Fraunhofer SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

TRUSTED CORE NETWORK

HARDWARE-BASED SECURITY FOR INDUSTRIAL IT NETWORKS

Fraunhofer Institute for Secure Information Technology

Contact:
Andreas Fuchs
Rheinstrasse 75
64295 Darmstadt
Germany

Phone +49 6151 869-228
Fax +49 6151 869-224
andreas.fuchs@sit.fraunhofer.de
www.sit.fraunhofer.de

To improve production, control and maintenance processes, companies increasingly interconnect their industrial environments with office IT and internet. This also intensifies the threat that operation flow may be impaired or that attackers may specifically manipulate or sabotage industrial equipment and machines. In order to counter this Fraunhofer SIT has developed a hardware-based solution for safeguarding industrial networks. Security information does not interfere with data routed through the network, therefore it meets the specific industrial requirements with regard to real-time performance, availability and IT security level, and can be integrated easily and inexpensively into existing industrial IT networks.

Special requirements apply to IT infrastructures in manufacturing plants and in automatization processes. To prevent production downtime, system availability and meeting the real-time requirements of the communication technology are essential for production and control processes. Until recently, industrial environments and their IT networks have been separate from office IT and internet. Today the industry is increasingly connecting heterogeneous IT networks to improve production flow and reduce stock, even to networks outside of the producing company's control.

Firewalls and Virtual Private Networks (VPN) are considered state-of-the-art for protecting networks. These approaches are well established in the IT world. However, often they do not fulfill the specific requirements industrial environments pose, because they delay process relevant communication in part and may occasionally even cause an increased complexity. Furthermore, the protection of industrial networks' borders or perimeters has different requirements. For example, remote maintenance of production plants: Here it is often imperative to involve service providers, which leads to a complex threat situation. Besides, conventional IT security architectures do not guarantee the high availability typically required for industrial plants, because office IT security requirments cannot be compared to the requirements demanded in production and automatization: For example, the manipulation of control systems may result in physical damage or even be dangerous for humans or the environment. Issues such as the warranty for leased machines have to be considered as well. This is why Fraunhofer SIT and its partners have developed an innovative solution, in which network nodes are safeguarded as sensitive constituents, thus providing a trusted basis for implementing secure information and communication infrastructures.

Hardware-based Trust Establishment

Fraunhofer SIT's Trusted Core Network (TCN) is able to review a node's identity and to guarantee the node's desired state: For this TCN uses a distributed/redundant node control, checking in a peer-to-peer manner the identity and state of the neighboring nodes. A Trusted Network Discovery protocol facilitates locating all active devices within the direct environment. Using the Trusted Platform Module (TPM) the system identifies the node and compares the current state to the target state. Modifications or manipulations can thus be detected in a fast and distributed manner, alerts will be sent directly to central monitoring and the spreading of attacks and malware can be prevented. Besides the device's identity, the Trusted Core Network reviews downloaded executable software and configuration data. If changes are found appropriate countermeasures can be taken, so that essential functions may be maintained (resiliency), even in the case of manipulations or successful attacks on individual components.

Zero-Touch Configuration

Once a new device is integrated into a Trusted Core Network it has to be configured accordingly. To facilitate efficient management Fraunhofer SIT has developed a protocol for Zero Touch Configuration, based on the TPM security functions. Registering the devices only requires a unique device ID, for example the fingerprint of a cryptographic key imported automatically via QR code. During device production, no customer specific information needs to be implemented, so that the extra costs typical for complex security solutions may be avoided, as is the case in public key infrastructures, for example. When the technician hooks up the device, the configuration and the registration among other things are initiated automatically. No USB sticks, laptop or user interface at the device is required for configuration. An intervention would be necessary only if a failure or fault occurs.

Implementation

Fraunhofer SIT and two of its industrial partners realized the Trusted Core Network concept as a prototype for two operational environments. For the industrial networks, commercially available Hirschmann Eagle routers were used, enhanced by TPMs at the I2C bus. These routers review all directly adjacent devices and report the results to an IF-MAP server, which is used to visualize the information about the current network state.The Trusted Core Network was developed within the BMBF project ANSII to provide a secure foundation for anomaly detection in industrial webworks.

Wireless Trusted Networks

Especially in spacious installations the wired or Access Point centric communication can be problematic. Accordingly, so called Mobile Ad-Hoc Networks (MANET) are deployed in these scenarios. In a MANET, all devices act as a node and relay routing information to other nodes. TrustMANET developed by Fraunhofer SIT applies the Trusted Core Network concept in mobile ad-hoc networks. The nodes check each other before a new one is admitted to the network. This check will then be repeated on a regular basis. This also impedes the spreading of attacks in a network. TrustMANET was partly funded by the European Commission in the SecFutur project.

Service offer

In the context of hardware-based security, Fraunhofer SIT can provide support, research and development in the following areas:

- Development of security architectures for the specific requirements of critical information and communication technology in production, automatization and highly integrated systems
- Integration into existing security mechanisms
- Development of new protocols and security functions
- Support during the development of new products
- Enhancement of existing product lines with hardware-based security
- Consultation on hardware-based security
- Evaluation of security architectures
- Practical security tests of machines, devices and components

Project partners:

infineon

HIRSCHMANN
A BELDEN BRAND

Funding partners:

Project SecFutur has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 256668.

Project ANSII has received funding from the Federal Ministry of Education and Research.

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung