Available online at www.sciencedirect.com

ScienceDirect

Manufacturing Letters 2 (2014) 74–77

www.elsevier.com/locate/mfglet

Research Letters

Cyber-physical security challenges in manufacturing systems

Lee J. Wells [a], Jaime A. Camelio [a,*], Christopher B. Williams [b], Jules White [c]

[a] Grado Department of Industrial and Systems Engineering, Virginia Tech, United States
[b] Department of Mechanical Engineering, Virginia Tech, United States
[c] Electrical Engineering & Computer Science, Vanderbilt University, United States

Received 22 August 2013; received in revised form 29 January 2014; accepted 29 January 2014
Available online 12 February 2014

Abstract

As technology progresses, cyber-physical systems are becoming susceptible to a wider range of attacks. In manufacturing, these attacks pose a significant threat to ensuring products conform to their original design intent and to maintaining the safety of equipment, employees, and consumers. This letter discusses the importance of research and development of cyber-security tools specifically designed for manufacturing. A case study of a cyber-attack on a small-scale manufacturing system is presented to (i) illustrate the ease of implementing attacks, (ii) highlight their drastic effects and (iii) demonstrate the need for educating the current and future manufacturing workforce.

Keywords: Cyber security; Manufacturing; Quality control; Cyber attacks

1. Background and motivation

Cyber-attacks have drastically increased since their infancy in the early 1980's with operations such as the suspected 'Logic Bomb' that exploded the Trans-Siberian Pipeline [1]. As the number of attacks grows, their visibility decreases and maliciousness increases (Fig. 1). Over the past decades, this has been seen in aerospace [2], control systems [3], financial systems [4], and presidential campaign offices [5]. Attackers have repeatedly shown that no system is off-limits or out-of-reach. In addition, opportunities for attacks are increasing with the Internet of Things (IoT) [6], where the number of networked devices is rapidly expanding across every sector, including manufacturing.

While enhanced manufacturing system connectivity provides significant analytical and supply-chain management capabilities, it also opens the door for attacks against cyber-physical components. An attack can alter design files or process parameters (e.g. tool paths) to bring a part out of specification. In addition, this attack could also modify the quality control (QC) system to avoid proper quality assessment. Such attacks can disrupt the product/system design process and/or adversely affect a product's design intent, performance, or quality. The results of which could delay a product's launch, ruin equipment, increase warranty costs, or reduce customer trust. More importantly, these attacks pose a risk to human safety for operators and consumers.

2. Cyber-security weaknesses in manufacturing systems

The first step towards preventing, detecting, and mitigating the effects of cyber-attacks in manufacturing is to understand and overcome the current weaknesses in areas, such as design systems, production control, QC, and manufacturing cyber-security research and education. This section briefly describes these weaknesses. Here a weakness

* Corresponding author. Address: Virginia Tech, 250 Durham Hall, Blacksburg, VA 24061, Unites States. Tel.: +1 540 231 8976; fax: +1 540 231 1831.
E-mail address: jcamelio@vt.edu (J.A. Camelio).

http://dx.doi.org/10.1016/j.mfglet.2014.01.005
2213-8463/

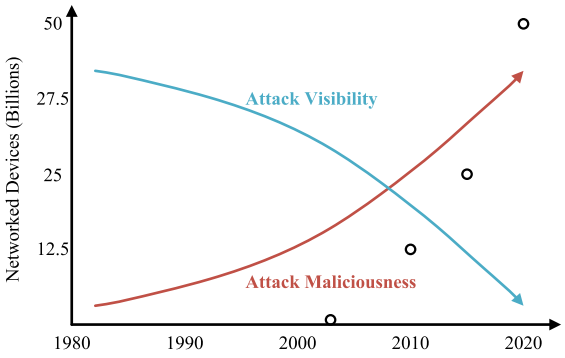

Fig. 1. Growth of Networked Devices [6] and Cyber-Attack Visibility and Maliciousness Trends, Adapted from [7,8].

refers to anything that impedes the development of cyber-security solutions.

2.1. Concerns of industry

One of the most important barriers for cyber-security in manufacturing is that industry is more concerned with attacks aimed at intellectual property (IP) theft. This is warranted as computer security has traditionally focused on protecting information [9]. As manufacturing systems have evolved into an IoT that rely on Softwares as a Service and cloud computing; attack opportunities now extend beyond IP theft. As industrial needs often drive research, it is vital that industry becomes aware of cyber-attack threats and the full extent of their consequences.

In addition, CAE software developers often maintain that their products are encrypted and 100% protected, which gives industry a false sense of security. Given enough time and computational resources, all encryptions can be broken. Moreover, a single poor cryptographic decision can put a system at risk, as recently seen with Android mobile devices. However, whether or not a system can be hacked is irrelevant considering that the majority of attacks on cyber-physical systems have come from insiders (e.g. disgruntled employees) [10–14].

2.2. Current research efforts

While cyber-security for manufacturing is not novel, current research efforts focus on high-level security issues, such as vulnerabilities in Supervisory Control and Data Acquisition Networks [15–18]. Here manufacturing is grouped with critical infrastructures [19] such as electrical power generation and distribution, water and waste management, and transportation systems. While manufacturing shares similarities with critical infrastructures, they have distinctly different requirements for cyber-security. Manufacturing systems are more than a collection of control systems; they are highly integrated with the product lifecycle. Hence, a manufacturing system can be attacked anywhere from initial design to final inspection, and anywhere in the supply chain. In order to develop efficient security measures for manufacturing requires a manufacturing specific research area within cyber-security.

2.3. Quality control

Since cyber-physical systems affect the physical world, they offer an additional avenue for detecting attacks beyond traditional cyber-security [9]. In manufacturing, QC is used to ensure a process' stability by measuring key product/process characteristics. However, current QC approaches are not designed to detect the effects of cyber-attacks. Specifically, QC approaches are based upon assumptions (sustained system shifts, rational sub-grouping, feature-based monitoring, etc.) that are no longer valid under the presence of an attack. In fact, these assumptions can be used against a QC system to create undetectable attacks. Additionally, QC systems can be compromised as they are often integrated into the digital manufacturing network.

Furthermore, the purpose of QC extends past detection and focuses on recovering from process disturbances. Current diagnostic procedures do not consider cyber-attacks as possible root-causes. Therefore, if the effect of an attack is detected; a significant amount of time, effort, and money would be wasted in unsuccessfully determining the cause. In this context, QC approaches need to be fundamentally re-evaluated to ensure protection.

2.4. Education

Modern engineering curriculums focus heavily on the development of CAE skills. However, outside of modeling errors (e.g. Finite Element Analysis), these tools are considered and taught as infallible. It is vital that future engineers and designers become exposed to the threats cyber-attacks pose on cyber-physical systems.

Curriculums focused on security for cyber-physical systems have been proposed and implemented [20–22]. However, they focus on control systems and do not consider manufacturing-specific issues, such as compromised CAE software. It is fundamental that manufacturing workforce development has a focus in increasing awareness of potential cyber-attacks, as education is the first step towards defending against attacks.

3. Case study

A case study was performed to demonstrate the feasibility of a cyber-attack on a simple manufacturing system and to understand the diagnostic capabilities of engineers who do not anticipate cyber-attacks. This section briefly describes the experiment and resulting observations.

3.1. Experiment

In this experiment sophomore-level engineering students, at a large land-grant university, were challenged to

design and manufacture a tensile test specimen. A tensile test specimen was chosen due to its ease of design, machining, and quantifiable performance loss from an attack. The students were asked to complete the following steps:

Step 1: Create a specific ASTM compliant tensile test specimen using Computer Aided Design (CAD) software.
Step 2: Generate tool paths for a 3-axis mill to machine the specimen using Computer Aided Manufacturing (CAM) software. Here specific machining parameters were given to the students (e.g. machining sequence, tool dimensions, cutting parameters).
Step 3: Transfer the generated tool paths (stored as an ASCII file) to a PC controlled mill (via a USB storage device).
Step 4: Machine the specimen.

Unbeknownst to the students, the PC used in Step 3 was infected with a virus designed to alter the tool path file (thus altering the fabricated specimen's dimensions), as illustrated in Fig. 2. Specifically, this virus waits for a file transfer event of a specific file extension. Once this event occurs, instead of transferring the desired file, the software transfers a different file with altered tool paths. These new tool paths result in a part with a cross-sectional area 19% less than the design, which equates to a 19% loss in performance (e.g. force required to yield). If this part were produced in an actual manufacturing system with a compromised QC system, the end-product would prematurely or catastrophically fail in-use.

3.2. Observations and results

This experiment was performed with seven groups of 3–4 students each. The first three groups did not measure the part and the effects of the attack went undetected. Based upon exit interviews, the consensus was that there was no need to measure the part since it "looked correct." For these students, the only possible errors would come from machining (tool-offsets, motor control inaccuracies, etc.) and were inherent to the system. While this is a simple result, it highlights the belief held by future engineers that CAE tools are infallible; a belief that is not challenged in current curricula.

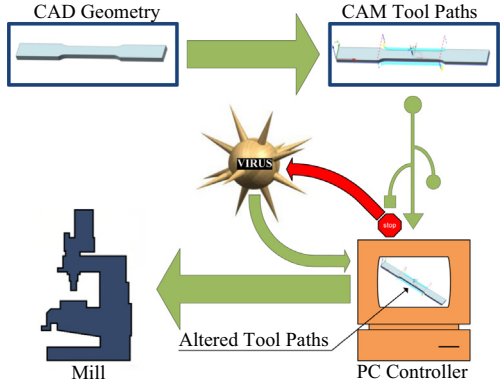

Fig. 2. Cyber-Attack Implementation for Case Study.

The last four groups were encouraged to measure the fabricated specimens. As a result, each group determined that their part was incorrect. Three diagnostic approaches were taken to determine what went wrong.

- The first approach, followed by two groups, was to go through every step of the process, checking CAD/CAM parameters and data transfers between steps. Although time consuming, this approach led to the "correct" conclusion that the PC was incorrectly transferring the tool path file.
- The second approach (one group) was the opposite of the first; every step was checked in reverse order. In this approach the error in the file transfer went unnoticed as the group did not consider it a possible point of failure, and thus resulted in no diagnosis.
- The third approach (one group) consisted of randomly checking different process steps that could have gone wrong. Without a systematic process of deduction, no diagnosis was made.

Even though two of the seven groups successfully determined that part quality was comprised from file transfer error, no group was able to diagnose the problem as a cyber-attack.

4. Conclusions

As technologies progress, more facets of human life are enveloped into the digital world. This opens the door to a vast array of cyber-attack opportunities spanning across social, economic, political, and industrial sectors. As a pre-emptive measure, it is vital that weaknesses are identified, addressed, and ultimately removed. While the case study described herein involves novice engineers fabricating a simple part, it showcases several cyber-security weaknesses that plague manufacturing. Specifically, it demonstrates that even a simple attack on a tool-path file can significantly impact a part's performance. In addition, it demonstrates that future engineers are unaware of the threats cyber-attacks pose, and when subjected to an attack, are unable to efficiently or effectively diagnose the cause.

References

[1] Rost J, Glass RL. The dark side of software engineering: evil on computing projects. John Wiley & Sons; 2011.
[2] Centre for the Protection of National Infrastructure. Cyber security in civil aviation; 2012. Available from: http://www.cpni.gov.uk/documents/publications/2012/2012020-cyber_security_in_civil_aviation.pdf [Retrieved August 7, 2013].
[3] Manzo V. Stuxnet and the Danger of Cyberwar; 2013. Available from: http://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030?page=show [Retrieved August 7, 2013].

[4] Rashid FY. Cyber Attacks Against Stock Exchanges Threaten Financial Markets: Report; 2013. Available from: http://www.securityweek.com/cyber-attacks-against-stock-exchanges-threaten-financial-markets-report [Retrieved August 7].
[5] Lewis JA. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic & International Studies; 2002.
[6] Evans D. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. CISCO White paper; 2011. Available from: https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Retrieved March 13, 2014]..
[7] Bayuk J, Cavit D, Guerrino E, Mahony J, McDowell B, Nelson W, Snevel R. Malware Risks and Mitigation Report. Washington, DC: BITS Financial Services Roundtable; 2011.
[8] Watin-Augouard M. Prospective Analysis on Trends in Cybercrime from 2011 to 2020. National Gendarmerie; 2011.
[9] Cardenas A, Amin S, Sinopoli B, Giani A, Perrig A, Sastry, S. Challenges for securing cyber physical systems. In: Workshop on Future Directions in Cyber-Physical Systems Security. DHS; 2009.
[10] Scott MW. Sacramento man pleads guilty to attempting to shut down California's power grid. United States Attorney: Eastern District of California, News Release; 2007.
[11] Scott MW. willows man arrested for hacking into Tehama Colusa canal authority computer system. United States Attorney: Eastern District of California, News Release; 2007.
[12] Slay J, Miller M. Lessons learned from the maroochy water breach. Critical Infrastructure Protection – IFIP International Federation for Information Processing 2007;253:73–82.
[13] Kravets D. Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System; 2009. Available from: http://www.wired.com/threatlevel/2009/03/feds-hacker-dis [Retrieved August 9, 2013].
[14] Poulsen K. Ex-Employee Fingered in Texas Power Company Hack; 2009. Available from: http://www.wired.com/threatlevel/2009/05/efh/ [Retrieved August 9, 2013].
[15] Igure VM, Laughter SA, Williams RD. Security issues in SCADA networks. Computers & Security 2006;25(7):498–506.
[16] Ten CW, Liu CC, Manimaran G. Vulnerability assessment of cybersecurity for SCADA systems. IEEE Transactions on Power Systems 2008;23(4):1836–46.
[17] Ericsson GN. Cyber security and power system communication – essential parts of a smart grid infrastructure. IEEE Transactions on Power Delivery 2010;25(3):1501–7.
[18] Cárdenas AA, Amin S, Lin ZS, Huang YL, Huang CY, Sastry S. Attacks against process control systems: risk assessment, detection, and response. In: Proceedings of the 6th ACM symposium on information, computer and communications, security; 2011. p. 355–66.
[19] Stamp J, Dillinger J, Young W, DePoy J. Common vulnerabilities in critical infrastructure control systems. SAND2003-1772C. Sandia National Laboratories; 2003.
[20] Hahn A, Kregel B, Govindarasu M, Fitzpatrick J, Adnan R, Sridhar S, and Higdon M. Development of the power cyber SCADA security testbed. Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research, New York; 2010. p. 21:1–21:4.
[21] Morris T, Vaughn R, Dandass YS. A testbed for SCADA control system cybersecurity research and pedagogy. Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research, ACM; 2011. p. 27.
[22] Luallen ME, Labruyere JP. Developing a critical infrastructure and control systems cybersecurity curriculum. 46th Hawaii International Conference on System Sciences (HICSS); 2013. p. 1782–91.