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.

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

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

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