could provide recommendations to system designers to address threats identified with proper countermeasures. Threat Modelling can be performed from different perspectives, e.g., Attacker-centric Model and System-centric Model. Attacker-Centric Model is a process that starts by profiling possible attackers, then evaluating their goals as well as the knowledge and resources available. Based on these findings, the model can implement necessary mitigation strategies. For example, researchers proposed to use Game theory to assess the security of CPS and improve the system's survivability in the face of strategic adversities. Stem-Centric Model focuses on identifying all possible attacks that target each of the system elements. Another commonly used approach is the attack tree-based modelling. It represents potential threats against a system using a tree structure, where the root node represents the overall threat, and leaf nodes represent the different ways of attacks. Several recent research efforts have focused on the safety analysis of medical systems. They utilized a timed automaton model to express the safety property of a medical system and modelled the timing relationship between system components to prove the safety of the system. Some of the notable instances where threat modelling was used would be when Halper in et al. presented a general framework for evaluating the security and privacy of wireless implantable medical devices. Burleson et al. discussed design principles for securing implantable medical devices. Rushanan et al. emphasized the need of achieving trustworthy communication, trustworthy software, and trustworthy hardware and sensor interfaces in implantable medical devices and body area networks. Zhang et al. discussed trustworthiness concerns of medical devices and possible countermeasures against these threats in HCPS. The authors summarized major trustworthiness requirements of a HCPS, including reliability and availability of medical devices, confidentiality and integrity of patient data. Tamara et al. analysed cyber-security attacks against teleported robotic surgery systems, focusing on denial-of-service (DoS) attacks. The prior work on security and threat modelling for cyber-physical systems also shed light on similar problems with medical cyber-physical systems. Cyber-physical systems have common design characteristics, such as integrating components from multiple vendors with various design goals and are under similar general safety requirements, such as maintaining human lives. However, to the best of my knowledge, a systematic analysis of security threats for modern medical CPS systems isn't a well-studied subject in the literature.

## A. Trust and Threat Models:

1. H-CPS Stakeholders: A healthcare cyber-physical system can be designed in various forms. Here we assume a centralized design model in which a control component is in place. In this model, the control component has two subsystems. One subsystem interacts directly with the practitioners, and the second subsystem manages other components with direct human interactions. However, the second subsystem does need a network interface to a technical team to interfere when the system needs recovery from an urgent failure. Practitioners are the main stakeholders in HCPS. Practitioners (including doctors, nurses and other healthcare workers) can have various roles and responsibilities and may differ in their usage patterns. In a typical operation scenario, an assistant nurse may be in charge of monitoring the heartbeat of the patient. That puts the nurse in control of the electrocardiography (ECG) device. The data collected from the ECG may be viewed on a mobile device, in which case the simple protocol defines user input to the device to retrieve data. System administrators (or the technical team) are another important stakeholder group that maintains the system's reliability and availability. The system administration team may have various responsibility levels. In one wide-open case, system administrators can be as powerful as having access to the source code of individual system components, tamper with any operation, and replace executable binaries on the devices with updated ones. Non-medical staff can interact with individual components in HCPS. Office staff in a unit plays important roles and can directly work with the system to retrieve patient data depending on hospital policies; however, the roles of non-medical staff can differ.

## B. Trust Modelling:

2. Trust modelling of HCPS is a particularly important and difficult task. Trusting a particular component, software, or stakeholder can have catastrophic consequences involving a patient's health conditions and life.

We categorize the trust model with respect to individuals interacting with a HCPS as follows;

1. Trustworthy users represent relatively un-trustworthy individuals. The system may not completely function and achieve its goals without defining a set of fully trusted users. This is despite the fact that any individual, regardless of skills and career background, may intentionally or unintentionally commit mistakes that can affect patients' lives.

2. Trusted but error-prone users are similar to fully trusted users in their intentions but are expected to commit mistakes due to the lack of knowledge or training

3. Untrustworthy individuals exist in any environment. They do include general users that are not authorized to perform any medical actions or individuals that are either stakeholders or work closely with them but are not particularly authorized to work in a team that is responsible for the treatment of a patient.

4. Temporarily trustworthy individuals that may need access to a part of the system with specific operation authorization for a limited period of time.

The integrity of a system is violated by modifying existing information or fabricating new information. Attacks infiltrating the integrity of HCPS can be false packet/command injection or replaying outdated measures in the communication layer. Software-based exploits are a common way of compromising integrity, such as overwriting sensor values or critical control decision variables through memory corruption attacks. HCPS are also vulnerable to sensor data spoofing attacks in the physical layer, e.g., resonant acoustic injection attacks can disable the function of MEMS-based gyroscopes.

DDoS/DoS attacks are the main threats to the availability of MCPS, e.g., traffic jamming that disrupts communication through interference or collision, overflowing the buffer memory of network cards, and broadcasting spoofed network packets. By physically accessing to a medical device, it is possible an attacker modifies system configurations or corrupt data that impact the availability of the system

**EXAMPLE ARCHITECTURE:**

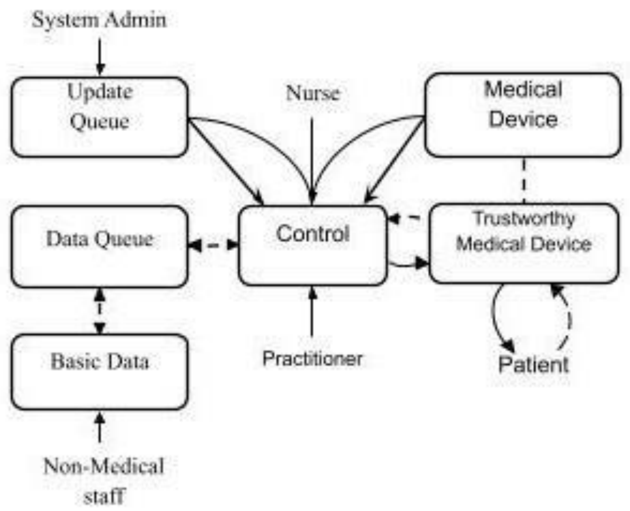

**Figure:1.**

- A proposed architecture in which a number of entrust worthy components are decoupled from the control centre in a Healthcare cyber-physical system.
- The dotted lines capture the flow of medical data while the solid lines capture the action initiation direction (according to general access control policies).
- The boxes represent system components and stakeholders are mentioned in the text.

## 5. SECURITY REMEDIES:

Even with the growing security concerns of HCPS, there are promising techniques against threats and attacks they are-

### A. Anomaly Detection

Runtime monitoring of HCPS is an effective countermeasure against various attacks. There has been considerable research activity on attack detection for CPS. The majority of existing works in this field are behaviour model-based, which can be further divided into two lines of research based on physical process models or cyber models. Physics-based models define normal operations in CPS for anomaly detection, where system states must follow immutable laws of physics in CPS. Cyber-based models characterize the expected program/system behaviors' to recognize potential attacks. Since CPS are application-specific, most existing works are designed to detect specific attacks for specific applications, such as smart grid, unmanned aerial vehicles and industrial control processes. Recent studies have shown that CPS may suffer from a variety of runtime attacks, including code-reuse attacks malicious code injection, non-control data attacks and false data injection attacks.

C- FLAT instruments target programs running on CPS devices to achieve the remote attestation of execution paths of these programs. Zimmer et al. exploited worst-case execution time information obtained through static analysis of application code to detect code injection attacks in CPS. In particular, Mitchell et al. analysed a behaviour-rule specification-based technique for intrusion detection in MCPS. They proposed to transform behaviour rules to a state machine, then at runtime check against the transformed state machine for deviation from a medical device's behaviour specification.

### B. Cryptographic Measures:

Cryptography is a commonly used approach for securing the communication channel from unauthorized access. However, most of the traditional cryptographic primitives that have been employed in general-purpose IT systems, both cyphers and hash functions, cannot be directly applied to HCPS due to the size, real-time, and power constraints of medical devices. For example, the high energy and implementation overhead of asymmetric cryptography pose significant challenges for encrypting sensitive data in HCPS. To mitigate this problem, compression techniques may be used before encryption to reduce the overhead.

### B. System Hardening:

A secure execution environment can be used to defend a wide range of threats in HCPS. Isolating security-critical applications from untrusted OS is a promising technique to enhance HCPS security, such as by the hardware security support of Intel's Trust Lite or ARM's Trust Zone technologies. HCPS can benefit from the inter-authentication of components to improve the system's integrity.

## 6. EVIDENCES AND CONCLUSION:

HCPS is a technology that has the potential to revolutionize the healthcare industry. Its ability to monitor, compare and analyse at an unprecedented level makes it a tool that can immensely help the healthcare industry. The paper examined the possible security challenges and issues that impact HCPS using Attacker centric and Stem Centric Threat modelling. The major challenges are due to the complicated nature of trust modelling within HCPS. The dynamic nature of reliable and unreliable entities threatens the system's integrity. Data fabrication, DDoS/DoS attacks, sensor data spoof attacks are all risk points that the paper has identified. These challenges and issues must initiate future discussions and interests of research work on security aspects of CPS. With a thorough understanding of the threat modelling in HCPS, we can provide solutions similar to those mentioned, such as Anomaly Detection, System Hardening and Cryptographic measures. Through sketching an abstract architecture of a HCPS, as we examined the roles of stakeholders and components and demonstrated various threat modelling options in HCPS, we envision future HCPS to enable clean security models that are verifiable. The discussion of major security techniques to mitigate the threats in Medical Cyber Physical System (MCPS) can further enhance design decisions made in future systems. Enhancing security and privacy in medical cyber-physical systems remains a serious challenge demanding careful considerations and joint efforts by the industry, the health systems, and the research community.

## REFERENCES:

- Abera, T., Asokan, N., Davi, L., Ekberg, J., Nyman, T., Paverd, A., Sadeghi, Tsudik, G. (2016). "C-FLAT: control-flow attestation for embedded systems software", in CCS.
- Alemzadeh, R. K. Iyer, Z. T. Kalbarczyk, N. Leveson, and J. Raman, "Adverse events in robotic surgery: A retrospective study of 14 years of FDA data," CoRR, vol. abs/1507.03518, 2015.
- Arney, R. Jetley, P. Jones, I. Lee, and O. Sokolsky, "Formal methods based development of a PCA infusion pump reference model: Generic infusion pump (gip) project," in Proceedings of the 2007 Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability, ser. HCMDSS-MDPNP '07, 2007, pp. 23–33.
- Arney, M. Pajic, J. M. Goldman, I. Lee, R. Mangharam, and Sokolsky, "Toward patient safety in closed-loop medical device systems," in PICCPS '10, 2010, pp. 139– 148.
- "Content of premarket sub-missions for management of cyber security in medical devices," https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidancecedocuments/ucm356190.pdf, [On-line; accessed 20-December-2021]. "Postmarket management of cybersecurity in medical devices," https://www.fda.gov/downloads/Medical Devices/Device Regulation and Guidance /Guidance Documents / UCM482022. pdf, [Online; accessed 20-December-2021].
- Javaid, Y., Sun, W., Devabhaktuni, V. K., Alam, M. (2012)."Cyber security threat analysis and modelling of an unmanned aerial vehicle system," in IEEE Conference on Technologies for Homeland Security (HST), pp. 585–590.
- Kim, M. Sun, S. Mohan, H. Yun, L. Sha, and T. F. Abdelzaher, "A framework for the safe interoperability of medical devices in the presence of network failures," in ICCPS '10, 2010.
- Kocabas, O. Soyata, T, and M. K. Aktas, "Emerging security mecha-nisms for medical cyber physical systems," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 13, no. 3, pp. 401–416, May 2016.
- Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, Mullen-Fortino, S. Park, A. Roederer, and K. K. Venkatasubrama-nian, "Challenges and research directions in medical cyber-physical systems," Proceedings of the IEEE, vol. 100, no. 1, pp. 75–90, 212.
- Martins, G., Bhatia, S., Koutsoukos, X., Stouffer, K., Tang, C., Candell (2015). "Towards a systematic threat modelling approach for cyber-physical systems," in Resilience Week (RWS), pp. 1–6.
- "Microsoft SDL threat modelling tool" (2009). Network Security, no. 1, pp. 15 – 18.
- Nourian Madnick, S. (2015). "A systems theoretic approach to the security threats in cyber physical systems applied to Stuxnet", IEEE Transactions on Dependable and Secure Computing. Manikas.
- Sandberg, H., Amin, S. Johansson, K. H. (2015). "Cyber physical security in networked control systems: An introduction to the issue," IEEE Control Systems, vol. 35, no. 1, pp. 20–23.
- T. W., Feinstein, D. Y., Thornton, M. A. (2012). "Modelling medical system threats with conditional probabilities using multiple-valued logic decision diagrams", IEEE 42nd International Symposium on Multiple-Valued Logic, pp. 244– 249.

- Pajic, M., Mangharam, R., Sokolsky, O., Arney, D., Goldman, J. Lee, D. I. (2014). “Model-driven safety analysis of closed-loop medical systems”, IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 3–16.
- Wu, P. L., Sha, L., Berlin, R. B. Goldman, J. M. (2015). “Safe workflow adaptation and validation protocol for medical cyber-physical systems”, in 41st Euromicro Conference on Software Engineering and Advanced Applications, 20. pp. 464–471.
- Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T. Maisel, W. H. (2008). “Security and privacy for implantable medical devices”, IEEE Pervasive Computing, vol. 7, no. 1, pp. 30–39.
- Burleson, W., Clark, S. S., Ransford, B. Fu, K. (2012). “Design challenges for secure implantable medical devices”, in DAC Design Automation Conference 2012, pp. 12–17.
- Rushanan, M., Rubin, A. D., Kune, D. F. Swanson, C. M. (2014). “Sok: Security and privacy in implantable medical devices and body area networks”, in Proceedings of the 2014 IEEE Symposium on Security and Privacy, ser. SP ’14, pp. 524–539.
- Zhang, M., Raghunathan, A. Jha, N. K. (2014). “Trustworthiness of medical devices and body area networks”, Proceedings of the IEEE, vol. 102, no. 8, pp. 1174–1188.
- Bonaci, T., Yan, J., Herron, J., Kohno, T. Chizeck, H. J. (2015). “Experimental analysis of denial-of-service attacks on teleoperated robotic systems”, in ICCPS, 15, pp. 11–20.
- Humayed, A., Lin, J., Li, F. Luo, B. (2017). “Cyber-physical systems security a survey,” IEEE Internet of Things Journal.
- Hanna, S., Rolles, R., Molina-Markham, A., Poosankam, P. Fu, K. (2011). Song, “Take two software updates and see me in the morning: The case for software security evaluations of medical devices”, in Proceedings of the 2Nd USENIX Conference on Health Security and Privacy, ser. HealthSec’11.
- Cheng, L., Liu, F. Yao, D. D. (2017). “Enterprise data breach: causes, challenges, prevention, and future directions”, WIREs Data Mining and Knowledge Discovery.