Security Aspects of Cyber Physical Systems

Ibtihaj Ahmad, Muhammad Kaab Zarrar, Takreem Saeed, Saad Rehman
Department of Computer Engineering, College of EME,
National University of Sciences and Technology, Pakistan

***Abstract*—Cyber Physical System (CPS) is one of the emerging technologies of the day due to its large number of applications. Its applications extends to automotive, commercial, medical, home appliances and manufacturing industries. Mass research is being conducted in this area including design models, signal processing, control system models, communication models and security. One of the most important aspects of these is security and privacy of CPS. There are a number of vulnerabilities and threats that can be used by an attacker to exploit a cyber physical system. This paper provides a brief review of current security threats, vulnerabilities and its solutions for CPS. For the sake of simplicity the security threats have been divided into two classes i.e. control security and information security. Based on this division various attack methods and their possible solutions have been discussed.**

***Index Terms*—Cyber Physical System, CPS, CPS Security Aspects**

I. Introduction

IN last couple of years a new set of emerging technologies has risen, known as Cyber Physical System (CPS). A cyber physical system can be defined as a segregation and interaction of various physical systems with the cyber systems. More briefly CPS is a web in which various physical and nonphysical systems are controlled by an embedded system, which usually takes its decisions based on input of other physical systems, usually sensors network. These decisions are based on complex data, collected from surrounding and its processes. In order to understand CPS comprehensive knowledge of embedded systems, physical processes, physical systems, control systems, communication systems, networking and software is required..

There are a large number of systems which can be classified as cyber physical system. Modern sophisticated cars are the good example of a CPS's. These cars consist of various sensors like pressure sensors, accelerometer, gyroscopes, thermo sensors etc. The main processor in the car system is connected with these sensors. It gets a complete sensation of outside physical environment. On the basis of data generated by these sensors the cyber system takes various decisions for automatic control of acoustics, cooling, suspension, driving safety and ease etc. All of these physical systems are in close communication with the central cyber system in real time. Other applications of CPS' may include unarmed vehicle (UAVs), power systems [1] such as smart grids, autonomous vehicles, education systems [2], medical [3], manufacturing [4] and industrial applications [5] etc. All these examples can be categorized as autonomous real time, sensor-based communication-enabled systems having data storage capability. Note that CPS has various similarities with IOT still its different from IOT [6]. In CPS, physical and cyber systems are in close communication with each other. CPS has more control element and internal communication, while IOT is the connection of many physical objects. IOT has more aspects of external communication. However some researcher still thinks that CPS and IOT are the two faces of same technology [7] [8]. Regardless of all this debate, one can agree on the fact that CPS and IOT share common security risks.

In future there may be a verity of applications of CPS. As the applications grow the CPS will have to face various challenges like more complex signal processing, control theory, communication, networking, security [9], embedded system challenges etc. But the most important aspect of these will be the security aspect. To understand the severity of this problem, lets take the example smart grid [10]. A smart grid provides facility of automated billing, could be attacked. The attack may be in the form of false energy units data. This may cost financial loss to the company. Another example of the security threat is Smart House, which may share personal data with online cyber system, may be attacked in order to steal personal data. These concerns make the security side of the picture more attractive to researchers.

By 2020, it is expected that we may have more than 30 billion of CPS and IOT devices. With that much growth the burden of strengthening the security also increases. The security of these systems is becoming a challenge for the designers. This have been reflected in a survey conducted by PWC, which says that in 2015 38% more cyber related security incidents were detected than in 2014. A similar survey conducted by SANS [11] found that attacks on control systems of CPS's has increased from 27% to 32%. While attacks on information system of CPS's has increased from 14.5% to 30.25%. The results can be seen in Fig.1. From these surveys it is also observed that the physical systems are less vulnerable to attacks as compared to cyber systems. In future CPS designers must have to work hard to overcome the security challenges especially those CPS's which are connected with Internet.

This paper gives a brief review of various aspects of a CPS's security, vulnerabilities and their solutions. The paper

978-1-5386-4427-0/18/$31.00

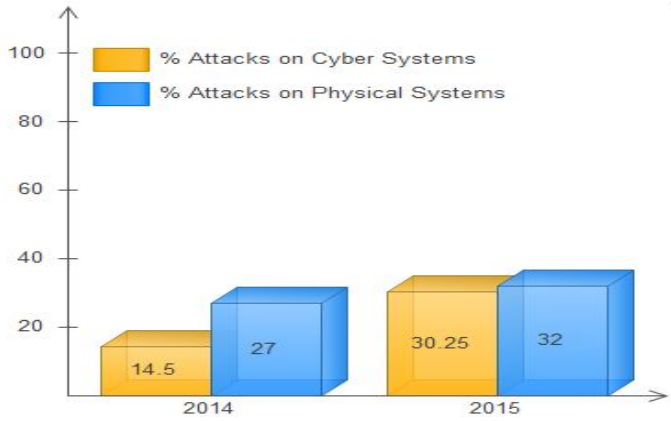

Fig. 1: Comparison of security incidents (2014-2015)

suggest the division of threats to CPS's into two basic types named control security, which is related to physical systems and information security, which is related to cyber systems. Based on this division various potential threats that a CPS can face are identified. Also the solutions to these security problems have been discussed.

II. Methodology

Security threats and Privacy is one of the most critical aspects of CPS especially when its cyber part is connected to internet. In CPS several of its components share enormous information and data with each other. To understand the CPS security in a better way, we have divided it into two main types, i.e. information security/vulnerabilities and control security/vulnerabilities. Control vulnerabilities involve attacks on sensors; actuators, small devices and their controllers while information vulnerabilities involve other cyber systems like embedded system, communication, networking, databases and cloud services. Table II shows various security risks and its solutions based on the above division.

To understand this classification lets take an example of smart home. Smart home consist of various devices categorized as sensors, actuators and cyber controllers. These devices may include, temperature sensors, photo sensors, proximity sensors, heating system, smart devices and small appliances etc. All these devices are connected to a cyber system via Internet or local net. They share a lot of data. Sometime the data may be stored on server for analysis or book keeping or for big data analysis. All of these devices combine to make concept of smart home. Such a CPS makes our life easier however it also raises security concerns and threats to our personal life. Before implementation of a CPS designers must fulfill security and integrity of private data.

A. Control vulnerabilities

This section can be further classified into vulnerabilities and risks related to sensors, their controllers and the interconnection or inter system communication. There may be attacks on sensors directly corrupting the original data by injecting false data through physical breach. The system may also be attacked by attacking the sensors controllers. This problem is a bit more serious due to the fact that controllers are usually directly connected to the cyber systems. Along with control systems, physical system inter communication network can also be used by an attacker to attack CPS. All such possibilities are discussed in detail below.

1) Physical Exploitation: In CPS one of the easiest attack for an attacker is physical exploitation of hardware and sensors network. Such an attack is more prominent in open access CPS whose sensors network is easily accessible to public. In such case the attacker may physically play with hardware. To understand this lets take an example of smart energy meter, Itron Centron [23], which automatically calculate electrical energy and send it to the company. This energy meter can be easily exploited. It is because of easy hardware access to the attacker. The attacker may corrupt the data by corrupting the sensing devices. This may cause financial loss to the company. One of the solutions of such hardware vulnerabilities is introducing smart protected hardware. For example in case of energy meter the sensor and its internal circuitry must be properly sealed. It may be able to generate alarm in case of any tempering with the seal.

2) System Model Estimation: In some cases the attacker may try to figure out the model of the control system of CPS. This is done by observing the data flow between sensors, actuators and its control system. After the model is known, he may then launch various attacks. So the basic purpose of knowing the model is to completely exploit all vulnerabilities of the system. Such Attack is known an Key plan text attack. Yuan [13] suggest that KPA can be used against a CPS. The main target of such attack is the closed loop control system. The mathematical model of KPA can be seen in Eq.(1). Where S(Z) is the system transfer function, $S^{-1}_{CL,12}$ is closed loop transfer function and $S_{C.TF}(z)$ is the controller transfer function.

$$S(z) = (I - S^{-1}_{CL,12})S_{C.TF}(z) \tag{1}$$

The solution to this attack method is implementing encryption in a controller. Usually the controller has not that much high computation capability. This may affect the controller performance. However this security measure is necessary and the designer has to make tradeoff between performance and security.

3) False Data Injection Attack: Another common attack method known as False Data Injection Attack (FDIA) [17] [18], may be a potential threat for CPS. This method involves the injection of false sensor data into the sensor controller by an attacker. Such attack methods can be mainly used to attack smart grids, smart homes and commodity CPS. Usually such attack is more commonly launched against a type of CPS

TABLE I: Related Work

Ref	Name	Problem Discussed	Solution Proposed	Remarks	About Paper
[12]	Security analysis on consumer and industrial IoT devices.	✓	✓		In this paper security of industrial IoT devices is analyzed with respect to hardware, software and networks and various backdoors are identified.
[13]	Security in cyber-physical systems: Controller design against known-plaintext attack	✓	✓	More effevtive, as solution require less computations	This paper defines a necessary condition with the help of which an attacker can find the transfer function of the physical system by using input and output data. This method is commonly known as Known Plaintext Attack.
[14]	Countermeasures to Enhance Cyber-Physical System Security and Safety	✓	✓	90% efficient. Effective for run time applications	A new method based on Intelligent Checker (IC) and Cross-correlator is introduced in order to detect system failures due to security loopholes
[15]	False Data Injection Attacks against State Estimation in Wireless Sensor Networks	✓	✓	It's assumed that system is equipped with failure detector	This paper present the effects of FDIA on state estimation of the sensor networks of a CPS.
[16]	Intelligent Checkers to Improve Attack Detection in Cyber Physical Systems	✓	✓	Not Tested	This work suggest a novel theory of intelligent checkers to improve CPS's security.
[17]	Efficient Prevention Technique for False Data Injection Attack in Smart Grid	✓	✓	FDIA Prevention is Guaranteed	This paper presents a prevention technique for FDI attack which is common in smart grids.
[18]	A Deep Learning-Based Cyber-Physical Strategy to Mitigate False Data Injection Attack in Smart Grids	✓	✓	Deep learning based solution is efficient for FDIA	This paper suggests the effectiveness of a deep learning based strategy to detect false data injection attack and defend the system in real time.
[19]	Attack Detection and Identification in Cyber Physical Systems	✓	✓	Provides a centralized attack detection	This paper proposes a security framework for CPS under attack. It proposes attack detection for centralized and distributed attacks.
[20]	Cyber Physical Systems: Dynamic Sensor Attacks and Strong Observability	✓			In this paper, the necessary conditions for undetectable dynamic sensor attacks against cyber-physical systems are introduced.
[21]	Design and Evaluation of Feature Distributed Malware Attacks against the Internet of Things (IoT)	✓			The paper discusses security of IoT based smart homes. It identifies a security lapse by developing an advanced malware known as feature distributed malware for the IoT.
[22]	A Threat to Mobile Cyber-physical Systems: Sensor-based Privacy Theft Attacks on Android Smartphones	✓			A sensor-based cyber-physical voice privacy theft trojan horse (CPVT) has been introduced in this paper, which is operated in real time by the attacker.
[23]	Introduction to Cyber-Physical System Security:A Cross-Layer Perspective	✓	✓		Various security risks have been identified based on various layers of cyber physical system.
[24]	Defending Cyber-Physical Systems against DoS Attacks	✓	✓	23 packets required for forward path	This paper propose a counter method for DDos attack which is based on probabilistic packet marking scheme to deduce forward paths from an attacker to a victim site.
[25]	Dataset of anomalies and malicious acts in a cyber-physical subsystem	✓			This paper consists of a database that is designed to study how information quality estimation helps in detecting anomalies and malicious acts in CPS.
[26]	Cyber security attacks to modern vehicular systems	✓			This paper discusses various expects and approaches to prevent and detect common attacks on the modern cyber physical vehicular systems
[27]	Taxonomy for description of cross-domain attacks on CPS	✓			This paper presents a taxonomy to describe common attacks on CPS. It classifies both conventional CPS attacks as well as cross-domain CPS attacks. Further, it explains quantitative and qualitative analysis of these attacks.
[28]	Covert Attacks in Cyber-Physical Control Systems	✓	✓		This paper aims to explore vulnerabilities and propose security solutions for cyber-physical systems by introducing a covert attack for service degradation.
[29]	A game-theoretic approach to model and quantify the security of cyber-physical systems	✓		Present an approach to evaluate security of a CPS	This paper classifies CPS security into two parts of intrusion and disruption. A game-theoretical methodology is introduced to study the relation between an attacker and the victim.
[30]	A multi-layered and kill-chain based security analysis framework for cyber-physical systems	✓	✓		In this paper progressive stages of an attack on a CPS is discussed. The stages contain the attackers objective, cyber profiteering, control-theoretic and physical system properties.
[31]	Dynamic attack detection in cyber-physical systems with side initial state information	✓	✓		This paper aim to highlight the effect of initial zero state information to detect the attacks on CPS. It also provides a design for dynamic attack detector.

which has wireless sensors network [15]. The ultimate reason of such attack may be the prevention of a physical device or actuator to work properly or financial loss to company (as in case of smart grid). FDIA can be effectively be identified using cross correlator [14]. Intelligent checkers (IC) [16] can also be one of the prevention method from FDIA. One of the closest neighbor of FDIA is dynamic sensor attack. In this method the attacker use the intercommunication vulnerabilities between sensor network and its controller. The attacker may change the physical behavior of the physical system by simply stopping the true data and feed false data into the controller by playing with sensors physically or through cyber system (in case of wireless network). This attack method can be modeled according to Eq.(2) and (3).Where x(n) is current system condition, while y(n) is the sensors measurements. K represent system dynamics, l is sensors network and k is the attack methodology.

$$x(n+1) = Kx(n) \tag{2}$$

$$Y(n+1) = lx(n) + kx(n) \tag{3}$$

Chen [20] defines the counter measure to identify this sought of attack and take corrective measures. It uses the dynamic property of the system to provide strong observibility of the physical and control system. Another solution of such potential problem is to include a security layer in smart devices and sensors. This may decrease the performance due to the fact that sensors and other small devices have lower computational power.

4) Zero State Inducing: Zero state inducing is an attacking technique that can be perpetuated for an arbitrary long time beginning at time zero. In zero state inducing attack the change in output is equal to the response of the system when its initial state is zero i.e. x(0) = 0. In such attack an attack $E(T)$ occur against a system $\sum$ happening at time zero of the system state. Mathematically, $MTE(T) = 0$ when $W1V(\sum)_{=}0$. W1. These attacks occur on the CPS systems weak monitored places $V()$ while the output of these places at that time W1 is non zero. Usually zero state inducing attack is almost undetectable.

B. Information vulnerabilities

Information vulnerabilities include loopholes in cyber systems especially those parts of CPS which are connected to local networks or internet. The internet connectivity of CPS makes it open for remote attacks like Malware, Viruses, Trojan horse, Backdoors etc. It increases the attack chances to a very great extent. Attack choices of intruder may include attack on embedded system, database, communication system etc. Various attack methods that can be used for this purpose are shown in Table 1. We will discuss all of these one by one.

1) Bootstrap Vulnerabilities: One of the major risks to CPS is at the time of system boot up. At boot up time the system loads resources with the help of bootstrap program. Usually a typical bootstrap program has no security guarantee. There is no mechanism to stop the execution of an unauthorized program which is a kind of security threat to CPS. Parno [32], Parno [33] and Arbaugh [34] explains this problem and its solution. A secure boot strap program includes code authorization. Before executing any code it authorizes that code. The authorizing usually occurs via signature of trusted authority. Any code that is unauthorized is immediately stopped from being executed. It slows down boot process but at the same time it adds up security layer to the system.

2) Malware: According to [35], Malwares (software that can grant unauthorized access to any system and gather sensitive information) are one of the potential threat to the CPS. Malware can damage or corrupt CPS's like smart homes, smart grids etc. It can steal sensitive data or it may induce anomalous behavior of physical systems. [21]introduce an attack method known as FDM (feature distributed malware) which can be used against Internet enabled CPS. The proposed method launches attack on the low computation and less secure smart devices like, network cameras, LEDs etc. This attack method targets the smart sensors and other low cost devices due to the fact that they have less security and are easy to be targeted as compared to other high computation cyber systems. It then uses their service connection to launch other malicious attacks. One serious concern associated with such attacks are D-Dos attacks, which is briefly discussed down the paper.

3) Man-in-the-Middle: Man-in-the-middle attack in CPS happens when an attacker tries to eavesdrop on the communication between a cyber-system and the server. The attacker inserts himself into the communication and may inject false information and intercept the data transfers between a cyber systems. Packet injection, session hijacking [43] and SSL stripping [44] are common techniques of Man-in-the-middle Attack. These attacks can be prevented by using virtual private network for the communication in a CPS. One of the sub type of MitM is spoofing, where an attacker tries to act on another persons behalf in order to gain illegal access to the system. Spoofer initiates the communication from an unknown source but tries to act as a reliable source or IP address. Three common types of spoofing attacks are ARP spoofing attacks, DNS spoofing attack and IP Spoofing attack. These attacks are usually created and launched on networks to steal information or to access systems confidential information. Spoofing could be avoided by packet filtering or by using a secure encryption protocol i.e. Secure Shell, HTTP Secure. Prevention of such attacks also include methods like DVCerts and DAPS e.t.c.

4) Service Degradation: Another attacking method called service degradation attacks reduces the overall efficiency

TABLE II: Classification of various Attack Methods

Attack Classification	Attack Target	Attack Method	Effective Solution for CPS	References
Control	Hardware	Physical Exploitation	Smart Hardware	[12]
Control	Control System	Plain text attack	Improved Controller design	[13]
Control	Sensors and Controller	False Data Injection Attack	Cross Correlation, Intelligent Checker, Encryption	[14] [15] [16] [17] [18]
Control	Sensors	Dynamic Sensor Attack	Design Improvement and strong observability	[19] [20]
Information	Embedded system	Boot Process Attack	Root of Trust, AEIGS	[32] [33] [34]
Information and Control	Internet services for sensors	Feature Distributed Malware	Increase sensor security	[35] [21]
Information	Remote Communication	Backdoor Remote Access and Trojan Horse	Depends on the type of attack	[36] [37] [22]
Information	Software	Software Exploitation	Updates	[23]
Information	Embedded Systems	Denial of service(Dos)	Forward Path, Patches	[38] [24] [39]
Information	Communication	MITM	DVCert, DAPS	[27] [26] [25] [30] [40] [41]
Control	Contol System	Zero State Inducing Attack	Dynamic Attack Detector	[31]
Information	Control/Cyber Systems	SD Attack	Network Segmentation, Firewall policies	[28] [29] [42]

of the system while applied in a control loop. They may reduce the efficiency of physical systems in the CPS or they may decrease the mean time between failure (MTBF) of the system in a long run by inserting some false value data into the system. Attacker sometime degrades the system by causing steady state error or by inducing an overshoot during the transient response of the system. This may cause damage to physical systems in CPS i.e. mechanical, chemical or electromechanical systems. Prevention of such attacks is possible by increasing the difficulty to access to the control loop of the system which can be achieved by applying network segmentation, firewall policies and demilitarized zones in the system.

5) Backdoor: A backdoor is a computer program which enable an attacker to gain unauthorized access and maintain access to a cyber system. After granting access the attacker may then launch various attacks. Nasser [36] gives brief a detail of backdoor attack. It also tells us about system backdoors and application backdoor. A system backdoor may be a major security concern for CPS as it target point is design of hardware like FPGA and other embedded systems. Backdoors may either created by company for remote administration or by an intruder. Companies usually create system backdoor while application backdoors are usually created by the attacker. One of the most common method to create application backdoor is to use Trojan horse. Example of the Trojan horse attack in smart phone CPS, known as CPVT, is explained in [22]. It shows how sensors of a smart phone can be used to steel private data.

6) Software: Any hardware in CPS is driven by software which is usually similar to the general cyber systems like our PC's. So the vulnerabilities found in these systems may also be a threat for the CPS [23]. However there is an advantage of this similarity i.e. some of the software updates are always available to CPS when released for these generalized systems. Sometime the cyber system may also need its own software updates. Langweg [45] shows classification of software attacks that may be threat to CPS.

7) Denial of Service: When the system resources are over flooded such that the privileged legitimate user is unable to access or use a system resources then it is called as Denial of service (DoS) Attack. A more severe and effective version of DoS is Distributed DoS (DDoS) in which a large number of hosts attack the target simultaneously. On October 21, 2016 the biggest Distributed DoS attack was launched against Dyn servers in USA through the small CPS and IOT devices, bringing down sites like Twitter, CNN, and Guardian etc. This incident shows that small non secure CPS devices may not only be a security risk for themselves but also for other systems. Ar [38] shows various DoS attacks and its classifications. Solutions to this problem are implementation of better network infrastructure, DoS mitigation capability in the CPS device itself or at the adjacent cloud network. Nur [24] also suggest a solution for this problem which is based on forward path to the target.

III. Conclusion

In this paper we introduced various security risks and vulnerabilities that may affect cyber-physical systems. These were classified into two categories i.e. Control vulnerabilities and Information vulnerabilities based on cyber and physical layers. Various attack methods from each class were critically discussed. The possible solutions to these security concerns were also discussed. In future enormous growth is expected in CPS application. With growth the security concerns would also rise. The designers would need to develop more secure model. This paper may act as a basic guide line to design a basic CPS security model.

References

[1] C. Krishna and I. Koren, "Thermal-aware management techniques for cyber-physical systems," *Sustainable Computing: Informatics and Systems*, 2017.

[2] H. Yetis, M. Baygin, and M. Karakose, "An investigation for benefits of cyber-physical systems in higher education courses," in *Information Technology Based Higher Education and Training (ITHET), 2016 15th International Conference on*. IEEE, 2016, pp. 1–5.

[3] J. Pawlick and Q. Zhu, "Strategic trust in cloud-enabled cyber-physical systems with an application to glucose control," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 12, pp. 2906–2919, 2017.

[4] A. J. C. Trappey, C. V. Trappey, U. H. Govindarajan, J. J. Sun, and A. C. Chuang, "A review of technology standards and patent portfolios for enabling cyber-physical systems in advanced manufacturing," *IEEE Access*, vol. 4, pp. 7356–7382, 2016.

[5] T. Järvinen, G. S. Lorite, A.-R. Rautio, K. L. Juhász, Á. Kukovecz, Z. Kónya, K. Kordas, and G. Toth, "Portable cyber-physical system for indoor and outdoor gas sensing," *Sensors and Actuators B: Chemical*, 2017.

[6] J. Wan, H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research." *TIIS*, vol. 5, no. 11, pp. 1891–1908, 2011.

[7] C. Pu, "A world of opportunities: Cps, iot, and beyond," in *Proceedings of the 5th ACM international conference on Distributed event-based system*. ACM, 2011, pp. 229–230.

[8] S. F. Ochoa, G. Fortino, and G. Di Fatta, "Cyber-physical systems, internet of things and big data," 2017.

[9] L. ZHANG, W. Qing, and T. Bin, "Security threats and measures for the cyber-physical systems," *The Journal of China Universities of Posts and Telecommunications*, vol. 20, pp. 25–29, 2013.

[10] A. Stefanov and C.-C. Liu, "Cyber-physical system security and impact analysis," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 11 238–11 243, 2014.

[11] D. Harp, "Sans 2016 state of ics security survey," June 2016.

[12] J. Wurm, K. Hoang, O. Arias, A. R. Sadeghi, and Y. Jin, "Security analysis on consumer and industrial iot devices," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*, Jan 2016, pp. 519–524.

[13] Y. Yuan and Y. Mo, "Security in cyber-physical systems: Controller design against known-plaintext attack," in *2015 54th IEEE Conference on Decision and Control (CDC)*, Dec 2015, pp. 5814–5819.

[14] G. Sabaliauskaite and A. P. Mathur, "Countermeasures to enhance cyber-physical system security and safety," in *2014 IEEE 38th International Computer Software and Applications Conference Workshops*, July 2014, pp. 13–18.

[15] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *49th IEEE Conference on Decision and Control (CDC)*, Dec 2010, pp. 5967–5972.

[16] G. Sabaliauskaite and A. P. Mathur, "Intelligent checkers to improve attack detection in cyber physical systems," in *2013 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, Oct 2013, pp. 27–30.

[17] A. Abdallah and X. S. Shen, "Efficient prevention technique for false data injection attack in smart grid," in *2016 IEEE International Conference on Communications (ICC)*, May 2016, pp. 1–6.

[18] J. Wei and G. J. Mendis, "A deep learning-based cyber-physical strategy to mitigate false data injection attack in smart grids," in *2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*, April 2016, pp. 1–6.

[19] F. Pasqualetti, F. Drfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[20] Y. Chen, S. Kar, and J. M. Moura, "Cyber-physical systems: Dynamic sensor attacks and strong observability," in *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 2015, pp. 1752–1756.

[21] B. Min and V. Varadharajan, "Design and evaluation of feature distributed malware attacks against the internet of things (iot)," in *2015 20th International Conference on Engineering of Complex Computer Systems (ICECCS)*, Dec 2015, pp. 80–89.

[22] L. Lei, Y. Wang, J. Zhou, L. Wang, and Z. Zhang, "A threat to mobile cyber-physical systems: Sensor-based privacy theft attacks on android smartphones," in *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 2013, pp. 126–133.

[23] J. Wurm, Y. Jin, Y. Liu, S. Hu, K. Heffner, F. Rahman, and M. Tehranipoor, "Introduction to cyber-physical system security: A cross-layer perspective."

[24] A. Y. Nur and M. E. Tozal, "Defending cyber-physical systems against dos attacks," in *2016 IEEE International Conference on Smart Computing (SMARTCOMP)*, May 2016, pp. 1–3.

[25] P. M. Laso, D. Brosset, and J. Puentes, "Dataset of anomalies and malicious acts in a cyber-physical subsystem," *Data in Brief*, vol. 14, p. 186, 2017.

[26] L. Pan, X. Zheng, H. Chen, T. Luan, H. Bootwala, and L. Batten, "Cyber security attacks to modern vehicular systems," *Journal of Information Security and Applications*, vol. 36, pp. 90–100, 2017.

[27] M. Yampolskiy, P. Horvath, X. D. Koutsoukos, Y. Xue, and J. Sztipanovits, "Taxonomy for description of cross-domain attacks on cps," in *Proceedings of the 2nd ACM international conference on High confidence networked systems*. ACM, 2013, pp. 135–142.

[28] A. de Sa, L. Carmo, and R. Machado, "Covert attacks in cyber-physical control systems," *IEEE Transactions on Industrial Informatics*, 2017.

[29] H. Orojloo and M. A. Azgomi, "A game-theoretic approach to model and quantify the security of cyber-physical systems," *Computers in Industry*, vol. 88, pp. 44–57, 2017.

[30] A. Hahn, R. K. Thomas, I. Lozano, and A. Cardenas, "A multi-layered and kill-chain based security analysis framework for cyber-physical systems," *International Journal of Critical Infrastructure Protection*, vol. 11, pp. 39–50, 2015.

[31] Y. Chen, S. Kar, and J. M. Moura, "Dynamic attack detection in cyber-physical systems with side initial state information," *IEEE Transactions on Automatic Control*, vol. 62, no. 9, pp. 4618–4624, 2017.

[32] B. Parno, J. M. McCune, and A. Perrig, "Bootstrapping trust in commodity computers," in *2010 IEEE Symposium on Security and Privacy*, May 2010, pp. 414–429.

[33] B. Parno, "Bootstrapping trust in a" trusted" platform." in *HotSec*, 2008.

[34] W. A. Arbaugh, D. J. Farber, and J. M. Smith, "A secure and reliable bootstrap architecture," in *Proceedings. 1997 IEEE Symposium on Security and Privacy (Cat. No.97CB36097)*, May 1997, pp. 65–71.

[35] B. Min and V. Varadharajan, "Design and analysis of a new feature-distributed malware," in *2014 IEEE 13th International Conference on Trust, Security and Privacy in Computing and Communications*, Sept 2014, pp. 457–464.

[36] O. Nasser, S. AlThuhli, M. Mohammed, R. AlMamari, and F. Hajamohideen, "An investigation of backdoors implication to avoid regional security impediment," in *2015 Global Conference on Communication Technologies (GCCT)*, April 2015, pp. 409–412.

[37] M. Tehranipoor and F. Koushanfar, "A survey of hardware trojan taxonomy and detection," *IEEE Design Test of Computers*, vol. 27, no. 1, pp. 10–25, Jan 2010.

[38] A. Ar, S. F. Oktu, and S. B. . Yaln, "Internet-of-things security: Denial of service attacks," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, May 2015, pp. 903–906.

[39] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun, and L. Zhang, "Interest flooding attack and countermeasures in named data networking," in *IFIP Networking Conference, 2013*. IEEE, 2013, pp. 1–9.

[40] S. Puangpronpitag and N. Masusai, "An efficient and feasible solution to arp spoof problem," in *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009. ECTI-CON 2009. 6th International Conference on*, vol. 2. IEEE, 2009, pp. 910–913.

[41] I. Dacosta, M. Ahamad, and P. Traynor, "Trust no one else: Detecting mitm attacks against ssl/tls without third-parties," in *European Symposium on Research in Computer Security*. Springer, 2012, pp. 199–216.

[42] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "The cicada attack: degradation and denial of service in ir ranging," in *Ultra-Wideband (ICUWB), 2010 IEEE International Conference on*, vol. 2. IEEE, 2010, pp. 1–4.

[43] S. Kapoor, "Session hijacking exploiting tcp, udp and http sessions," *infosecwriters. com/text_resources/.../SKapoor_SessionHijacking. pdf*, 2006.

[44] B. McCorkendale and W. E. Sobel, "Ssl validation and stripping using trustworthiness factors," Jun. 15 2010, uS Patent 7,739,494.

[45] H. Langweg and E. Snekkenes, "A classification of malicious software attacks," in *IEEE International Conference on Performance, Computing, and Communications, 2004*, 2004, pp. 827–832.