Manufacturing Letters xxx (2017) xxx–xxx

Contents lists available at ScienceDirect

Manufacturing Letters

journal homepage: www.elsevier.com/locate/mfglet

Letters

DACDI (Define, Audit, Correlate, Disclose, and Improve) framework to address cyber-manufacturing attacks and intrusions

Mingtao Wu, Young Moon [*]

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

ARTICLE INFO

Article history:
Received 29 August 2017
Received in revised form 13 December 2017
Accepted 16 December 2017
Available online xxxx

Keywords:
Cyber-Manufacturing System
Intrusion detection system
Simulation
Cyber security

ABSTRACT

Cyber-Manufacturing Systems (CMS) is a vision for advanced manufacturing where physical components are fully integrated with computational processes via computer networks and the Internet. Despite of many benefits that CMS ushers in, realizing it is not possible without addressing emerging security issues in CMS. Among various attack incidents reported in manufacturing, the cyber-physical attacks are least understood – yet can lead to grave consequences. The need for understanding intrusion detection in CMS and developing an effective intrusion detection system is critical for the success deployment of CMS. Five-step cyber-physical intrusion detection framework has been developed.

1. Introduction

Cyber-Manufacturing Systems (CMS) is a vision of future manufacturing where physical components are fully integrated with computational processes via computer networks and the Internet. Although the CMS promises great benefits in cost, efficiency, and sustainability [1], realizing the CMS is not possible without addressing emerging issues accompanying with the higher level of connectivity [2]. Among various attack incidents reported in manufacturing, the cyber-physical attacks are least understood [3] – yet can lead to serious consequences. Those attacks intrude into manufacturing systems in digital format, carrying physical damage payload that can cause manufacturing equipment or products to develop over-wearing, breakages, scraps or any other unintended changes [4]. One example of cyber-physical attacks – Stuxnet worm [5] – illustrates that such attack can be active for months or years before even being detected.

Previous intrusion detection studies focused on individual manufacturing processes such as the additive manufacturing [6–8] or CNC machining [9], rather than considering manufacturing system as a whole. Critical components for intrusion detection such as network, host, quality control inspections are neglected in these works. Five-step intrusion detection framework – DACDI (*D*efine, *A*udit, *C*orrelate, *D*isclose, and *I*mprove) – is designed specifically for CMS. A model CMS is used to collect cyber as well as physical audit data, and to demonstrate the feasibility of operating the intrusion detection system. Data on power consumption, acoustics, images, and acceleration forces collected from the model CMS are used to validate the effectiveness of the intrusion detection system.

2. DACDI: an intrusion detection process in CMS

DACDI stands for Define, Audit, Correlate, Disclose, and Improve (Fig. 1). It is a framework to implement the cyber-physical intrusion detection system on different CMS environments. It is also a collection of systematic and statistical analyses for detecting intrusions, reducing their influences, and improving the level of security after detection. Professionals in manufacturing, cyber-security, and control system can adapt it as a guideline to address attacks and intrusions in a CMS environment.

2.1. Define

The first step is to define the overall scope of work – defining seven **A**s: *A*rchitecture, *A*ttack surface, *A*ttack vector, *A*ttack impact, *A*ttack target, *A*ttack consequence and *A*udit material. An architecture of application environments can be adopted to define the scope. Examples include the CMS hierarchical five-layer architecture [1], cloud manufacturing concept architecture [10], and reference architecture model Industrie 4.0 [11]. A taxonomy of cross-domain attacks on CMS can be used to define attack vector, attack impact, attack target, and attack consequence [12]. Along with well-defined scope and risks, selection of audit data is the result of this step.

[*] Corresponding author.
E-mail address: ybmoon@syr.edu (Y. Moon).

https://doi.org/10.1016/j.mfglet.2017.12.009
2213-8463/© 2017 Society of Manufacturing Engineers (SME). Published by Elsevier Ltd. All rights reserved.

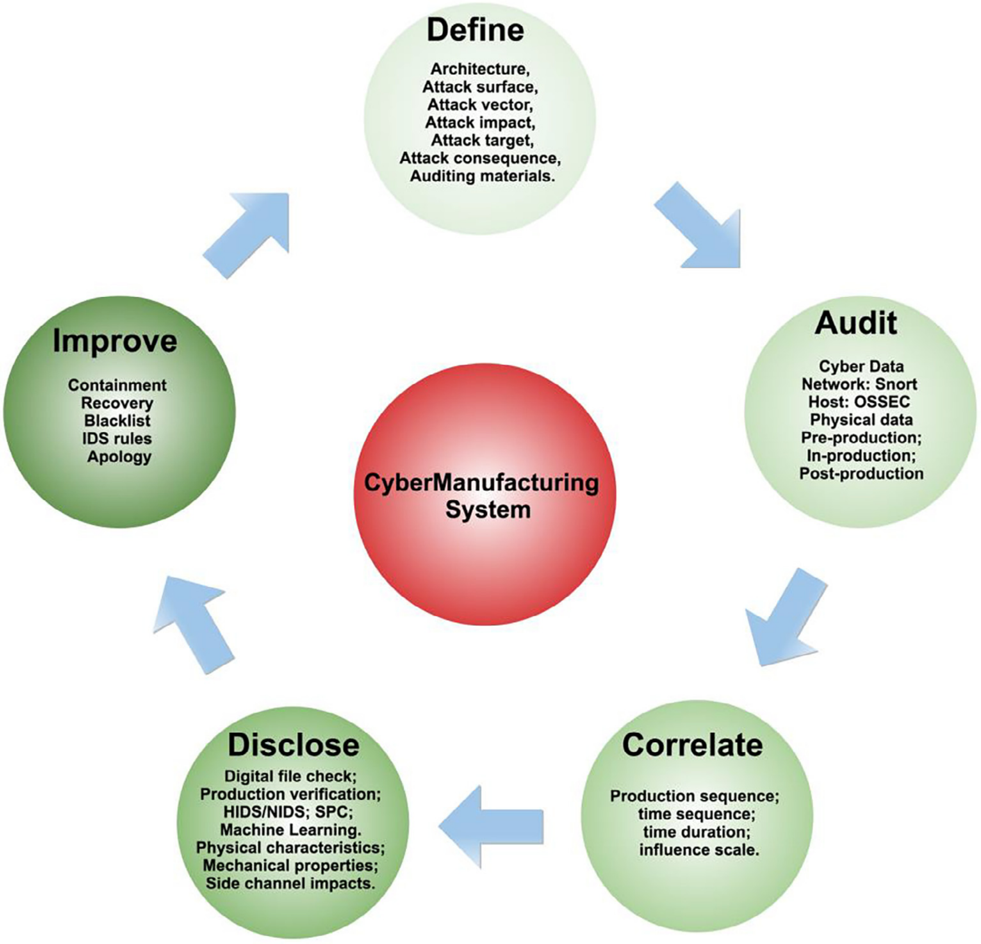

Fig. 1. DACDI intrusion detection approach.

2.2. Audit

Auditing data is the process of collecting data for intrusion detection in CMS. Two types of data are collected for the intrusion detection purpose: cyber data and physical data. Cyber data can be used for: (i) detecting amateuristic and known attacks, and (ii) correlating with physical anomaly occurrences. Network and host activities – login attempts, network connections, or log file changes – may be part of cyber data. Physical data can be used to detect cyber-physical intrusion more accurately [4]. The physical data may be obtained from sources such as product inspection processes, manufacturing processes, and system level operations.

2.3. Correlate

This phase correlates the cyber and physical data with four rules: time sequence, production sequence, attack scale, and time duration. It aims to reduce the false alarms and find the root cause of alerts.

2.4. Disclose

A collection of methods from cyber security, machine learning, and quality control are integrated to disclose and stop the intrusion as early as possible. This step is divided into three stages: (i) pre-production, (ii) in-production, and (iii) post-production. The first stage utilizes host and network monitoring, digital file check and production verification for disclosing intrusion. The second stage uses statistical process control (SPC) and machine learning for detecting malicious changes in manufacturing processes. The third stage applies inspection of (i) physical characteristics, (ii) mechanical properties, and (iii) side-channel impacts after manufacturing.

2.5. Improve

Once an intrusion is detected, the security policy should be improved to address similar attacks. Procedures for containment and recovery are applied to the vulnerable software and the damaged hardware. The blacklist and detection rule are added according to the attack incident to improve the security level.

3. Model CMS environment

To build a model CMS (Fig. 2) to validate the DACDI framework, the following guidelines are established:

- The environment adopts an architecture of manufacturing systems. In this work, the CMS hierarchical five-layer architecture is chosen [1].
- The environment should be able to collect cyber as well as physical data for the purpose of intrusion detection.
- Operational details such as job allocation, automation, and logistics are not considered.
- One physical local provider is included.