Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 114 (2017) 367–374

Procedia Computer Science

www.elsevier.com/locate/procedia

Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems, CAS October 30 – November 1, 2017, Chicago, Illinois, USA

Taxonomy of Cross-Domain Attacks on CyberManufacturing System

Mingtao Wu, Young B. Moon*

Syracuse University, 263 Link Hall, Department of Mechanical and Aerospace Engineering, Syracuse University, Syracuse NY 13244, USA

Abstract

CyberManufacturing system (CMS) is a concept for next generation manufacturing system where manufacturing components are seamlessly integrated through technologies such as the internet of things, cloud computing, sensors network, machine learning, and new manufacturing processes. A key to realizing the CMS is its ability to handle cyber-attacks. For example, infill malicious defects can be created by cyber-attacks in additive manufacturing processes, resulting in changes in yield load and strain at failure as well as natural frequency. Cyber-attacks on CMS are not just limited to attacks on its computing sphere. Cross-domain attacks over both the physical and the computing spheres become critical. A taxonomy has been developed to specify the nature of the attacks, particularly when they are cross-domain. The taxonomy can help security professionals identify and detect cross-domain attacks in CMS. The taxonomy has been constructed in four dimensions: attack vector, attack impact, attack target, and attack consequence. To illustrate how the taxonomy can be utilized in detecting cross-domain attacks on CMS, infill malicious attacks on 3D printing processes are used as an example.

Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.

Keywords: Taxonomy; CyberManufacturing System; cross-domain attacks.

* Corresponding author. Tel.: +1-315-443-4366.
E-mail address: ybmoon@syr.edu

1877-0509
Peer-review under responsibility of the scientific committee of the Complex Adaptive Systems Conference with Theme: Engineering Cyber Physical Systems.
10.1016/j.procs.2017.09.050

1. Introduction

CyberManufacturing System (CMS), a blueprint for next-generation manufacturing systems, attempts to integrate computational processes and physical components at an unprecedentedly higher and tighter level. By implementing the latest technologies such as Industrial Internet of Things (IIoT), Artificial intelligence (AI), Cloud Computing, Fog Computing, Cyber-Physical System, Service-Oriented Technologies, Modeling and Simulation, Embedded Systems, Sensor Networks, Wireless Communications, and Advanced Manufacturing Processes, the CMS possesses unique characteristics such as self-awareness, self-prediction, self-optimization, and self-configuration abilities[1]. Related concepts such as "Industrie 4.0" by Germany, "Monozukuri" by Japan, "Factories of the Future" by EU, and "Industrial Internet" by GE, confirm the universal recognition of the importance of the CMS vision.

However, the openness to the Internet creates vulnerability and enlarges the attack surface where attackers can intrude into or extract data from the manufacturing system. Cyber-attacks on Stuxnet caused over 1000 centrifuges being maliciously sped up or slowed down and finally destroyed. Similar attacks took place on critical infrastructures and manufacturers such as steel mill in Germany[2], Davis-Besse power plant in Oak Harbor, Ohio, USA[3], and water filtering plant in Pennsylvania, USA[4]. Common attacking methods such as denial-of-service (DoS) attack, phishing, drive-by downloads, and SQL injection are all considered plausible ways of attacking manufacturing systems[5]. Cross-domain attacks (especially cyber-physical attacks[6]) are new types of attacks, but not well-understood[7]. A well-conceived taxonomy can be useful in understanding such cross-domain attacks.

Historical attacks on systems similar to CMS are analyzed in Section 2. Other taxonomies on cyber attacks are reviewed in Section 3. In Section 4, a taxonomy with four dimensions on cross-domain attacks in CMS environment is proposed. Applications of the taxonomy using five examples are provided in Section 5. Finally, conclusion and future work are presented in Section 6.

2. Cross-domain attacks on CMS and similar systems

A cyber-attack can compromise vulnerabilities in victims' confidentiality, integrity, and availability. In this section, real-life examples of cyber-attacks on manufacturing systems or critical infrastructures are examined. Potential vulnerabilities, attack vectors, and consequences are identified from the analysis. A virtual attack on a CMS is developed to simulate a pathway to execute cyber-physical attack on the system.

2.1. Examples on Manufacturing systems

According to the Repository of Industrial Security Incidents (RISI) Database, attackers aimed at a furnace in a steel mill and caused damage to the physical systems in Germany in 2014[8]. Similarly, in Japan in 2008, a major car manufacturer was infected with a computer virus. A system controlling production line operations was infected when additional computers were connected to a control system network. Approximately 50 computers were infected. Handling capacity was reduced, but fortunately there was no production shut-down[8]. In these cross domain attack cases, the attackers intruded the systems by social engineering or virus; then caused damage to machines and production lines.

2.2. Examples on Critical infrastructures

The critical infrastructures share similarities with modern manufacturing systems since the networks, control systems, and actuators have similar vulnerabilities that cross-domain attacks aim for. In Iran in 2010, secret Iranian centrifuges were targeted by Stuxnet[9], a malicious computer worm. Stuxnet specifically targeted programmable logic controllers (PLCs), collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart. On the infected machines, the centrifuges were maliciously sped up or slowed down, and finally destroyed. In the United States in 2003, the computers of the Davis-Besse nuclear power plant in Oak Harbor, Ohio, were infected with the Slammer worm, shutting down safety display systems[3]. The Slammer worm disabled a safety monitoring system for nearly five hours, despite a trust by plant personnel that the network was protected by a

firewall[10]. However, the breach did not pose a safety hazard because the Davis-Besse nuclear power plant had been offline since 2002.

2.3. A CyberManufacturing System Scenario

CyberManufacturing system has not been fully realized yet. Therefore, a virtual attack based on a CMS architecture illustrates how attackers can embed a malicious void in 3D printing parts that is proven by Sturm[11] to be vulnerable.

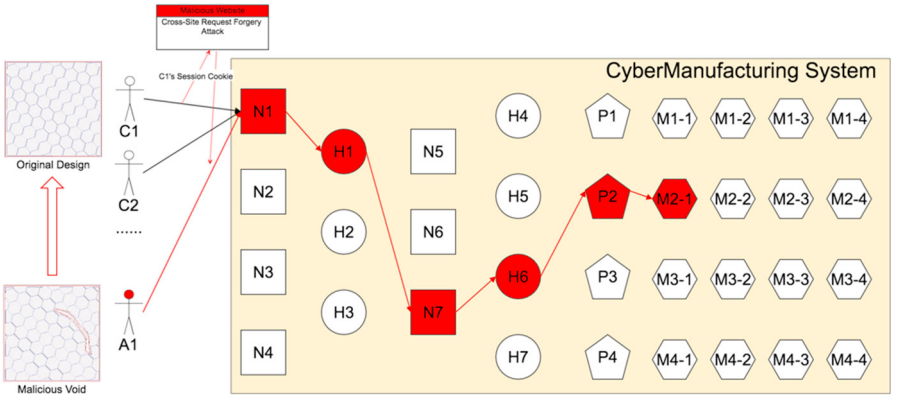

Fig.1. CSRF attack process in CMS with malicious void

In Fig.1, C*i* refers to customers. A*i* refers to attackers. N*i* refers to network nodes in different layers in CMS. H*i* refers to host nodes in different layers in CMS. P*i* refers to production systems, and M*i-j* refers to the machines in a production system P*i*.

The customer C*1* finds a company called CMS3D with its website "www.cms3d.com" for placing orders. The customer wants to make and purchase a self-designed 3D printable brake assembly. C*1* uploads all the ".stl" file needed for 3D printing process to the CMS3D data server with additional requests such as quantity, color, deadline, etc.

The attacker A*1* builds a malicious website called "CMS Coupon" that tricks CMS customers into browsing the malicious page when logged into the "CMS3D" website. A*1* starts a Cross-Site Request Forgery (CSRF) attack, also known as session riding. This attack lets A*1* gain access to the customer account and injects HTTP requests to the download, edits with malicious void attack and replaces the customer's original ".stl" file.

The malicious ".stl" file passes through a design center, a global business center, and is assigned to a production system P*2*. The part with malicious void cannot be detected by operators and inspectors due to the enclosed surface of 3D printing parts. Without monitoring the part with vision detection methods[6,12,13], this defective part is delivered to C*1*.

The above five real-life examples and one virtual example from CMS illustrates how the intrusion occurs in a cyber domain, but affects the victims in the physical domain. These physical victims normally experience costly consequences. However, those cross-domain attacks are not well understood enough compared to traditional IT cyber security problems.

3. Taxonomies on Cyber-Attacks

For general cyber-attacks, Howard and Longstaff[14] established a taxonomy for classifying and understanding computer security incident information. It was constructed in seven dimensions: attackers, tool, vulnerability, action, target, unauthorized result and objectives. The work presented a common language for computer security incidents. However, this taxonomy cannot describe the security incident information in CMS. For example, under the dimension of target, it does not cover any physical objects from manufacturing processes.

Hansman and Hunt[15] proposed a taxonomy of network and computer attacks with four dimensions: attack vector, target, vulnerabilities, and further effects. The first dimension, attack vector is the main mechanism that the attack uses

in reaching the victim. Most of the attack types are covered in the first dimension such as buffer overflow, virus, and worms. However, new attack vectors found after 2005 such as shell-shock attack are not covered in this taxonomy. Also, in the second dimension, the hardware target includes computers only. Thus this taxonomy has limited relevance on CMS attacks.

Simmons[16] developed a cyber-attack taxonomy named AVOIDIT with five dimensions: attack vector, operational impact, defense, information impact, and target. The first dimension, attack vector explains the exploited vulnerability including design flaws, kernel flaws, buffer overflow, race condition, etc. The second dimension, operational impact explains the ability for an attacker to culminate. It also provided high-level information for non-expert to better understand cyber-attacks. The second dimension provides a good angle for people less familiar with cyber-attacks which can help clarify the attack methods in CMS. However, the AVOIDIT cannot fully describe and classify the cross-domain attacks in CMS especially in physical attack vectors, impact and target. Also, the attack consequence is uncovered in AVOIDIT taxonomy.

Yampolskiy[17] proposed a taxonomy for describing attacks in cyber-physical system (CPS). The proposed taxonomy is capable of representing both conventional cyber-attacks and cross-domain attacks. The taxonomy dimension including influenced element, influence, victim element, impact on victim, attack means and preconditions. Furthermore, based on the proposed taxonomy, they defined four attack categories: Cyber-to-Cyber (C2C), Cyber-to-Physical (C2P), Physical-to-Physical (P2P), and Physical-to-Cyber (P2C). The dimension of cyber and physical enhances the clarification and understanding of the attacks in CPS. However, details are lacking in the taxonomy to be useful in CMS. Moreover, the dimension of attack vector still need to be constructed.

4. Taxonomy on CMS Cross-Domain Attacks

The purposes of developing this taxonomy are as follows. First, it helps developing a common language for cross-domain attacks in manufacturing discipline. Second, it helps understanding the new attacks and attack types in CMS environment. Third, it helps defining what data should be recorded and analyzed for intrusion detection. Fourth, the countermeasures and preventions can be developed using the taxonomy. Lastly, it will be useful for domain experts from both cyber security and manufacturing disciplines in understanding the cross-domain attacks in CMS.

The uniqueness of this taxonomy is: 1) it consists of four dimensions: attack vector, attack impact, attack target and attack consequence, 2) each dimension then divided into “cyber” and “physical” sub-dimensions adding necessary details for CMS applications.

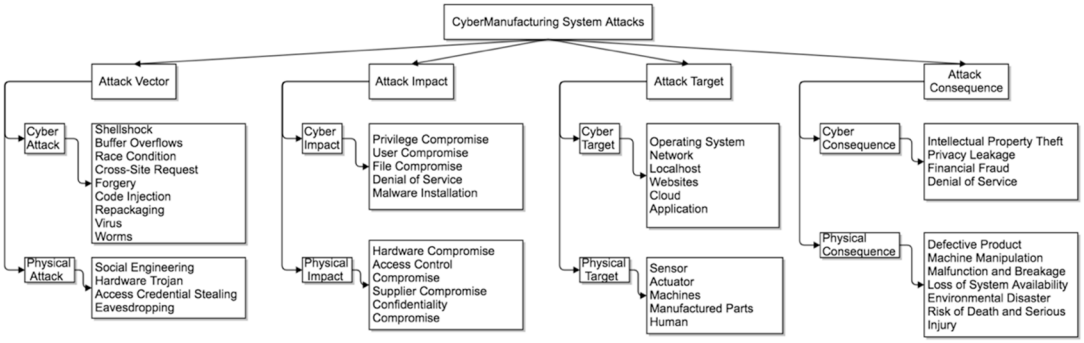

Fig.2. Taxonomy attack of CyberManufacturing System

4.1. First dimension: attack vector

Attack vector, or attack method, is the path an attack gets access to the victim. It is a crucial dimension because it provides essential information for describing an attack [15].

(a) Cyber-attack vector

Cyber-attack vector in CMS mainly comes from a network and computer attacks in a digital format. The taxonomy includes shellshock, buffer overflow, race condition, cross-site request forgery, code injection, repackaging, virus, and worms.

• **Shellshock:** It is a security bug in Unix Bash shell, first discovered on 24 September 2014. This vulnerability can exploit various systems and be launched either remotely or from a local machine. The Internet-facing services in CMS, such as service facing customers, can use Bash to process certain requests. This can allow an attacker gain the root/super or user/administrator access and run malicious commands that result in unauthorized access to a computer system.

• **Buffer Overflow:** This refers to a condition when a program tries to write data beyond the limit of pre-allocated fixed length buffers. It happens when a piece of code or data do not check for appropriate length of input and the value is not the size the program expects[16]. This vulnerability can be exploited by a malicious user who gained the root/super or user/administrator access and execute arbitrary commands.

• **Race Condition:** A race condition occurs when multiple processes access and manipulate the same data concurrently. It allows an attacker to gain the root/super or user/administrator privileges while a program or process is in those privilege modes.

• **Cross-Site Request Forgery (CSRF):** Also known as *session riding*, this is a type of attack on website where unauthorized commands are transmitted from a user that the website trusts. It can happen on web applications facing customers in CMS. A CSRF attack involves a victim user (customer), a trusted site (CMS web), and a malicious site (attack site). When the customer holds an active session with a CMS web application while visiting a malicious site, the malicious site can inject an HTTP requests to the CMS web application user session, causing change in account information.

• **Code Injection:** Code injection is caused by attackers' inputing code into a vulnerable computer program and change the process of execution. The places in CMS for code injection may include SQL (Structured Query Language), OS commands, etc. For example, most small and industrial strength database applications can be accessed using SQL statements for structural modification and content manipulation[18]. Malicious users can use SQL injection and manipulate other customer's information.

• **Repackaging:** This is a type of attacks on Android OS applications. Attackers download popular applications from a store, unpack and modify the application with malicious requests of privileges, then post the application in certain third-party app stores. In CMS, the designs with CAD models can be offered online. Similar to repackaging an application, attackers can repackage a design by reverse engineering or just modifying the CAD file; then uploading back to online platforms. Such attacks can cause defective parts, products, or even machine malfunctions.

• **Virus:** This self-replicating program can spread through some types of infected file[15].

• **Worms:** This self-replicating program can propagate without using infected files. Worms usually propagate through network services on computers or through emails.

(b) Physical attack vector

Physical-attack vector in CMS can come from a person, hardware or a sensor in a physical format. The taxonomy includes social engineering, hardware Trojan, access credential stealing, and eavesdropping for physical attack vector.

• **Social Engineering:** This attack is a process of using social interactions to acquire information about a victim or computer system. It includes human interaction activities and often involves tricking person into breaking security procedures. For example, A CMS employee may be asked to open a malicious flash drive and infect the host inside the CMS environment.

• **Hardware Trojan:** A Hardware Trojan embeds backdoor program and modification in an integrated circuit. It tries to by-pass or disable the security fence of a system. It can release private data by radio outflow. Hardware Trojans can also disable, derange or destroy the entire or segments of a chip[19].

• **Access Credential Stealing:** Some credential infromation can be stolen.

• **Eavesdropping:** Eavesdrops on communication, physical signals such as acoustic emission from 3D printing[20], or keystroke can lead to IP stealing or even credential loss.

4.2. Second dimension: Attack Impact

The second dimension, attack impact explains the degree of consequences via intrusion. The purpose of this dimension is to clarify the direct consequence of attack incident. It also provides information for understanding the impact of the attacks. For example, an attacker uses buffer overflow attack vector to gain the root/super or user/administrator. This impacts the CMS environment with root compromises.

(a) Cyber Impact

The cyber impact shows the impact on digital platforms, such as web application, program, operating system, digital file, etc. The taxonomy includes privilege compromise, user compromise, file compromise, denial of service, and malware installation.

- **Privilege Compromise:** By using attack vectors such as buffer overflow, shellshock, race condition, the attacker can gain higher privileges such as superuser.
- **User Compromise:** An attacker gains unauthorized use of other user account or privileges on a host, web application, or database. An attack such as CSRF can achieve this goal on web applications.
- **File Compromise:** In CMS, CAD/CAM files play a major role. Attacker makes malicious change by using repackaging, code injection, thus can change the critical structure and physical characteristic of the design.
- **Denial of Service (DoS):** An attacker can conduct a denial-of-service attack (DoS attack) that makes a connected machine such as a database or computation resource inaccessible to its intended clients.
- **Malware Installation:** An attack can be launched via user-installed malware, whether user installation or drive-by installation. Installed malware can allow an adversary to gain full control of the compromised systems, potentially leading to the exposure of sensitive information or remote control of the host.

(b) Physical Impact

- **Hardware Compromise:** Social engineering attacks can cause hardware malfunctioning such as hard drive, DVD drive, or computers.
- **Access Control Compromise:** The access credential stealing or social engineering can lead to the compromise of the physical access control in CMS environment.
- **Supplier Compromise:** Hardware Trojan from a supplier compromises the integrity of the source.
- **Confidentiality Compromise:** Eavesdropping in CMS environment working area, communication or even physical provider layer can cause confidentiality compromises.

4.3. Third dimension: Attack Target

(a) Cyber Target

- **Operating System:** OS exists in CMS environment from customer layer to physical provider layer. An attack can be formulated to target vulnerabilities within a particular operating system. The operating system in manufacturing system with legacy equipment normally lacks in updated security measures, thus is highly vulnerable to attacks.
- **Network:** A network itself or its protocols can be attackers' targets too. For example, a ping flood attacks a network rather than hardware or software[15].
- **Localhost:** An attacker can aim the target on the host computers from CMS environment or customers.
- **Website:** It is the interface for customers to communicate with CMS environment.
- **Cloud:** A cloud service in CMS is any resource that is available over the Internet. The cloud service resources can be Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).
- **Application:** The applications can be targeted, including the job allocation functions, the machine learning and data analytics functions, or real-time simulation functions in CMS.

(b) Physical Target

- **Sensor:** It allows the manufacturing system under monitoring and can provide data for perdition and simulation.
- **Actuator:** An actuator is a fundamental component of a machine that moves or controls a mechanism or system.

• **Machines:** Machine is the key component of physical provider layer in CMS. It can also be an assembly of actuators, sensors and control unit such as programmable logic controller (PLC).
• **Manufactured Parts:** Manufactured parts or assemblies are the finished products from a production line.
• **Human:** Human can be a target victim in CMS as well. Operators, assembly workers working next to robots are endangered when hackers can send malicious control to actuators.

4.4. Fourth dimension: Attack Consequence

(a) Cyber Consequence

• **Intellectual Property Theft / Piracy:** Intellectual property theft in manufacturing cost billions of dollars and loss of jobs. The counterfeit products and stolen designs can damage customers' and manufacturers' interests or credentials.
• **Privacy Leakage:** The leakage of private information from customers in CMS database can be one of the critical consequences.
• **Financial Fraud:** The leakage of customer's financial information such as credit card information during purchase, billing address, can lead to financial frauds.
• **Denial of Service (DoS):** Denial of service can be both the impacts and the consequences. An example is the DoS of a server (impact) causing the DoS of the customer online billing system (consequence).

(b) Physical Consequence

• **Defective Product:** Defective products or even malicious products are physical consequences. The scrap cost, recall will be drawn with defective products or part being manufactured. Following consequences such as damage to company image or risk of human lives.
• **Machine Manipulation:** Attacks can cause problems on machines such power over consumption, unpredicted breakage, compromised precision, slow-down, etc.
• **Malfunction and Breakage:** The breakage or malfunction can be a consequence of machine manipulation.
• **Loss of System Availability:** The critical availability of physical components such as 3D printers, CNC machines, logistics can be compromised.
• **Environmental Disaster:** Environmental disasters such as leakage and explosion are critical physical consequences.
• **Risk of Death and Serious Injury:** Human as most fragile component of CMS is at risk of their health and life when working in environment with hazardous chemical, radiation and robots.

5. Attack analysis

Five attack examples provided in Section 2 are considered using the proposed taxonomy.

Table 1. Analysis of attack examples with CMS cross-domain taxonomy.

Incident Name	Attack Vector	Attack Impact	Attack Target	Attack Consequence
1, CMS malicious void attack, 2017	Cyber: Cross-Site Request Forgery	Cyber: User Compromise	Physical: Manufactured Parts	Physical: Defective Parts; Risk of Injury
2, German Mill, 2008	Physical: Social Engineering	Cyber: Privilege Compromise	Physical: Machine	Physical: Machine Breakage
3, Japanese Automobile Manufacturer, 2008	Cyber: Virus	Cyber: Denial of Service	Cyber: Localhost	Physical: Loss of System Availability
4, Iranian Nuclear Centrifuges, 2010	Cyber: Worm	Cyber: Malware Installation	Physical: Actuator	Physical: Machine Breakage
5, American nuclear power plant， 2003	Cyber: Worm	Cyber: Denial of Service	Physical: Machine	Physical: Loss of System Availability

Table 1 shows how four dimensions of the taxonomy are used in describing the attack examples. Most of the cross-domain attacks in CMS and similar environments starts with a cyber-attack vector or cyber impact; then result in the

victim system or component physical consequences. Exceptions exist such as in the German mill incident that began with a physical attack vector, and in the Japanese automobile manufacturer that had a cyber-attack target.

6. Conclusion and Future Work

The proposed taxonomy is a beginning of classifying the cross-domain attacks in CMS. This work provides a common language for cross-domain attacks in manufacturing discipline, and helps domain experts - from both cyber security and manufacturing fields - better understand the nature of attacks in CMS environment. Furthermore, the taxonomy can be used as a source for the security policy making, intrusion detection, prevention and countermeasure design in order to make a secured manufacturing system. It also provides a guideline on what kind of attacks should be expected, what types of components should be monitored in CMS, and what kind of consequence should be expected. A limitation of this work is regarding unknown new attack, which requires further investigation when it occurs. For future work, more dimensions can be added to the current taxonomy for more detailed classification. Also using the taxonomy in intrusion detection and prevention in realistic CMS will be pursued.

Reference

1. Song Z, Moon YB. Performance Analysis of CyberManufacturing Systems : A Simulation Study. In: *13th IFIP International Conference on Product Lifecycle Management*; 2016. p. 592-605.
2. Kim Zetter. A Cyberattack Has Caused Confirmed Physical Damage for the Second Time Ever. WIRED. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/; 2015.
3. C´ AA, ardenas. Challenges for Securing Cyber Physical Systems. In: *Work Futur Dir cyber-physical Syst Secur*; 2009.
4. Esposito R. Hackers Penetrate Water System Computers. ABC. http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra; 2006.
5. Mcmillen D. Manufacturing Security: Managing Machines in Motion processes. IBM. https://securityintelligence.com/manufacturing-security-managing-machines-in-motion/; 2016.
6. Wu M, Song Z, Moon YB. Detecting Cyber-Physical Attacks in CyberManufacturing Systems with Machine Learning Methods. *J Intell Manuf*; 2017, (in press).
7. Yampolskiy M, Andel TR, McDonald JT, Glisson WB, Yasinsac A. Towards Security of Additive Layer Manufacturing. In: arXiv preprint.
8. The Repository of Industrial Security Incidents. http://www.risidata.com/; 2017.
9. Langner R. Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*. 2011; **9(3)**: 49-51.
10. Poulsen K. Slammer worm crashed Ohio nuke plant network. Security Focus; 2003.
11. Sturm LD, Williams CB, Camelio JA, White J, Parker R. Cyber-Physical Vunerabilities In Additive Manufacturing Systems. In: *International Solid Freeform Fabrication Symposium Proceedings*; 2014. p.951-963.
12. Wu M, Phoha V V., Moon YB, Belman AK. Detecting Malicious Defects in 3D Printing Process Using Machine Learning and Image Classification. In: P*roceedings of the ASME 2016 International Mechanical Engineering Congress and Exposition*; 2016. p.1-6.
13. Wu M, Zhou H, Lin LL, et al. Detecting Attacks in CyberManufacturing Systems: Additive Manufacturing Example. In: *International Conference on Mechanical, Materials and Manufacturing*; 2016. p.1-5.
14. Howard JD, Longstaff TA. A common language for computer security incidents. *Sandia National Laboratories*; 1998.
15. Hansman S, Hunt R. A taxonomy of network and computer attacks. *Computers & Security* 2005; **24(1)**: 31-43.
16. Simmons C, Ellis C, Shiva S, Dasgupta D, Wu Q. AVOIDIT: A cyber attack taxonomy. In: *9th Annu Symp Inf Assur*. 2014. p.12-22.
17. Yampolskiy M, Horvath P, Koutsoukos XD, Xue Y, Sztipanovits J. Taxonomy for description of cross-domain attacks on CPS. In: *Proceedings of the 2nd ACM International Conference on High Confidence Networked Systems*; 2013. p.135–142.
18. Zhu B, Joseph A, Sastry S. A Taxonomy of Cyber Attacks on SCADA Systems. In: *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing. IEEE*; 2011. p. 380-388.
19. Beaumont M, Hopkins B, Newby T. Hardware Trojans - Prevention, Detection, Countermeasures (A Literature Review). In: *Command Control Communications and Intelligence Div*; 2011.
20. Song C, Lin F, Ba Z, Ren K, Zhou C, Xu W. My Smartphone Knows What You Print : Exploring Smartphone-based Side-channel Attacks Against 3D Printers. In: *ACM CCS*; 2016. p.895-907.