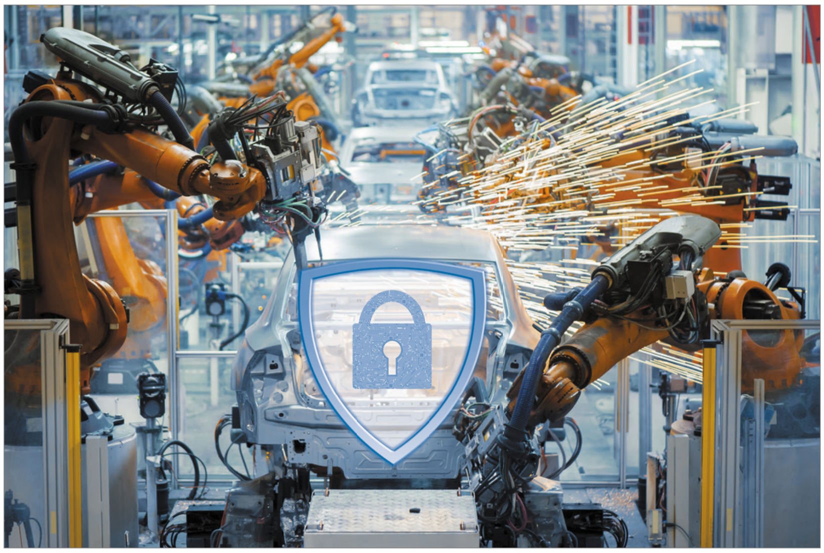
TECHNISCHE UNIVERSITÄT WIEN
Vienna | Austria

Information & Software
Engineering Group
Favoritenstraße 9
1040 Vienna, Austria
www.ifs.tuwien.ac.at

More IT Security for Integrated Industry

Customized security solutions protect production systems for Industry 4.0 from cyber attacks – as early as in the development phase



Picture: © shutterstock.com/xieyuliang

The computer worm Stuxnet sabotaged entire industrial plants some years ago. It targeted nuclear facilities in Iran, in particular, and made the media and a wider public aware of the potential of malware used to attack production facilities for the first time. Stuxnet triggered a long overdue rethinking of information security in this domain.

Cyber attacks on industrial plants have fallen off the public's radar again since Stuxnet, but the threat situation has actually grown worse. According to the 2016 annual report of the US authority ICS-CERT, the numbers had increased from approx. 140 to over 220 detected and reported attacks per year in the four years preceding the report. The number of unreported attacks is presumably considerably higher, as companies often do not report incidents out of fear of reputational damage.

The widespread introduction of networked production systems for integrated industry or Industry 4.0 is opening new avenues of attack to cyber criminals to target industrial plants as they were largely not connected to networks before.

In addition to production systems in operation, the planning phase is increasingly vulnerable. Criminals may introduce deficiencies that remain dormant and undetected until the plant is in operation via targeted attacks during the development process of plants already. This approach allows hackers to halt production processes without having to execute an external attack on a plant in operation. This can also be used to spread malware and infect other systems.

Stuxnet was a highly complex worm, but by gaining early access during the development phase a similar attack is far more easily effected and can potentially affect any industrial plant.

The Information & Software Engineering Group at TU Wien is developing effective protection mechanisms for production systems engineering (PSE) to allow companies to prepare against this new type of threat by means of qualified security measures.

Objectives

To be able to operate digital factories reliably, the security of data, of information, and of production processes must be ensured. This requires a comprehensive security concept covering the entire development process. Therefore information processes have to be protected from the conceptual stage onwards.

A crucial part is the access to shared documents and data sets for multiple parties, which is realized by networked data repositories. The increased use of such repositories and the growing number of partners involved – possibly of varying reliability – complicates the protection of these valuable resources.

Therefore, it is necessary to design information processes that ensure maximum security while neither limiting the functionality of repositories nor impeding efficient development work.

Solution

The solution developed by TU Wien entails individually tailored security measures for information processes, the use of tried and tested methods for security by design in production systems, and adapting testing processes to allow the rapid identification of security flaws.

Proven security concepts from the domain of software development are applied to the planning of industrial plants. This results in the following individual measures:

- Integration of security functionalities in industry data formats such as AutomationML
- Efficiently securing key data repositories for the engineering process
- Customized modeling of realistic threat scenarios for production systems
- Risk assessment for planned and existing industrial plants (security ontology)
- Design and implementation of security tests in the testing and verification phase of the production system

Notes

Results

Experience from software industry shows that the introduction of a secure development cycle evidently improves information security and operational reliability. Such “Secure Software Development Lifecycle” (SDLC) was, for example, introduced by Microsoft in 2002. By 2008, the number of vulnerabilities in new operating systems had been reduced by 60%. It seems obvious that this kind of comprehensive and effective security strategy should also be established as state of the art in developing and planning production systems.

Your Benefit

To protect your company from stoppage in production or damage to your reputation caused by malware, TU Wien offers support and project cooperation in the following areas:

- Consulting on the implementation of a secure development cycle for production systems
- Conceptual design of secure information processes
- Security analysis of industrial components
- Security consulting for existing production systems
- Network analysis training for the detection of attacks on industrial plants

Kontakt

Dr. Edgar Weippl
TU Wien - Information & Software
Engineering Group
www.ifs.tuwien.ac.at
T: +43 1 58801 18888
edgar.weippl@tuwien.ac.at