Preventing Cybercrime in Industrial Manufacturing Operations

April 30
2015

GO TO WEBSITE FOR MORE INFORMATION

By Marcellus Buchheit, Wibu-Systems USA

New connected technologies are rapidly advancing and dramatically changing the landscape of the modern manufacturing environment. At the core of these advances are the next generation of IP-based devices and systems and the software used to program and control them. Control systems are increasingly interconnected and communicate via public networks. Machinery can be monitored and controlled remotely and production data can be collected in real-time on the shop floor, enabling managers to make faster, more informed decisions, operate more efficiently, and turn out more product in less time.

The increasing reliance on IP-based manufacturing, however, has opened the door to cyber attacks on critical systems designed to control, supervise and automate the operations. A report by the Center for Strategic and International Studies (CSIS) and sponsored by McAfee, concluded that cybercrime costs businesses approximately $400 billion worldwide, with an impact on approximately 200,000 jobs in the U.S. and 150,000 jobs in the EU. The report found that cybercrime's effect on intellectual property (IP) was particularly damaging, and countries where IP creation and IP-intensive industries are important for wealth creation lost more in trade, jobs and income from cybercrime than countries depending more on agriculture or industries of low-level manufacturing.

Furthermore, the report predicted that the cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet.

Beyond the socio-economic losses resulting from cybercrime, one must consider the danger posed by malicious attacks on critical infrastructure and industrial processes, like transportation systems, drinking water filtration plants, or utilities. For example, recall the disruptive ability of cyber espionage demonstrated by the 2010 attack that used a computer virus called Stuxnet to temporarily disable 1,000 centrifuges that Iranians were using to enrich uranium.

Cyberthreats are Real

The threats to connected manufacturing operations are real and give rise to a need for secure counter measures; not only to prevent the loss of intellectual property but to prevent the introduction of malware through code tampering. These threats are increasing because most new industrial process systems are based on standard operating architectures like VxWorks or Embedded Linux which can be easily analyzed globally to the find the weakest points to start the malicious attack. The theft of intellectual property can be readily seen in the counterfeit products that appear in the global market, from low cost consumer goods to high end electronics. Hackers can steal IP, and in many cases, the manufacturer may not even be aware of the theft until they find their copied products being sold openly.

Consider how these threats can materialize:

An attacker can develop a device that appears similar to the original but whose functions have been altered for harmful purposes.

A hacker develops his malicious software and installs it by replacing the memory card in an embedded system.

An attacker extracts the memory cards from an embedded system, manipulates the software, and reinstalls it into the system.

An attacker remotely controls the communication interfaces from outside and alters the data without ever accessing the premises.

Manufacturers, however, can protect themselves and their equipment from cybercrime. Automated manufacturing equipment, from individual controllers to entire plants, relies on the use of individual or multiple integrated control systems, typically including a combination of both hardware and software that plant engineers use to program the desired applications. Software is the critical component for the proprietary functions and applications. The integration of software protection in these machines can prevent the copying of machine designs or the illicit transfer of intellectual property and competitive know how. Furthermore, available software protection technology prevents sabotage and manipulation of the software.

Preventive Measures from Third Parties

Fortunately, software security firms offer several off-the-shelf solutions whereby manufacturers can safeguard their systems and assets. From a business perspective, these protective measures prevent the copying of machine designs and the unlawful transfer of essential intellectual property. From a technological standpoint, the solutions are used to prevent cyber attacks in the form of reverse engineering, code tampering and privacy breeches.

Many commercial security solutions are based on strong encryption and embedding of secure hardware elements (like dedicated ASICs and smart card chips) that can be used for software protection, IP protection and integrity protection. As the digitalization of manufacturing operations increases, the relevance of digital data protection in production and, more generally, of networked data protection and systems integrity will play a much greater role.

Several of these solutions make use of symmetric encryption technology, where software is stored encrypted in a device's non-volatile memory. At runtime, required parts of the software are decrypted in the RAM of the system. The cryptographic keys for this decryption are stored securely in TPM (Trusted Platform Module) chips or smart card chips in industrial dongles so that they cannot be duplicated. In this way, the software in the embedded control device is protected and prevents the theft or reproduction of intellectual property.

Another preventive measure is enabled by also encrypting the program code, which renders use of compilers and disassemblers for reverse engineering nearly impossible.

More sophisticated security techniques can also be implemented, including integrity checks, secure boot loading, and chains of certificates.

Real World Examples

With headquarters in Belgium, the LVD Group is a worldwide manufacturer of software-driven sheet metal/plate working machine tools and automation systems. The power of LVD's success is the result of symbiosis between the intelligent LVD offline software and technological machine performance. Their new generation of metalworking machines incorporates an advanced touch screen graphical user interface that provides the company with a significant competitive advantage in machine performance. Given the strategic advantage provided by their proprietary software, LVD realized the importance of protecting their IP investment and implemented a third party software protection solution (CodeMeter from Wibu-Systems) to prevent reverse engineering and piracy.

The Dutch VMI Group is a global tire machine manufacturer. Their automated machinery is used in the manufacture of 20% of the world's tire production. Their manufacturing systems incorporate automation software and are driven and monitored by sophisticated sensors and vision cameras. With field engineers servicing these automated tire production machines around the globe, VMI felt the need to secure access to the Programmed Logic Controllers on installations. To protect against tampering or unauthorized access to their machinery and protect its intellectual property, they implemented a commercial solution (CodeMeter from Wibu-Systems) for password storage and management technology, a strong authentication capability, and remote password handling.

"There's a high degree of knowledge and programming work necessary for the control requirements of tire production. Our software contains essential algorithms that control the operation of our machines; a reason why we need protection. Precautionary measures to manage access to the code, especially for remote locations, are essential," said Jan Grashuis, Vice President R&D, The VMI Group. "

Passwords used by the field engineers to access the controllers are encrypted and stored in either a secure dongle, which is a tamperproof hardware device incorporating an embedded smart card controller, or a software license file. A password manager in VMI's corporate office grants user rights to the field engineer remotely from a central corporate server. Once granted rights, the service engineer can then maintain only the assigned machines for only the set of functionalities and time range granted by the password manager. In this way, VMI protects its machinery from any fraudulent modifications.

In conclusion, it is clear that cyber threats to IP-enabled, automated manufacturing operations are real, and as more machines and system become interconnected, the threats will grow. Responsible manufacturers need to make the business choice to protect their devices, systems and Intellectual Property from theft and tampering.

About the Author

Marcellus Buchheit is cofounder of WIBU-SYSTEMS AG, a global leader in secure and flexible licensing, IP protection, and anti-piracy technologies for software publishers and embedded systems providers. He currently acts as the President and CEO of Wibu-Systems USA.