Security tools for Industry 4.0

March 5 2014

To protect the applications of Industry 4.0 – such as Fraunhofer IGD's visual computing solutions – Fraunhofer SIT engineered security solutions that safeguard both people and equipment. Credit: Fraunhofer IGD

An increasing number of unsecured, computer-guided production machinery and networks in production facilities are gradually evolving into gateways for data theft. New security technologies may directly shield the sensitive data that is kept there.

You can hear the metallic buzz as the milling machine bores into the workpiece. Just a few last drill holes, and the camshaft is complete. The computer-guided machine performed the entire job – thanks to the digital manufacturing data that were uploaded onto its embedded computer beforehand. Everything runs without a hitch, only – the data are stolen.

Manufacturing data determine the production process for a product, and are just as valuable today as the design plans. They contain distinctive, inimitable information about the product and its manufacture. Whoever possesses this info merely needs the right equipment, et voilà: the pirated or counterfeit product is done. Whereas design data are well-protected from unauthorized outside access today, production data often lie exposed and unsecured in the computer-assisted machinery. An infected computer on the network, or just a USB stick, are all a thief would need to heist the data. Or hackers could directly attack the IT network – for instance, through unsecured network components, like routers or switches.

Encrypting manufacturing data upon creation

Researchers at the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt are exhibiting how these security gaps can be closed up at this year's CeBIT from 10 to 14 March, 2014 (Hall 9, Booth E40). They will be presenting, for example, a software application that immediately encrypts manufacturing data as soon as they emerge. Integrated into computer and equipment, they ensure that both communicate with each other through a protected transportation channel and that only licensed actions are executed. "To the best of our knowledge, no comparable safeguard has previously existed for manufacturing data that reside directly in the machine tool," states Thomas Dexheimer from the SIT's Security Testlab. Digital Rights Management (DRM) controls all important parameters of the assignment, such as designated use, quantity, etc. This way, brand manufacturers are able to guarantee that even external producers can only produce an authorized quantity, as instructed in advance – and no additional pirated units.

His colleague at SIT, Dr. Carsten Rudolph, is more involved with secured networks. At CeBIT, Rudolph will exhibit his "Trusted Core Network". "Hackers can also gain access to sensitive production data via unsecured network components. These are small computers themselves, and can be easily manipulated," says the "Trust and Compliance" department head at SIT. In order to prevent this, he called upon one piece of technology that, for the most part, lies dormant (in deep slumber) and, for all intents and purposes, unused on our PCs: the Trusted Platform Module. This relates to a small computer chip that can encrypt, decrypt, and digitally sign the data. Installed into a network component, it indicates which software is running on the component, and assigns a distinct identity to it. "As soon as the software changes in a component, the adjacent component registers this occurrence and notifies the administrator. Hacker attacks can be exposed quickly and easily this way," says Rudolph.

"Both security technologies are important building blocks for the targeted Industry 4.0 scenario," says Dexheimer. The term "Industry 4.0" stands for the fourth industrial revolution. After water and steam power, followed by electrical energy, electronics and information technology, now, the cyber-physical systems (IT systems embedded in machinery that communicate with each other via wireless or cabled networks) and the Internet of Things are expected to move into the factory halls. "This revolution can only work if the intellectual property is sufficiently protected. And that's a tall order, because the targets of production IT will increase exponentially, due to ever growing digitization and networking," explains Dexheimer.

At this year's CeBIT, both researchers – Dexheimer and Rudolph – will present a computer-assisted machine tool using a CAD computer and a 3D printer. SIT's security software is installed both on the computer and the printer. The data are encrypted on the computer, and decrypted by the printer. The printer also validates the licensed authorization to conduct the print job. To ensure that the data are also securely embedded in the network, the scientists have built a Trusted Platform Module into multiple routers, and are displaying this as a demo. "An attacker cannot hack this there, because he or she will get nowhere near the built-in key," explains Rudolph.

Provided by Fraunhofer-Gesellschaft

Citation: Security tools for Industry 4.0 (2014, March 5) retrieved 27 April 2024 from https://phys.org/news/2014-03-tools-industry.html