Security Implications in Cyber Physical Systems

Balika J. Chelliah, Ashwin P Ajith, Chirag G Samtani, Dipyaman Paul, Chaitanya Bachhav

Abstract: ***CPS are frameworks that incorporate physical components with the virtual universe of data handling through sensors or actuators. They are made out of different constituent parts that team up to make some worldwide conduct. These parts are programming frameworks, innovative interface, and sensors/actuators that communicate with the present system. CPS regularly incorporate segments from a wide range of specialist co-ops or producers. A CPS exhibits an accumulation of difficulties not constantly found in an established business data framework or inserted framework. A mix of various designing parts is required to build a CPS, spreading over the spaces just as the comparing application divisions, as a control known as frameworks building.***

Index Terms: Cyber Physical Systems; Security; Sensors; Actuators

I. INTRODUCTION

Cyber Physical Systems (CPS) include processing, organizing, and interfacing digital operations with physical procedures. Systems screen and implanted PCs control the physical procedures, with input circles where physical procedures influence calculations and the other way around. Such frameworks have a practical and societal potential which is tremendously more noteworthy than what has been acknowledged, and real ventures are being made worldwide to build up this innovation. In Cyber Physical Systems the physical procedures and programming and systems administration are coordinated, giving deliberations and displaying, structure, and investigation techniques. The basic foundations will be engaged by these frameworks, they can possibly altogether sway everyday lives as they structure the reason for keen administrations. Then again, the expanded utilization of CPS has its very own disservices that could have significant ramifications for clients. Security issues or digital assaults around there have turned into a worldwide issue.

Revised Manuscript Received on April 14, 2019.

Balika J. Chelliah, Assistant Professor, Department of Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India

Ashwin P Ajith, Undergraduate Student Department of Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India

Chirag G Samtani, Undergraduate Student Department of Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India

Dipyaman Paul, Undergraduate Student Department of Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India

Chaitanya Bachhav, Undergraduate Student Department of Computer Science & Engineering, SRM Institute of Science and Technology, Chennai, India

In this way, planning secure and effective CPS is a functioning zone of research. Security issues are just the same old thing new, yet progresses in innovation have made it important to grow better approaches to manage new rising dangers. These new dangers will keep on being misused and digital assaults will keep on occurring, consequently the requirement for new techniques to ensure any CPS. This paper centers around the security issues at the diverse layers of CPS engineering, surveying the hazard and different systems for verifying CPS. At last, challenges, zones for future research and conceivable arrangements are exhibited and discussed. The security implications for cyber physical frameworks are enforced by the Cyber Physical Systems Security (CPSSEC).

Cyber Physical Systems frameworks are a wellspring of upper hand in the current technological innovations and economy, thus developing new opportunities for multiple enterprises. Subsequently, CPS and IoT also increase various cyber- security risks and attack surfaces and vectors. The consequences of unintentional or intentional attacks could have severe impact on human lives. Fig. 1 State Flow Diagram of CPS. As nowadays all the nodes are connected to the internet and immense amount of data is being transferred, bold and harmonized efforts are required to improve security. Though there are many existing systems which take care of the security of the Cyber Physical Systems. But the existing systems do not register dynamic security changes, which may lead to the Cyber Physical Systems being left vulnerable to various attacks.

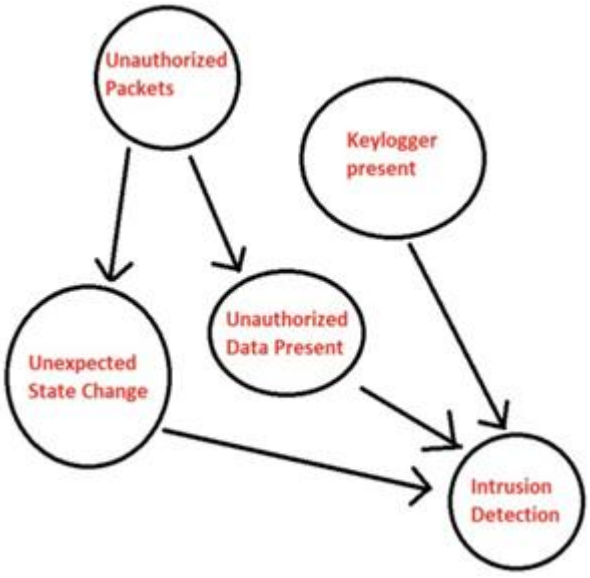

Fig. 1 State Flow Diagram of CPS

II. BACKGROUND AND RELATED WORKS

A. Attack Detection based on model and Mitigation to Generate Automatic Control

Digital frameworks assume a basic job in improving the effectiveness and unwavering quality of intensity framework activity and guaranteeing the framework stays inside safe working edges. A foe can cause extreme harm to the basic physical framework by bargaining the control and observing applications encouraged by the digital layer. Insurance of basic resources from electronic dangers has generally been done through customary digital safety efforts that include have based and organize based security innovations.

In any case, it has been perceived that profoundly talented assaults can sidestep these security instruments to upset the smooth task of control frameworks. There is a developing need for digital assault strong control rules that look past conventional digital safeguard instruments to find exceedingly talented assaults. Accompanying commitments regarding the assault analysis are made.

A general structure to the utilization of assault flexible control to control frameworks as a synthesis of brilliant assault identification and relief. A model-based oddity discovery and assault alleviation calculation for AGC is built. The discovery ability of the proposed oddity identification calculation through reproduction ponders is assessed. The outcomes prove that the calculation is equipped for recognizing scaling and slope assaults with low false positive and negative rates. The proposed model-based relief calculation is additionally effective in keeping up framework recurrence inside adequate points of confinement amid the assault time frame.

B. Adaptive Security Enforcement

The purpose of a Cyber Physical system is to take real time data from the physical world, using its array of sensors and actuators, and then feed the collected data to the cyber systems, or computers, so that they can be processed and used to produce the desired results. Rapid in the field of advances in science and engineering improve the bond between virtual and physical components through smart security mechanisms, that improve the resilience, capability, purpose, reliability, safety, and usability of cyber-physical systems.

In such systems main focus is on the relationship between the physical and cyber elements and how do they play their part. The major focus is on the importance of protection of both the cyber and physical elements from various attacks.

C. Human-On-the-Loop Paradigm for Security Aware System

Analysis of the impact of human interaction with a system is considered in the security aware systems design. Unmanned vehicles and unarmed weapons can act autonomously due to enhancement in this particular area, the major objective is to improve usability of the interface[2].

D. Design Implementations in CPS Framework

The concept of cross-layer design framework for resource constrained cyber physical systems proves to be helpful in enforcing security. A combination of close loop feedback modules on the operational layer and cyber-security techniques at the embedded platform layer is present in the framework.

E. Determination of Attack Severity

A quantitative hierarchical assessment model that comprises of attack severity, a technique for evaluation of the cyber security risk of CPS, attack success probability and attack con- sequence is proposed, this is capable enough for assessment of the risks posed by an ongoing attack at host level and system level.

F. Registering Topological Changes Dynamically

The main objective is development of adaptive security systems and protection of important virtues in case operational environment changes. Engineering a topology aware security system is proposed, this is achieved by identifying violations of security requirements which may be result of topological changes, this involves preventing violations by selecting a set of security controls.

III. DESIGN AND IMPLEMENTATION

A. Problem Statement

The existing cyber-physical systems are prone to a number of attacks due to the lack of proper security measures. In the information age cyber-physical systems are an integral part of every organization, the attacks on them may disrupt the regular operations of the organization. The lack of adaptive security leaves these systems vulnerable creating huge security gaps.

B. Architecture

The major parts of the architecture are Authentication server, Ticket Generating Server and the controller, all these parts are processes that run in the computer shown in Fig. 2. The signals must undergo various processes like in the speculative threat analysis module, which ensures safety from unwanted or malicious devices.

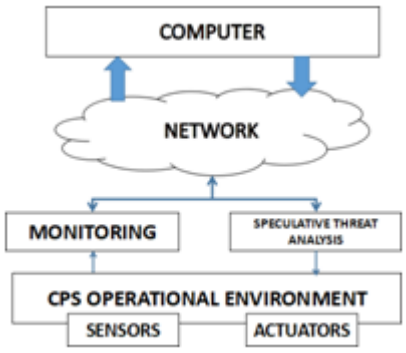

Fig. 2 Proposed Architecture

1) Sensors: Sensors are one of the most pivotal components of the Cyber Physical Operational Environment. The devices communicate with the system using signals, the sensors re- ceive these signals and pass them on for further processing. Any changes in the environment will be initially detected by sensors, they form

the first screening filter in the cyber- physical systems. The signals received by sensor must undergo proper security check so that the system remains impenetrable.

2) Actuators: Actuator selection forms the basis of the cyber-physical system framework. They are used to automate certain tasks when received signals initiate a particular process. A series of activities are triggered due to them, these activities directly affect the cyber-physical environment and may cause major changes in the security framework.

C. Bigraphical Reactive Systems

Bigraphs are pictorial calculus for representation of logical and syntactic systems in terms of correlations and locality.

1) Authentication: In order to ensure that unauthorized devices or users do not penetrate the system, all the devices must go through an authentication procedure. The devices that try to gain access, forward a request to the Authentication Server (AS), which then responds by sending a pre- authentication request. The client then sends authenticator key + client- timestamp. The key is encrypted, if proved to be valid the Ticket Granting Server (TGS) sends a TGS key and session key. The client decrypts the session key, the TGS key includes a copy of session key, ticket lifetime and server- timestamp. Once the client gains these credentials then it can send authenticator to the main server, access is granted once the main server sends confirmation.

2) Trespass Detection: Any uncertainties regarding the signal characteristics must be eliminated, each signal is processed so as to detect maleficence, the signal response will be sent based on whether it is determined to be safe or not. Malicious signals will be identifies and the CPS will be notified of their presence.

Bigraphs can be represented as combination of multiple graphs and trees. Each node represents device connected in the sys- tem. A combination of nested nodes in present in the Bigraphs. They are used to depict distributed systems for omnipresent processing, using Bigraphs the topology of virtual and tangible spaces is dynamically represented, this helps in modelling the system efficiently so as to study and identify the various topological configurations that may manifest during critical operations. These models can be used to perform speculative threat analysis by model checking so that the effect of the expansion of topological configurations on the contentment of security requirements can be calculated.

D. Modules

1) Speculative Threat Analysis: Module checking is implemented, in order to generate space representation that represents breach in security requirements due to sceptical actions of the devices or representatives. The component that performs analysis receives the attributes of the signal which may cause changes in system configuration. This entire process is crucial in enforcing security when it comes to the ever- changing topologies of the system. The objective of this module is to analyze the configurations, followed by identification of vulnerabilities. All the security violations amidst the accountable requests will be marked so that necessary security measures can be implemented.

Monitoring: The system consists of multiple devices, which may need certain privileges to gain access to other components which form an integral part of the CPS. It is necessary to enforce accountability in any system to successfully identify the threats. If there are no records that contain details of the actions performed, it becomes difficult to identify malicious requests or actions. Monitoring involves generation of logs, these logs provide information requests made, requests granted, actions performed along with the details of the device/user performing said actions.

Algorithm 1 Trespass Detect

```
Result: S = s{, s4, s5, . . .}
procedure TRESPASSDETECT(sigVector)
set S=
while sigVector do
    if sigVector.peek().isvalid then
        S.add(sigVector.peek())
        sigVector.del()
    else
        continue
    end
end
end procedure
```

An empty set is created initially and all the signals are present in a vector, if a signal is found to be compromised or harmful it is added to the set S, the sources of these signals are identified through logs maintained by the monitoring system.

5) Signal Vector Verification through Stochastic Local Search: Every signal is assigned a valid bit which may have values 0 or 1, based on this bit it can be determined if the signal is safe or not. All the signal value combinations are inspected. If they are valid the signal is added to the safe zone. This process is repeated as and when needed to ensure the strength of the security system.

IV. RESULTS AND DISCUSSIONS

A. Results

The directed bigraph which is generated cannot be used unless it is converted to a platform independent object, using DBtk the nested links are converted into usable objects that can be linked with an Object-Relational Model. The resultant bigraph is translated into SVG-format that is based on XML. Fig /refpicture 3 depicts the access control vs security level when CPS security techniques Σare implemented (black) and when they are not applied (red).

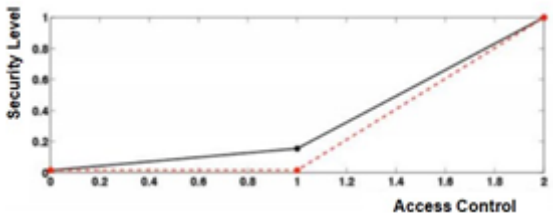

Fig. 3 Changes in Security Level w.r.t Access control

B. Design Framework

Design Automation can be implemented by expanding the Artificial Intelligence Design Framework (AIDF). This will result in dynamic development of specific framework for the cyber-physical environments. Incorporating AIDF will help eliminate the security gaps which may arise during the design phase. Thus, the system vulnerabilities can be minimized.

C. Threat Analyser

Attacks on the cyber physical systems can be anticipated based on the objective of the processes initiated or requests made. All the past requests and actions can be looked-up in the logs, this proves to be helpful in analysing requests for malicious intent. Patterns can be identified and analysed so that threats can be detected before major damages occur, by implementing required security measures.

D. BigWb

BigWb is a graphical evolution environment for bigraphical reactive systems. Its objective is to provide a merged GUI for bigraph tools. It is used to link bigraphs based on their causative classification. The link graph is used to connect the various sites of bigraphs. A matching tool engine is used to infer the changes in system topology, however the rules of doing so are non-deterministic.

The directed bigraph which is generated cannot be used unless it is converted to a platform independent object, using DBtk the nested links are converted into usable objects that can be linked with an Object-Relational Model. This helps in generation of the IPO (ide

E. Limitations

Reconfiguration is difficult, as if system breach occurs entire environment is compromised and the complete system must be rebuilt from scratch

F. Future Work

More sophisticated and anticipatory sensors can be incorporated in the cyber physical system that are capable of automating trivial security tasks, thus preventing mundane checkpoint regulations. Cyber Physical System Design Automation Framework is substantially better than regular AIDF, it certainly provides more dynamic responses proving to be much easier to implement.

V. CONCLUSION

This paper proposes implementations of adaptive security in Cyber Physical Systems, thereby preventing loss of sensitive information, or resources, from being accessed by unauthorized people. The Adaptive security makes sure to update the security policies whenever there is a certain change in the network topology by enforcing accountability and data integrity.

REFERENCES

1. Christos Tsigkanos, Liliana Pasquale, Carlo Ghezzi and Bashar Nuseibeh, “On the Interplay Between Cyber and Physical Spaces for Adap- tive Security,” IEEE transaction on Dependable and Secure Computing, vol. 15, no .3, August. 2018.
2. Mahmoud Elfar, Haibei Zhu, Adithya Raghunathan, Yi Y. Tay, Jeffrey Wubbenhorst, M. L. Cummings and Miroslav Pajic, ”WiP-Abstract: Plat- form for Security-Aware Design of Human-on-the-Loop Cyber-Physical Systems”, IEEE 8th International Conference on Cyber-Physical Sys- tems, April. 2017.
3. Bowen Zheng, Peng Deng, Rajasekhar Anguluri, Qi Zhu and Fabio Pasqualetti, “Cross-Layer Codesign for Secure Cyber-Physical Systems,” IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Volume: 35 , Issue: 5 , May 2016.
4. Wenbo Wu, Rui Kang and Zi Li, “Risk assessment method for cyber security of cyber physical systems,”2015 First International Conference on Reliability Systems Engineering, October. 2015.
5. Christos Tsigkanos, Liliana Pasquale, Claudio Menghi, Carlo Ghezzi and Bashar Nuseibeh, “Engineering Topology Aware Adaptive Security: Preventing Requirements violations at Runtime, IEEE 22nd International Requirements Engineering Conference, August. 2014.
6. Giedre Sabaliauskaite and Aditya P. Mathur, “Intelligent Checkers to Improve Attack Detection in Cyber Physical Systems, International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery,” October. 2013.
7. Jin Wei and Deepa Kundur, ”Two-tier hierarchical cyber-physical security analysis framework for smart grid, IEEE Power and Energy Society General Meeting”, July. 2012.
8. Kenneth Kofi Fletcher and Xiaoqing Liu, ”Security Requirements Anal- ysis, Specification, Prioritization and Policy Development in Cyber- Physical Systems, 2011 Fifth International Conference on Secure Soft- ware Integration and Reliability Improvement - Companion”, June. 2011.
9. Wei Jiang, Wensheng Guo and Nan Sang, ”Periodic Real-Time Message Scheduling for Confidentiality-Aware Cyber-Physical System in Wire- less Networks”, August. 2010.
10. B. McMillin, ”Complexities of information security in Cyber-Physical Power Systems, IEEE/PES Power Systems Conference and Exposition”, March. 2009.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication