Defence-In-Depth: IT Security For Energy Automation

Dr. Stephan Hutterer

Sprecher Automation GmbH, Linz / Austria
Product Manager
stephan.hutterer@sprecher-automation.com
Whitepaper / Published: 12.04.2017

Both the increasing number of security-relevant incidents and the current legal requirements are a considerable challenge for operators of critical infrastructures. IT security must be deeply anchored in devices fulfilling control functions in order to provide sufficient protection for power grids. This paper discusses the concept of defence-in-depth respectively necessary technologies in the domain of power system control and protection.

I. Introduction

There is a significant rise in the number of cyber attacks, specifically in the field of critical infrastructures. Legislation provides for stringent provisions concerning the operation of critical infrastructures such as energy grids, at national level - for example in Germany by the Law on IT security [1] and at European level via the NIS (Network and Information Security) Directive [2]. Thus, operating companies are faced with new challenges, both technologically and economically speaking, in order to implement IT security in their systems.

Today, manufacturers of devices and equipment are required to offer economical and practical solutions to support their customers at their best. Modular automation platforms for energy transmission and distribution are in development for application in critical infrastructures. Software engineers and IT professionals must consider their task as not only to provide mature and hardened products but also to give comprehensive advice as system integrators in order to cope with these challenges together with their customers.

II. In-depth protection by Defence-In-Depth

An all-round protected system calls for mature mechanisms at all levels. In this context regarding secure system architectures, the BDEW Whitepaper [3] also demands the very central Defence-In-Depth principle. This principle describes the general necessity to provide continuous protection by implementing interlocking security concepts at all system levels. This approach has the clear advantage that even if a potential attack was able to overcome a hierarchically external security measure, it would be ultimately prevented by additional in-depth security mechanisms.
Regarding automation and protection equipment, this would mean, for example, that encryption processes and network segmentation are applied for network security at an external security layer. But even in case these mechanisms were overcome and sent data was manipulated, the equipment would be able to recognize potential tampering in the messages received and would be able to react accordingly.
Thus, Defence-in-Depth is a fundamental concept in the system architecture of digital systems to be secured, which is not only relevant in general, but is also demanded specifically by directives and standards relevant to the energy industry such as the BDEW Whitepaper[1] or IEC 62351 [4], and must be consequently implemented.

III. SPRECON - Practical implementation in modern equipment

Referring to protection or automation devices, fundamental levels or security targets can be defined, structured hierarchically from the inside outwards, which are discussed in detail in the following and shown in Fig. 1:

A. System integrity:

The keyword system integrity includes all measures in order to ensure manipulation prevention of processes and data in the device.

Regarding data, this means primarily examination of received data against validity or plausibility and correctness. This concerns process data received, for example telecontrol telegrams or the contents thereof and also configurations transferred to the device. It must be possible at any time to check transferred data via cryptographic integrity mechanisms, meaning that possible tampering with the data, for example by Man-in-the-Middle attacks, can be detected and processed by the device. While conventional communication protocols for process data include integrity mechanisms as on-boards, manufacturers are especially called upon regarding transmission of configuration data. SPRECON [4] is one such example, and it applies multi-levelled interlocking integrity mechanisms in order to ensure the integrity of processed data.

Preventing process manipulation is an equally important objective. Primarily, it must be possible to ensure that devices can only be operated using valid firmware supplied by the

[1]BDEW German Association of Energy and Water Industries, https://www.bdew.de/internet.nsf/id/EN_Home.

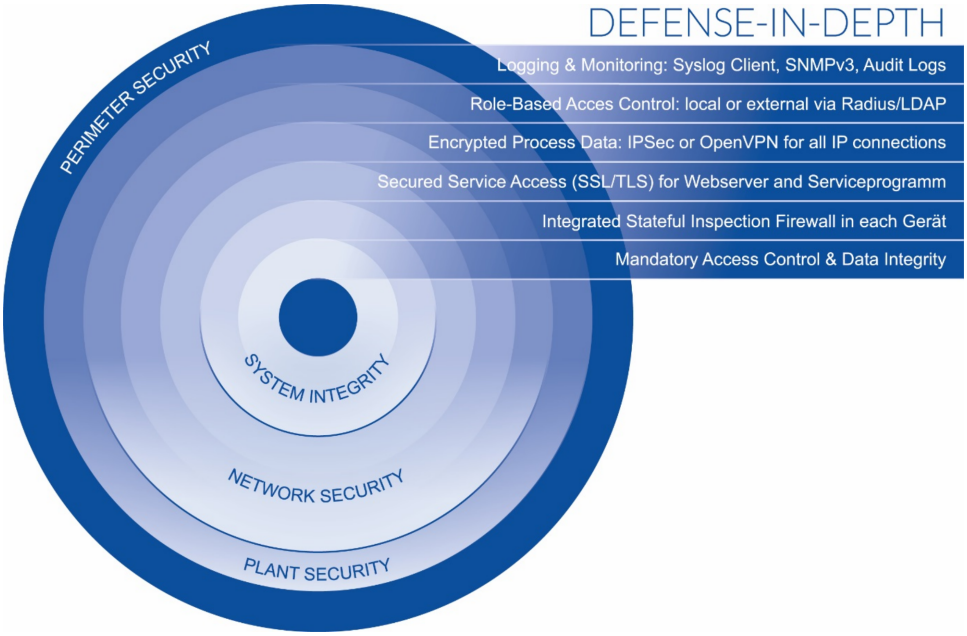

Fig. 1. Defence-In-Depth Concept

manufacturer. To this effect, firmware signatures are used in the SPRECON system. This signature enables the hardware to check ultimately whether the downloaded firmware is valid and signed and is thus tamper-proof. The counterpart necessary to this effect is a mechanism provided by an installed TPM (Trusted Platform Module) which is able to check the firmware using a certificate issued by the manufacturer in the production process. In case manipulated firmware has been downloaded onto the device, the signature fails and the device can therefore block the start or trigger appropriate messages and error handling processes.

Man-in-the-Middle Attacks

With man-in-the-middle (MiM) attacks and attacker secretly relays and eventually tampers communicated traffic between two parties A and B, such that both parties believe they directly communicate with each other. One form of MiM attacks is eavesdropping, where the attacker actively intercepts the communication, such that there are two separated communications from party A to the attacker, and from the attacker to party B, but still those parties believe to have a direct communication link from A to B.

B. System hardening

All measures regarding system integrity protect the control system at the lowermost level. To get access from the network, preceding protective mechanisms must be implemented to rule out access in advance or to enhance such fundamental protection. With this in mind, potential access vectors from the network must be minimized. Exemplary attack vectors could be flooding (e.g. with SYN packages), unauthorized network access, usage of insecure network ports, and many others. This in turn requires comprehensive system hardening at network level (as demanded, for example, in sect. 2.2 of the BDEW Whitepaper [3]).

System hardening is based on a comprehensive and fully integrated firewall within protection and control devices. It enables restricting network traffic in order to permit only packages communicated by and to devices within the network which have been defined in advance. Thus, for example, telegrams issued from third parties can be blocked on principle in advance and the risk involved by so-called Denial-of-Service attacks can be prevented via connection limits. Consequently, integrated firewalls provide a module both elementary and generic for the security of a device which is indispensable for any practical implementation. While the above-mentioned options are only a small choice of what is possible, firewalls provide a comprehensive possibility to completely control the traffic from and to a device.

In addition to the firewall for hardening at network level, hardening measures must also be taken at operating system level. Accordingly, a system may operate and offer within the network only the services that are actually used. If, for example, a web interface is offered for analysis and configuration of the device, but not used by the operator, this implies a both significant and unnecessary risk. Thus, services and especially network ports that are not used must be surveyed and deactivated in any project-specific configuration in order to minimize the risk of attack.

Engineers have created devices which feature fully integrated and configurable Stateful Inspection Firewalls [5,6]. In current projects, this firewall is an essential component in the implementation of secure systems. While contrary to

common external firewalls, an integrated firewall provides a clearly more detailed protection directly in the device, it also reduces the necessity of additional network components, thus reducing the overall system complexity and the maintenance work for the operator. This does not only include configuration of the firewall but also complies with defined configuration guidelines for each project implementation in order to harden devices in accordance with a specific project. Moreover, the (Minimal) Need-To-Know principle must be applied at operating system level. Accordingly, users and processes may only possess the rights required for executing their assigned functions. While some system architecture design provides software processes with minimum rights only, systems such as SPRECON also implement Mandatory Access Control (MAC) which enhances these restrictions additionally and thus permits enhanced security at operating system level [7], where access rights to resources and files are not only assigned to users, but also to user programs and daemons.

C. Access Control and Network Security

To protect a system completely, based on the concepts of network-related device hardening, all accesses to this system must be both secured and controlled.

This calls for the central concept of authentication and authorization of users, meaning that a user, before being authorized to perform certain actions (= authorization), must authenticate (= authentication) prior to using the device (for instance for maintenance or configuration work), for example via user name and password. To facilitate the management of authorizations and users even more, the RBAC (Role-Based Access Control) principle is applied. RBAC assigns roles to users which have a uniform spectrum of rights. Such roles are defined as examples in the BDEW Whitepaper [3] or more detailed in the IEC 62351-8 standard [4]. Thus, the standard roles such as Observer or Administrator are complemented by roles such as Operator. Users having this role would be equipped, for example, with specific rights to change the configuration and operate devices, but would not have an overall authorization for all functions.

It should be noted here that authentication and authorization are always required at the end point and thus last but not least, in the device as such, meaning that the protection or control device must be capable of checking whether a specific access is valid. Interrogation and examination of the user merely at engineering tool level would mean vulnerability to unnecessary attack vectors. User management can thus be centralised by interfacing to an external service, for instance via the RADIUS[2] protocol. Fig. 2 shows an appropriate example.

To this effect, in case of access to a device, this protocol would first check the authenticity of the user via the authentication server before the user is granted access to the system, for example, in order to change configurations or to read analytical data. While in this case the user data can be saved locally, at the device, central management often offers considerable advantages. By interfacing a central authentication service, user data can be managed for the entire network (i. e. for each station or even across several stations) for all devices. Should changes be required (for example: password updates, cancellation of rights for individual users, deleting/creating users), this only needs to be configured at one location and is subsequently available for all the connected devices. However, especially in case of a possible network failure, for example in emergency situations, locally administered users at the device must nevertheless be available in order to permit device maintenance even without connection to the central service. As an additional step for access control, powerful cryptographic encryptions must be provided in order to protect the data communicated between maintenance or engineering computers and the terminal device. Thus, user data transmitted during log-on and all configuration data or system states transmitted subsequently are protected against unauthorized access and manipulation. This is an important safeguard, especially for remote maintenance access performed via WAN (Wide Area Network). In this way, not only maintenance or engineering data, but also process data which is also communicated via WAN, would have to be protected in a strongly cryptographic fashion both in terms of authenticity and of integrity, depending on the scenario.

All these requirements are actually important components for securing systems at network level and must be used to provide overall protection for data systems. Appropriate requirements also exist in current relevant guidelines such as the BDEW Whitepaper [3] or in corresponding parts of the IEC 62351-3 [4] or IEC 62351-10 [4] which include detailed requirements.

For control and protection devices in the energy domain, all access means to devices typically need to be encrypted via HTTPS or TLS 1.2 and thus correspond to a future-proof state-of-the-art in line with ENISA (European Network and Information Security Agency) [8]. While user data for RBAC can be managed at the device in a secure way, any external services can also be interfaced via the standardised RADIUS protocol, for example. Optional VPN (Virtual Private Networks) connections can also be established for secure transmission via IPSec or OpenVPN, thus permitting implementation of cryptographic securing of process data.

IV. Conclusion

IT-Security has become a central technological component in operating energy networks. While operators of critical infrastructures are - on principle - faced with the challenge to identify risks in the scope of the introduction of information security management systems (ISMS) or a possible certification acc. to ISO 27019 [9], these risks must be minimised, last but not least, as economically as possible

[2]Remote Authentication Dial-In User Service (RADIUS) is a standardized protocol (RFC 2865, 2866) used for remote authentication, authorization and accounting.

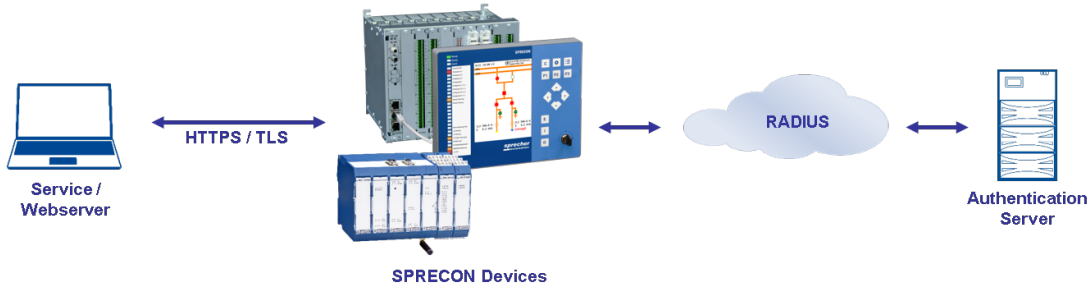

Fig. 2. Concept of remote authentication and authorization for device configuration and maintenance.

by appropriate measures. To this effect, manufacturers are required to offer comprehensive technologies, thus reacting flexibly to the application scenarios of the devices concerned. Here, security technologies must be offered as comprehensive modular systems in order to permit project-specific securing and risk minimization in protection and control systems.

In this context, the Defence-In-Depth principle is an essential concept. As illustrated in the article, polymorphic security technologies must merge consistently at several levels in a multi-level system in order to provide overall protection.

Products have been developed in order to offer such technologies systematically on all hierarchical system levels [5, 6]. Thus, complete integration of the technologies has been demonstrated by the example of an integrated firewall, which results in cost-efficient and secure project implementation that paves the way towards IT-secure energy generation, distribution and transmission.

REFERENCES

[1] *Draft of a Cybersecurity Act (IT security act)*. Federal Gazette 2015, Part I No. 31, published in Bonn on 24 July 2015., IEC TR 61850-90-1, Mar. 2010.
[2] *NIS Network and Information Security Directive*. https://ec.europa.eu/digital-single-market/en/cybersecurity. Retrieved 2016-11-08. IEEE Std 1588-2008, Jul. 2008.
[3] Bundesverband der Energie- und Wasserwirtschaft e. V. (BDEW): *Whitepaper - Requirements for secure control and telecommunications systems*. Revised version 1.1, March 2015, www.bdew.de.
[4] International Electrotechnical Commission: *IEC 62351 - Power systems management and associated information exchange Data and communications security*.
[5] SPRECON Protection & Control Products, https://www.sprecher-automation.com/en/products/. Retrieved 2016-11-08.
[6] IT Security in Power Grids, https://www.sprecher-automation.com/en/it-security/. Retrieved 2016-11-08.
[7] *Security-Enhanced Linux - NSA/CSS*, https://www.nsa.gov/what-we-do/research/selinux/. National Security Agency. 2009-01-15. Retrieved 2016-11-08.
[8] European Union Agency for Network and Information Security (ENISA): *Algorithms, key size and parameters report*. https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014. Retrieved 2016-11-08.
[9] ISO 27000-series. *ISO 27001 Information Security Management*. International Electrotechnical Commission (IEC), 2013.