International Journal of Electrical and Power Engineering 13 (1): 5-11, 2019
ISSN: 1990-7958

Threat Identifying Cyber Physical Systems Security

Morteza Pakizeh
Faculty of Engineering, Islamic Azad University, Tabriz Science and Research Branch, Tabriz, Iran
Pakizeh.m@gmail.com

Abstract: Critical infrastructures are vital assets for the public safety, economic welfare and national security of countries. Cyber systems are used extensively to monitor and control critical infrastructures. A number of infrastructures are connected to the internet via. corporate networks. Cyber security is therefore, an important item of the national security agenda of a country. These systems will empower our critical infrastructure and have the potential to significantly impact our daily lives as they form the basis for emerging and future smart services. On the other hand, the increased use of CPS brings more threats that could have major consequences for users but advances in technology make it necessary to develop new threats will continue to be exploited and cyber attacks will continue to emerge, hence, the need for new methods to protect CPS. This study introduces a novel framework for understanding cyber attacks and the related risks of multi elements, multi-layered to cyber-physical systems. The longer-term goal is to use the framework as a means to reduce cyber-physical system security properties and to enumerate the principles for designing systems that are resilient to cyber attacks and analysis of the security issues at the various layers of CPS architecture, risk assessment and techniques for securing CPS. Finally, challenges and possible solutions are presented and discussed.

Key words: Cyber security, cyber physical systemsm, security analysis, CPS security, internet, CPS

INTRODUCTION

Cyber-Physical Systems (CPS) are receiving a lot of attentions recently with examples including smart cities, intelligent homes with network of appliances and so on. These systems are equipped with a large network of sensors distributed across different components which leads to a tremendous amount of measurement data available to system operators. The most common applications are military, environmental, health assistant and home applications fields. However, despite its advantages over other types of networks, WSNs have shown shortages related to high energy consumption rate, especially, in CHs, limited processing power, limited memory capacity and low communication reliability (Al-Smoul *et al*., 2016). These physical devices can be identified with physical attributes or information sensing equipment such as infrared sensors or Radio Frequency Identification (RFID) and can then be connected to a networking system, in most cases the internet, to send the captured data to the computational subsystem (Zhang *et al*., 2011). With the increased focus on data handling capacity, data communications capability and integration of information systems as well as physical devices, the demand for integrating CPS in different fields is also, increasing, resulting in widely gained attention not only from universities and research and development labs but also, from industry and government agencies (Lu *et al*., 2015). As an example of CPS, Industrial Control Systems (ICS) are isolated by communication protocols and operating systems from the outer systems. Security concerns ranging from application environment and communication technology should be addressed at the early stages of the design (Gamundani, 2015). However, this exposes CPS to more vulnerabilities and threats (Nourian and Madnick, 2015). As an example, industrial control systems have been considered secure when not connected to the outside world (Nourian and Madnick, 2015) without taking into account insider attacks. Thus, this indicates that the extensive connectivity between cyber and physical components raises the important issue of security. More attacks are expected as many intractions among different components are connected outside of their area to provide better services such as smart grid networks. Perhaps the most infamous cyber-attack on a physical system was the "Stuxnet" virus. Between late 2009 and early 2010, Stuxnet allegedly destroyed as many as 1000 Iranian high speed centrifuges used for uranium enrichment specifically, the lifespans of these centrifuges were significantly reduced by periodically changing their rotational speeds (Albright *et al*., 2010). In addition, to the Stuxnet virus, other examples also, involved cyber-attacks on physical systems such as the "logic bomb" that was reportedly inserted in the Trans Siberian pipeline's control software. This attack changed pump and valve settings, causing a massive explosion in 1982 (Rost and Glass, 2011); in 2016, there was an attack on a power grid

which cut power to over 100,000 people (Tuptuk and Hailes, 2016). These examples demonstrate that no system is beyond the reach by cyber-attackers and intelligent manufacturing systems are no exception. Over the last few years, manufacturing has been one of the most targeted sectors for cyber-attacks by spear-phishing attacks. In addition, the critical manufacturing sector accounted for the most security incidents reported to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (Anonymous, 2015a, b). Most of the efforts in security solutions were based on the available solutions designed specifically for classical Information Technology (IT) systems to develop or create advanced solutions. However, these solutions are not designed for CPS (Wang *et al*., 2010; Konstantinou *et al*., 2015). Additionally, most of the research focuses on the performance, stability, robustness and efficiency of physical systems rather than security which is broadly ignored, usually as a result of constrained factors such as low processing, communication and adequate storage ability capacities. However, if security is disregarded, CPS will not work in a stable manner (Lu *et al*., 2014). Finally, implementing a vulnerability assessment approach will raise awareness among industry practitioners regarding the existence of malicious cyber-physical attacks and their potentially serious consequences and section 2 discusses related CPS security. Finally, section 3 provides our conclusions and future work. By Wu *et al*. (2010) which comes with five layers: business, application, processing, transmission and perception. Even though there are different assumptions about the number of layers, CPS fundamentally operates at three layers: perception, transmission and application (Zhao and Ge, 2013). Each of these layers is defined by the devices within it and the related functions that should be implemented (La and Kim, 2010). CPS architecture as perception (physical) layer, data transmission (network) layer and application (cyber) layer. The first layer is the perception layer, also, called the recognition layer or sensors layer (Mahmoud *et al*., 2015). Devices at this layer have the ability to collect real-time data that is needed for different purposes (e.g., monitoring and tracking), interpret what they receive from the physical world and perform commands from the application layer. The second layer is the transmission layer (also, known as the transport layer (Lu *et al*., 2015) or network layer (Khan *et al*., 2012) which is responsible for interchanging and processing data between the perception and the application. The third and most interactive layer is the application layer. Its mission is to process the received information from the data transmission level and issue commands to be executed by the physical units, sensors and actuators (Zhao and Ge, 2013). This layer works by implementing complex decision-making algorithms on the aggregated data to generate correct decisions and control commands which will be used in corrective actions. In addition, this layer receives and processes information from the perception layer and then determine the required automated actions to be invoked (Khan *et al*., 2012). Typical three layers cyber-physical systems are as follow:

Application layer:
- Smart home
- Smart city
- Smart health

Transmission layer:
- Wi-Fi
- Bluetooth
- Router

Perception layer:
- Sensors
- RFID
- GPS

MATERIALS AND METHODS

Cyber-physical system model: The model layers include the physical layer, control layer and cyber layer. Each layer is defined in detail below.

Physical layer: The physical layer represents the physical rendering of the cyber-physical system. It captures the physical properties of the system and the physical architecture including the decisions involving the process variables that are measured using sensors and the manipulated variables that are controlled using actuators. The physical properties of a system are characterized by the plant dynamics which can be linear or nonlinear, deterministic or stochastic, time varying or time-invariant, hybrid or non-hybrid and fast changing or slow changing (e.g., power grid voltages and currents can change and propagate in milliseconds while chemical processes can take hours to change their states). The architectural properties of the physical layer depend on the numbers of measurements and actuation signals and the specific level of the architectural hierarchy. For example, the massive scale of the electric power grid makes it impossible for a single authority to autonomously control the grid; as such the power grid is controlled as a federated system where each component subsystem is controlled by a single authority but in a decentralized manner. In contrast, the water level in a tank can be maintained via. centralized control using a single sensor and actuator. Physical and architectural decisions also, consider the dimension of the

system of interest. Basic control algorithms are Single-Input-Single-Output (SISO); however, most real-world industrial control problems are complex and rely on Multiple-Input-Multiple-Output (MIMO) algorithms. Just as confidentiality, integrity and availability are core security properties that must be preserved in the face of cyber attacks, there are equivalent control-theoretic properties that must be assured in the physical system. These properties include stability, safety and efficiency. The most important property of a control system is stability. Another important property in control system design is safety, the ability to prevent accidents that harm humans or damage equipment. In control theory, the notion of safety is usually translated to the ability to keep the system state in a desired (i.e., safe) region. Finally, the efficiency of a control system is the degree to which it achieves its purpose or mission. The optimality of a control algorithm is usually measured as its ability to follow reference signals that minimize the costs involved in running the system (e.g., fuel costs and operational costs).

Control layer: Controllability and observability are properties that do not directly affect the output but are useful for analyzing control algorithms. These notions were originally defined for linear, time-invariant systems but they have intuitive interpretations for general control systems. Note that observability and controllability are mathematical duals.

Controllability: This is the ability of an external input to drive the internal system state from an initial state to another state in a finite time interval. A similar notion is output controllability which describes the ability of an external input to drive the output from an initial condition to a final condition in a finite time interval. A system is controllable, if it is possible to execute a control algorithm that can make the system stable.

Observability: This is a measure of how well the dynamic behavior of a system (i.e., internal system states) can be inferred based on information about its external outputs (i.e., sensor measurements). In practice, a system is observable, if it is possible to create an observer (also, known as a state estimator) that can accurately track the system state given sensor measurements. Each control architecture has unique security considerations. For example, in a linear system, an attacker can have a simple attack strategy to destabilize the system; however, in a nonlinear system, an attacker might be able to explore complex dynamics such as finding a resonant frequency of the system.

Cyber layer: The cyber layer is where the control aspects of a cyber physical system are implemented as computerized control systems. This is typically realized through special-purpose hardware platforms. The hardware interfaces with electrical, communications and mechanical subsystems and must be optimized to satisfy real-time computing constraints. The execution platform comprises hardware components such as devices, memory, buses and processors. These components represent the physical aspects of the system. Software components which model code execution, include processes, threads, data and subprograms needed to support execution.

CPS security: In general, the security in CPS is classified into two areas: information (data) security and control security. Information security involves securing information during data aggregation, processing and large-scale sharing in the network environment, especially, open loosely coupled networks. Control security encompasses resolving any control issues in the network environment and mitigating the control system from any attacks on system estimation and control algorithms (Lu *et al*., 2013; Cardenas *et al*., 2011). Information security focuses on data protection, for example by using encryption whereas control security focuses on protecting the dynamics of control systems against cyber-attacks (Lu *et al*., 2015). The sole focus of the remainder of this study is on information security. In addition, to discussing the distinguishing characteristics between CPS and traditional IT systems, this section presents an analysis of the most important security factors, objectives, attacks and risk assessments for CPS.

Distinguishing characteristics: In IT systems, access restriction and control can be applied without affecting the system services. On the other hand, any IT protection measures applied for CPS could affect or delay the real-time response of the physical parts of CPS which usually demand real-time responses. For example, the main risk factors for ICS are consolidated technologies, unified protocols, expanded connectivity and public information access which mostly result in insecure connections (Stouffer *et al*., 2011). Thus, applying IT strategies for CPS may unfortunately affect real-time responses and provide potential adversaries with many new opportunities to disrupt the services provided by the CPS. However, due to the unique characteristics of the CPS, traditional IT security strategies and approaches are not sufficient for addressing CPS security challenges due to the differences in specifications and connectivity from CPS (Nourian and Madnick, 2015). In addition to the three security objectives of traditional IT systems, authenticity is considered as the fourth CPS security objective. Authenticity indicates that all transactions and communications must be guaranteed that are between legitimate parties (Wood and Stankovic, 2008) in all

related processes such as sensing, communication or actuation (Wang *et al*., 2010), hence, ensuring that the source of any action that highly impacts the system was originated and issued from a trusted party (Wood and Stankovic, 2008). In other words, authenticity for CPS seeks to validate both communicated parties and authenticate and verify any related process (Wang *et al*., 2010). Though, confidentiality is ranked the first security objective for IT systems, availability comes first for CPS, then integrity, confidentiality and authenticity. However, authenticity should be ranked first as other security objectives are built on it and any failure to ensure that the right parties are who they claim to be will mean that other security goals will be useless. For example, if an unauthorized (e.g., malicious) party successfully accessed the system, confidential information will be released and the integrity will not be satisfied, since, such a party can manipulate information. Since, in most cases, there will be no human interaction to ensure the authentication process of the connected objects, a robust authentication mechanism must be included to protect the system and make the correct decisions for accepting or rejecting the received instructions and data (Anonymous, 2015a, b). Thus, the most important security factor in CPS is how to ensure proper access control to the system, known as identity-based in traditional IT security (Kirkpatrick *et al*., 2009). Another difference between IT and CPS is that traditional security techniques individually focus on addressing security for system components rather than the interactions among these components. Hence, the main goal is addressing safety (absence of failure) issues rather than security (unauthorized access). To some extent, security and safety analysis and solutions of complex systems can be provided by traditional techniques. However, new issues in such systems such as network heterogeneity, different component interactions and cyber connections are not successfully considered. An example, of such an issue is that a control parameter can be modified as a reason of unsuccessful authentication process. Thus, a security attack happens without failure incidence in the system (Nourian and Madnick, 2015). Hence, in some cases, a system cannot be considered secure with the absence of failure. As a result, applying traditional security techniques to CPS will not fully protect against attacks. Hence, the prime security challenge is the need to consider interactions among CPS components. Although, the three IT security objectives (confidentiality, integrity and availability) are necessary for CPS, they are not sufficient by themselves. If a cyber-system is not accessible, the physical processes will not be controlled and the consequences will be catastrophic (Lu *et al*., 2013), particularly for real-time operations. For example, without a proper confidentiality mechanism, secret data might be captured by an unauthorized party; without an appropriate integrity mechanism, critical data may lead to deception through false data; without adequate availability, the system might not be accessible when needed (Lu *et al*., 2014); without an authenticity mechanism, received data might be sent from an attacker or originated and issued from an unknown party. These four objectives are the four basic security goals of CPS. As CPS perform different processes at various stages and securing devices, data transmissions, applications and data storages and actuation processes are required. The following subsections briefly describe these requirements.

Securing access to devices: Securing access to devices becomes the first challenge. If authentication is not or is poorly supported, unauthorized objects will gain access and manipulate the system (Konstantinou *et al*., 2015), hence, neither trusting any underlying binary codes nor implementation at the application layers will be guaranteed.

Securing data transmissions: Data transmission security is required in order to detect impostors and malicious activities in CPS communication networks and block unauthorized access. As an example, attackers try to intercept the physical properties of system power consumption and timing behaviors to analyze the data being sent and received (Konstantinou *et al*., 2015). Some attackers aim to disrupt networks by launching DoS attacks or interrupting the routing topology (Raza, 2013). Some terminal devices which are not a complete computer system do not have high data processing and communication abilities or adequate storage capacities (Wang *et al*., 2010). This makes these devices more vulnerable to penetration. On the other hand, in industrial control system terminals, connectivity which relies on open networking standards, helps to improve system performance and reduces operational costs. Although, such terminals lead to more efficient and effective operation, they expose the system to higher possibilities of intrusions and malicious attacks such as malicious code (malware), Distributed Denial of Service (DDoS), eavesdropping and unauthorized access (Weiss, 2010). Another factor which directly leads to vulnerabilities is that the designing process is always constrained in processing time (speed), hardware resources and power consumption. Moreover, embedded systems are designed by experts who have limited experience of security issues and focus more on functionality, error corrections and performance than security (Raza, 2013). This, in turn, leads to vulnerabilities in the system which may leak secure information to unauthorized or undesired users.

Securing applications: The application layer combines different applications and security challenges. Privacy protection matters faced at this layer will not be addressed

in the other layers where some security challenges do not occur. Here, the private information of users can be analyzed by attackers, leading to private data leakage and privacy loss. Since, this data might contain past and present locations that the users visited, some data protection techniques regarding data protection at this layer include location camouflage, anonymous space or space encryption. In addition, many applications in this layer apply to user's social life, therefore, need to be protected.

Securing data storage: Protecting stored secret data in CPS devices is important. Most CPS devices such as sensors are tiny, wirelessly connected and resource-constrained nodes (Raza, 2013). Although, various software based solutions use cryptographic techniques to encrypt data in such devices, they are not sufficient due to the constraints of memory and weak processing capabilities of these devices. As a result, lightweight security mechanisms are required (Lu *et al*., 2013).

Securing actuation: Actuation security means that any actuation actions must be issued from authorized sources. This will ensure that the provided feedback and control commands are correct and protected against adversaries (Fahey and Wells, 2016). As a result of using the internet as a transmission layer in CPS connections, internet security issues will also be involved. In general, security should be implemented for the entire system as one end-to-end security scheme rather than for only the operating security mechanism at each layer. Moreover, heavyweight computations and large memory requirements are currently the primary requirement of any desired security solution (Stankovic, 2014).

Control systems and cyber-attacks: An example of a production control system in a manufacturing industry is shown in the risk of exposure to cyber-attacks has increased in production control systems in recent years because of connections to the outside world via. USB memory and maintenance networks, connections between information systems and the internet, deployments of open communication protocols (e.g., TCP/IP) and deployments of open source operating systems and tools. The Stuxnet computer virus which was confirmed in July 2010 is a concrete example of a cyber-attack on a production control system. This virus exploited a weakness in Microsoft's Windows OS and targeted the control system software of the German company Siemens. It spread via. external storage media and networks and had the distinguishing feature of spreading infection when a user browsed a file, especially, from USB memory (Falliere *et al*., 2011). There were also, reports that Stuxnet targeted the control systems of Iran's atomic power plants (Kobayashi *et al*., 2012). If an attack affects organizations and industries that are responsible for important social infrastructure, the damage will be extensive. In addition, if an attack compromises or disables the production control system at a manufacturing firm, it is likely that large business losses will ensue. As a result, manufacturing sites which up to this time have been regarded as a sector that is impervious to cyber attacks, require security measures. The following measures should be considered as production control system security measures (Stouffer *et al*., 2011).

(1) Software measures (i.e., application of security patches to general purpose OSs and antivirus software). (2) Minimal platform services (i.e., minimal number of applications, minimal number of databases and minimal number of protocols). (3) Multi-layered defenses (i.e., firewalls, intrusion defense systems, defenses based on zoning and physical access management). Applications of security patches (1) are basic and effective measures that are carried out routinely by information technology divisions for general-purpose operating systems such as Microsoft Windows and Linux because of new vulnerabilities that are reported nearly every month. For production control systems, on the other hand, the amount of time that is available for applying patches is limited and the possibility of side effects is a concern. There are problems that must be overcome for (1) regarding the timing of the patching process and the implementation of testing for confirming that there are no side effects. Regarding the measures for (2) and (3) when it is impossible to routinely carry out the measures for (1), consideration is given to substitute measures in order to minimize the potential for damage (Takano, 2007). However, these alternatives also are less than perfect. Therefore, it is vital to reliably carry out the measures for (1) which are the same as for ordinary information systems, in order to be able to cope with attacks from diverse routes. The proposal in the present study focuses on the current situation and on methods for eliminating software vulnerabilities which is the most basic measure while comprehending the efficacy of the measures for (2) and (3).

RESULTS AND DISCUSSION

Future research directions: To protect the CPS network from joining malicious nodes at the perception layer (physical attack), a robust authentication process is required. PUFs can be used to confirm the unique identity of CPS devices which ensures the integrity and authenticity of connected devices and can also be used for creating unique cryptographic keys. However, the main limitation of this approach is that many hardware devices are not provided with PUF implementation ability such as

RAM. In addition, not all devices can implement PUF technology. Thus, this technique cannot be widely adopted. A more efficient approach for dealing with security in CPS is by using a multi-layered approach where the security of the system is considered at the beginning of the design for each layer. There must also be a correlation between the security that will be implemented with cost and time. Furthermore, the three-layer architecture of CPS is suitable for realizing the technical issues at the beginning stages of security analysis. Another issue should be considered as one of the challenges for CPS is the heterogeneous data that collected from different devices, each of which uses different protocols leading to compatibility issues related to data format and communication protocols. The main challenge in CPS is designing protocols that can work on different devices and situations. Thus, there is a need for a unified encoding standard for information exchange protocols for each device such as RFID and WSN which have different information access formats, security control mechanisms and storage formats, all of which lead to different data processing approaches. The literature has shown this area of risk is left untouched by other assessments while the number and complexity of attacks on manufacturers continues to increase. Threat identification for cyber physical security in advanced manufacturing is a future research area. The proposed approach only identifies and assesses cyber-physical vulnerabilities. A natural extension is to determine the likelihood of each threat from previous data collected from

customer discovery and through the analysis of threats seen commonly in industry. Risk analysis is another capability which could be developed from the vulnerability assessment tool.

CONCLUSION

Since, it is a comparatively new area, limited work has been accomplished in the security field of CPS. Performing assessment, authentication and access control processes should take place without disrupting the runtime environment. This way helps to identify mitigating options after inferring risk assessment. Enhancing CPS security using security mechanisms such as encryption algorithms, authentication protocols and steganography will not address all security risks that might be faced. Such solutions might help to protect the targeted systems to some point. However, any solution should consider the application situation and context as part of assessing security risks. Thus, enhancing the application security will improve the security of the whole system. A security mechanism should be designed for the entire system rather than in a single layer. This assessment is a step in the right direction for manufacturers to begin to take cyber-physical security seriously. The proposed approach only identifies and assesses cyber-physical vulnerabilities. A natural extension is to determine the likelihood of each threat from previous data collected from customer discovery and through the analysis of threats seen commonly in industry. Contributing to the cyber-physical market requires a more robust approach that includes working with industry partners, gaining insights into the limitations of manufacturing enterprises and developing an organization-specific assessment approach that caters to the needs of the various manufacturing enterprises. The future work aims to bridge the gap between assessment tools and cyber-physical security for manufacturing by creating a cyber-physical vulnerability assessment tool.

REFERENCES

Al-Smoul, K.M., T.A. Al-Rawashdeh and A.A. Al-Dahoud, 2016. An Improved Solar Low Energy Adaptive Clustering Hierarchy (IS-LEACH) technique. Intl. J. Commun. Networks Inf. Secur., 8: 221-226.

Albright, D., P. Brannan and C. Walrond, 2010. Did stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?. MSc Thesis, Institute for Science and International Security, Washington, DC. USA.

Anonymous, 2015a. ICS-CERT monitor newsletters: November-December 2015. ICS-CERT, Department of Homeland Security, Washington, DC. USA.

Anonymous, 2015b. Security in the internet of things: Lessons from the past for the connected future. Wind River Systems, Inc., Alameda, California, USA. https://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

Cardenas, A.A., S. Amin, Z.S. Lin, Y.L. Huang and C.Y. Huang *et al*., 2011. Attacks against process control systems: Risk assessment, detection and response. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, March 22-24, 2011, ACM, Hong Kong, China, pp: 355-366.

Fahey, M. and N. Wells, 2016. Yahoo data breach is among the biggest in history. CNBC Inc., USA.

Falliere, N., L.O. Murchu and E. Chien, 2011. W32. stuxnet dossier. Symantec Software company, Mountain View, California, USA. https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Gamundani, A.M., 2015. An impact review on internet of things attacks. Proceedings of the 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), May 17-20, 2015, IEEE, Windhoek, Namibia, pp: 114-118.

Khan, R., S.U. Khan, R. Zaheer and S. Khan, 2012. Future internet: The internet of things architecture, possible applications and key challenges. Proceedings of the 2012 10th International Conference on Frontiers of Information Technology, December 17-19, 2012, IEEE, Islamabad, India, pp: 257-260.

Kirkpatrick, M., E. Bertino and F.T. Sheldon, 2009. Restricted authentication and encryption for cyber-physical systems. Proceedings of the DHS CPS Workshop on Restricted Authentication and Encryption for Cyber-Physical Systems, January 1, 2009, Oak Ridge National Laboratory, Oak Ridge, Tennessee, pp: 1-5.

Kobayashi, H., I. Kaine and S. Taniguchi, 2012. Threats and countermeasures against cyberattack. J. Inst. Electr. Eng. Jpn., 132: 344-348.

Konstantinou, C., M. Maniatakos, F. Saqib, S. Hu and J. Plusquellic *et al*., 2015. Cyber-physical systems: A security perspective. Proceedings of the 2015 20th IEEE European Conference on Test Symposium (ETS), May 25-29, 2015, IEEE, Cluj-Napoca, Romania, pp: 1-8.

La, H.J. and S.D. Kim, 2010. A service-based approach to designing cyber physical systems. Proceedings of the 2010 IEEE/ACIS 9th International Conference on Computer and Information Science, August 18-20, 2010, IEEE, Yamagata, Japan, pp: 895-900.

Lu, T., B. Xu, X. Guo, L. Zhao and F. Xie, 2013. A new multilevel framework for cyber-physical system security. Proceedings of the 1st International Workshop on the Swarm at the Edge of the Cloud (SEC'13@ESWeek), September 29, 2013, TerraSwarm, Montreal, Canada, pp: 1-2.

Lu, T., J. Lin, L. Zhao, Y. Li and Y. Peng, 2014. An analysis of cyber physical system security theories. Proceedings of the 2014 7th International Conference on Security Technology, December 20-23, 2014, IEEE, Haikou, China, pp: 19-21.

Lu, T., J. Lin, L. Zhao, Y. Li and Y. Peng, 2015. A security architecture in cyber-physical systems: Security theories, analysis, simulation and application fields. Intl. J. Secur. Appl., 9: 1-16.

Mahmoud, R., T. Yousuf, F. Aloul and I. Zualkernan, 2015. Internet of Things (IoT) security: Current status, challenges and prospective measures. Proceedings of the 2015 10th International Conference on Internet Technology and Secured Transactions (ICITST), December 14-16, 2015, IEEE, London, England, UK., pp: 336-341.

Nourian, A. and S. Madnick, 2015. A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet. IEEE. Trans. Dependable Secure Comput., 15: 2-13.

Raza, S., 2013. Lightweight security solutions for the internet of things. Ph.D Thesis, Malardalen University College, Vasteras, Sweden.

Rost, J. and R.L. Glass, 2011. The Dark Side of Software Engineering: Evil on Computing Projects. Wiley, Hoboken, New Jersey, USA., ISBN:978-0-470-92287-3, Pages: 316.

Stankovic, J.A., 2014. Research directions for the internet of things. IEEE. Internet Things J., 1: 3-9.

Stouffer, K., J. Falco and K. Scarfone, 2011. Guide to Industrial Control Systems (ICS) security. MBA Thesis, US Department of Commerce, National Institute of Standards and Technology, Gaithersburg, Maryland, USA.

Takano, M., 2007. Sustainable cyber security for tility facilities control system based on defense-in-depth concept. Proceedings of the SICE Annual Conference, September 17-20, 2007, IEEE, Takamatsu, Japan, pp: 2910-2913.

Tuptuk, N. and S. Hailes, 2016. The cyber attack on Ukraine's power grid is a warning of what's to come. The Conversation, Melbourne, Australia.

Wang, E.K., Y. Ye, X. Xu, S.M. Yiu and L.C.K. Hui *et al*., 2010. Security issues and challenges for cyber physical system. Proceedings of the 2010 IEEE/ACM International Conference on Green Computing and Communications & Cyber, Physical Social Computing, December 18-20, 2010, IEEE, Hangzhou, China, pp: 733-738.

Weiss, J., 2010. Control system cyber vulnerabilities and potential mitigation of risk for utilities. Juniper Networks, Inc., Sunnyvale, California, USA.

Wood, A.D. and J.A. Stankovic, 2008. Security of Distributed, Ubiquitous and Embedded Computing Platforms. In: Wiley Handbook of Science and Technology for Homeland Security, Voeller, J.G. (Ed.). John Wiley & Sons, Hoboken, New Jersey, USA., ISBN:9780471761303, pp: 1090-1101.

Wu, M., T.J. Lu, F.Y. Ling, J., Sun and H.Y. Du, 2010. Research on the architecture of internet of things. Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) Vol. 5, August 20-22, 2010, IEEE, Chengdu, China, pp: 484-487.

Zhang, B., X.X. Ma and Z.G. Qin, 2011. Security architecture on the trusting internet of things. J. Electron. Sci. Technol., 9: 364-367.

Zhao, K. and L. Ge, 2013. A survey on the internet of things security. Proceedings of the 2013 9th International Conference on Computational Intelligence and Security, December 14-15, 2013, IEEE, Leshan, China, pp: 663-667.