Tech Now

PRODUCT PIRACY - STOPPING VIRTUAL THIEVES IN THEIR TRACKS

© Wibu-Systems AG

In times of Industrie 4.0, virtual thieves are particularly dangerous. Based on digital templates, they create identical products that cannot be differentiated from the original. VDMA members present ways for manufacturers to protect themselves.

By Nikolaus Fecht

They don't break locks, smash windows or climb over fences, but they're still more dangerous than any burglar. We're referring to hackers, who penetrate industry IT systems like virtual thieves and spies. A survey of VDMA members on successful countermeasures shows how the industry can protect itself.

Counterfeiting as a service has established itself

The danger of data theft grows with Industrie 4.0 as new threats come along with it. If product pirates gain access to digital templates for 3D printing they can create identical parts that cannot be identified as counterfeits. This being the case, there already are commissioned counterfeiters who are cooperating with 3D manufacturing centers specialized in this.

"Digital templates, software in plants and central databases are the primary target of attacks," warned VDMA President Dr. Reinhold Festge in the preface of the new study on product piracy from the VDMA Product and Know-how Protection working group. He highly recommends investing in digital protective measures against product piracy.

Taking knowledge protection seriously

Oliver Winzenried, CEO and founder of Wibu-Systems AG in Karlsruhe, agrees. He carefully observes the trend to Industrie 4.0 with great interest. The chairman of the Product and Know-how Protection working group ("Protect-ing") sees that products with standardized hardware "can execute various functions by configuring software and parameters as positive, which can be updated and upgraded in the field, and thus new business models arise for manufacturers." However, he said the necessity to protect data and information of products in development and production rises with increasing functionality. "This conclusion also hits our customers in automation technology and in mechanical and plant engineering," reported Winzenried. "We are involved with several research and development projects on this topic in Germany, and leading mechanical engineering companies take them very seriously."

Traceability is the means to an end

Winzenried recommends that manufacturers implement a mix of product and knowledge protection measures that depends on the product. On one hand, training and "employee awareness" are said to be in demand, so that employees can identify their values to be protected and thus do not provide sensitive production details to suppliers about their bidding. On the other hand, legal and technical protective measures are said to be necessary. Traceability of products in the production and sales process is said to be a means to that end. "Traceability adds value in logistics and can be used for plausibility checks," said Winzenried. "The user can thus differentiate between the original and counterfeit products due to the use of smart labels."

Preventative protection is also important here. Winzenried recommends “trust anchors” associated with secure elements to encrypt software functions in production and store the keys securely away from any cloning attack. In his opinion, all of these protective measures make imitation and product piracy more difficult. He especially advises using them if devices (“Internet of Things”) and machines contain digital production data, parameters and embedded software.

According to the VDMA study “Product piracy 2016”, released in April 2016, up to 70 percent of the companies taking part in the study, indicated reverse engineering as the leading cause of successful product piracy. Embedded security - embedded IT systems with protective functions (e.g. encryption) - has apparently been successful as a countermeasure. “To me, security is protection against manipulation,” explained Winzenried. “Electronic signatures and asymmetrical cryptography is used for this, so that systems themselves can check whether software and data are not manipulated and come from an authorized dealer.” And therefore it is important that all connected devices in an intelligent machine or plant get a forgery-proof identity. This security measure is absolutely necessary for future open industrial networks. Embedded security can make an important and reliable contribution here.

Protecting intellectual property

How this can work in practice can be seen in two typical cases: A manufacturer from the textile machinery industry protects his machines from imitation by blocking access to the embedded software in control, which contains important knowledge - for example about especially fast and high-quality embroidering of textiles. “The machines can also process protected production data, known as punch data. This method allows not only the mechanical engineering company’s knowledge to be protected but also the customers’ intellectual property in the product data,” said Winzenried.

He went on to explain that the system also records the number of produced lots in order to prevent someone from using original production data in a textile factory to manufacture products at own cost for the gray market during an extra shift and going unnoticed.

The second example is taken from the industrial automation technology. In programmable logic controllers (PLC), embedded security helps with configuring the PLC functions. This measure makes selling easier for the control manufacturer and enables export control of functions subject to approval. “In development environments of mechanical or plant engineers, knowledge protection is also becoming more frequent,” explained Winzenried. He went on to say these measures and the integration for assigning of access rights into business processes is very important for worldwide service.

Secure transmission channels

Michael Wenninger, Senior Business Development Manager at MAN Diesel & Turbo SE in Augsburg, has been involved with Industrie 4.0 and the consequences thereof. “In the course of digitalizing the value chain, data exchange nearly exclusively established itself via digital media transfer making everyday processes more efficient and convenient. But keeping an eye on data security also harbours risks,” said Wenninger. It’s important for users to secure data transfer channels as well. The Augsburg company thus installed their own cloud (“Online-Service”), where they save and evaluate sensitive machine and sensor data such as their customers’ motors. This takes place, for example, in predictive maintenance situations. Wenninger explained further: “We use our own secure data tunnel based on the virtual private network principle for data transfer. Though because this isn’t one of our core competencies we get help from specialists of the associated industry who ensure secure technology.” The MAN manager recommends using the same standards across the sector. This creates a sustainable frame for efficient interoperability across company and country borders and for competitiveness in the connected market environment.

Uniquely identifying products

For upfront protection, Wenninger recommends a unique identification number for products utilizing automated technology solutions, where the number can also be used for other types of applications in logistics, supply chain and spare parts sales. According to him, it is with a flexible procedure that offers a multitude of measures and functions. This method would allow a scanner to retrieve operating instructions or uniquely identify a product by its serial number using, for example, a machine-readable DataMatrix code. This is where traceability comes in. “Thanks to the DataMatrix code, we can assign individual components of our motors various individualized information, for example, about wear and tear,” stated Wenninger. He went on to say, “we elegantly get a valuable feedback loop for our development in this manner.”

For MAN Diesel & Turbo, the goal of combining traceability and DataMatrix code is primarily for easy identification of the right component. “For us, the focus is avoiding a limitation of system availability and operation security due to faulty components. What’s important to us is ensuring the high quality and durability of our products,” explained Wenninger.

Product protection with RFID

René Steiner, Business Development Manager RFID at Hans Turck GmbH & Co. KG from Mülheim an der Ruhr, thinks that many mechanical engineering companies “are at risk of product piracy.” There is a trend, he said, especially when it comes to equipping parts of machines with RFID-Tags, and that this ‘tagging’ increases the added value of a machine. The control of a machine, he said, could perhaps automatically read the associated characteristic parameters from the integrated RFID data carrier when exchanging a roller.

Encrypting data using UID

For protecting sensitive data, Steiner recommends encrypting data with a unique identification number (UID) and an additional individual key in the higher-level system, in addition to an RFID password already present as an option. This allows data to be copied to other data carriers but they lose their validity due to the lack of key.

Additionally, he said, there is the option of labeling the data carrier with a special invisible individual marking. All of these measures contribute to the capability that only experts with the corresponding knowledge and the right equipment are able to fully copy an electronic component.

This method has proven itself in practice again and again. As such, Turck customers already equip their filters with RFID chips. “The machine’s control reads the chip and warns about using incorrect filters,” reported Steiner. The filter usage will also be saved in the machines’ electronic log. He said this creates transparency for both the machine’s manufacturer and the end customer in case of complaints.

For the end customer, he said, this additionally means avoiding dangers to persons and machines due to the use of inferior or counterfeit spare parts. Even rollers and cutting dies now contain RFID chips with which the component can be uniquely identified. The electronics allows the customer not only reliable identification, but also recording and saving important characteristic parameters and production data, such as in the case of maintenance.

Potential for cyber attacks

“Industrie 4.0 offers great potential for innovations, but also harbours numerous new loopholes for cyber-attacks,” observed Christoph Plass, member of the Managing Board of Unity AG from Paderborn. Attackers would no longer need physical contact to a system in order to steal intellectual property. Particularly, access to IT systems and lines of communication create new vulnerabilities, in his opinion: They thus need to be secured.

In addition, he said such intelligent technical systems can only be developed if manufacturers and their partners (suppliers) become more interconnected. However, successful cooperation relies on exchanging technical data, such as with 3D printing or with predictive maintenance. This being the case, technological inventions have to be protected against product piracy or theft. “Preventative measures for protecting intellectual property are thus to be proactively integrated into strategies, processes, products and systems,” recommended Plass.

Limiting access to data

He said the ideal protective measure for companies is the combination of legal, organizational and technical protection. Patents and registered design are included as legal measures. “Unfortunately, damage is already done before these measures work,” said Plass. For this reason, every manufacturer should also select suitable technical protection systems in order to proactively protect against product piracy. This could be done through labeling technologies, track and trace and preventative protection for software and knowledge. Companies should consider attacks from within and via cooperation with suppliers, and in addition, to concepts such as access control, make sensitive information and data only accessible to certain people.

A secure identity is key

In order to ensure the protection of intelligent technological systems, the challenges of system protection must be addressed and taken into consideration. “This is where the project team performs a decisive

measure: the sustainable measure ‘Prevention against product piracy - ‘itsowl-3P’” from the top cluster ‘it’s owl’” reported Plass. The collected recommendations about cluster management are made available to companies. He said a secure identity is important and is one which cannot be manipulated, falsified or abused. Furthermore software encryption alone isn’t enough to protect against attacks on machine codes. Ideally, the key is stored in specially protected hardware that can neither be read nor manipulated.

3D print against product piracy

Plass recommends additive production processes, often called 3D printing, as an option for protection against counterfeiting. This was how a specialist for aquarium lighting and water care developed a novel pump impeller via laser sintering. He said, “this production technology gives developers entirely new possibilities for design and offers companies special advantages against product counterfeiters.”

Further Information

pks.vdma.org/security | www.protect-ing.de | MAN Diesel & Turbo | Turck | Unity | Wibu-Systems | VDMAimpulse 01-2016 “Security: a moving target” | VDMAimpulse 01-2016: “A part of the game”

Contact

Steffen Zimmermann, VDMA Informatics, Managing Director Product and Know-how Protection,
E-Mail: steffen.zimmermann@vdma.org