IT NETWORK SECURITY FOR CONTROL AND COMMUNICATION SYSTEMS IN THE POWER INDUSTRY

Torsten RÖSSEL
Innominate Security Technologies AG, a Phoenix Contact Company – Germany
troessel@innominate.com

ABSTRACT

Designing, implementing, running, and managing control and communication systems to state-of-the-art security standards is a major challenge to both power system integrators and operators, even more so in multi-vendor environments. In this paper, we discuss how industrially ruggedized network security appliances can provide building blocks and contribute to security solutions in both retrofit and new construction situations. Based on a set of security functions as, e.g., provided by the mGuard® security technology from Innominate and requirements from a representative industry white paper, we illustrate the role of firewalls, virtual private networks (VPNs), integrity monitoring, and related functions in bringing an adequate level of IT network security to control and communication systems.

INTRODUCTION

Critical infrastructure protection is on the agenda of governments worldwide. The electric utilities sector runs one of those most critical infrastructures. Its availability depends on functional information and communication technology. Therefore, governments are appealing to power industry organizations to create and adhere to stringent voluntary guidelines for the IT and network security of their systems or even enforcing such security standards by legal regulation. In North America, cyber security regulation for the electricity sector is fairly advanced with the NERC CIP standards [1] and severe penalties for non-compliance to these standards being in place since 2006. Comparable legal enforcement of cyber security is not currently found in Europe where governments seem to rely on coordinated voluntary industry action for the time being.

THE BDEW WHITE PAPER

As a national example from Europe and in synch with the critical infrastructure protection (CIP) strategy [2] and planning [3] of the German government, the Federal Association of Energy and Water Industries (BDEW) has issued a white paper on requirements for secure control and telecommunication systems [4]. The paper defines basic security requirements and measures for IT-based control, automation, and telecommunication systems operated in the process environment of a utility. It is supposed to be included with future tenders for the design of new or retrofitting of existing control and communication systems in the power industry. Its target audience comprises system designers, vendors, integrators, and operators as well as maintenance service providers and suppliers of subsystems or components to such systems. Among others, the BDEW working group demands essential security measures in areas such as secure system architecture, general system hardening, patching and patch management, anti-virus protection, secure network design and communication standards, as well as secure remote access and maintenance processes.

INDUSTRIAL SECURITY APPLIANCES

Security appliances, more recently also referred to as unified threat management or UTM appliances, are a long known design concept from classical IT network security, bundling a set of security functions into a single, self-contained computer device. Office IT products in this category, however, are typically not appropriate for industrial use due to a variety of physical, functional, organizational, and structural reasons and divergent requirements in the industrial network environment beyond the apparently much higher risks at stake.

Industrial security solutions have to sustain the 10 to 20+ year life cycles of the systems they protect under tough environmental conditions with appropriate mounting and form factors. Their functionality should focus on industrial applications and protocols and not be overburdened with, e.g., spam and anti-virus filtering for e-mail traffic and other functions useless in non-office environments. They need to be operable under a still common lack of on-premises IT security expertise and cater for the typical reluctance to change a running process control system as well as the sensitivity to any downtimes caused by software or configuration updates. They have to live in a world characterized by very heterogeneous hardware, software, and older operating systems often considered outdated in business IT. And finally, industrial networks do typically have tree- and line-shaped topologies instead of the prevalent star-shaped topologies of office networks that many more centralized standard IT security concepts rely on.

Therefore, specific industry-compatible security appliances designed to these divergent requirements are nowadays available to the market from a number of vendors specializing in industrial network and security technologies.

Important functionalities of such devices include:

- Routing and network address translation (NAT) capabilities such as masquerading and 1:1 network mapping for network segmentation;
- Firewalls for control and filtering of incoming and outgoing network traffic according to a custom defined rule set; contemporary firewalls include protection against IP address spoofing and denial-of-service (DoS) attacks and are based on the stateful packet inspection (SPI) principle, using a technique known as connection tracking to allow for much more precise traffic control with a more compact rule set when compared to outdated plain packet filters;
- Virtual Private Networks (VPNs) allowing for secure communication across otherwise insecure, untrusted networks such as the Internet; VPNs use advanced encryption techniques to assure the authentication of the communicating parties as well as the integrity and confidentiality of the data communicated between them;
- Quality of Service (QoS) for bandwidth and traffic priority management under throughput limitations;
- System integrity assurance techniques detecting, e.g., unexpected manipulations by malware and protecting from their consequences;
- Support for redundancy and high availability scenarios protecting against device or path failures;
- Transparent modes of operation (typically called "stealth" or "bridge" modes) enabling a retrofit to existing networks without routing segmentation while still supporting all of the above functions;
- Secure device management interfaces and scalable solutions for the roll-out and remote, centralized management of large sets of distributed security appliances.

Autonomous industrial security appliances with their own dedicated hardware resources have a number of distinct advantages when compared with the direct (software) integration of security functions with the control and communication systems themselves. Security appliances do not compete with their protected systems for computational resources such as memory or processor time. In contrast, a software firewall on a controller or human machine interface can easily make a system even more susceptible to denial of service attacks consuming the majority of CPU resources and grinding the actual SCADA process to a halt. As they do not interfere with the systems they protect, security appliances can be added or retrofitted without impact on the functionality and performance of the production system. Having a minimal operating system of their own, they are much easier to harden against attacks and vulnerabilities, independent from any control system software. As an interesting aspect, this also allows to decouple the update cycles for the control system software (long, few, if any) from those of the security appliance firmware (shorter, more frequent, to keep the security up-to-date). In total, security appliances allow to implement the best practice network security strategy of a defence-in-depth with distributed protection of critical assets, independent of the network topology.

The mGuard® Technology

The mGuard technology portfolio has been developed by Innominate to provide specialized network and remote services security solutions for industrial environments [5]. It is a leading real-world implementation of the above concept, available through a variety of OEM and channel distribution partners, and comprises the following four major elements:

(1) A family of devices in ruggedized, industry-compatible form factors, called mGuard network security appliances;
(2) The embedded mGuard firmware [6], providing all the important network and security functions listed above;
(3) Device management software scaled for the efficient configuration and administration of large sets of mGuard devices;
(4) The mGuard Remote Services Portal as an efficient way for vendors and asset owning operators to organize for the secure remote access and maintenance to industrial equipment.

The primary question answered in this paper by matching this technology with the BDEW requirements is: How can industrial network security appliances contribute to fulfilling the security requirements for the overall system? Substantial contributions and solution building blocks are described in the following.

IMPLEMENTATION OF BDEW SECURITY REQUIREMENTS

General Requirements and Base System Hardening

Secure System Architecture

Distributed network security appliances lend themselves perfectly to implement the required principles of secure system design. They support the defence-in-depth principle in any appropriate granularity. Firewall rule sets typically blocking any connection that is not explicitly allowed are a nice implementation of the minimal-privileges and need-to-know principles. In addition, advanced products also support the redundancy principle for high availability solutions. Denial of service (DoS) protection and quality of service (QoS) functions are effective shields against DoS and network resource consumption attacks.

Patching and Patch Management

Patching and patch management capabilities are often found in security requirement catalogues. In reality, however, most industrial control systems have to be considered as non-patchable systems for a variety of reasons. Due to their long life cycles, security updates may not be available anymore for all components. Even if they were, there are strong

concerns that those updates might damage system stability, and the cost of sufficient testing to allay those concerns is too high. Network security appliances can be used to protect such non-patchable system components against potential exploits of their unpatched vulnerabilities. With such an alternative measure of basic system hardening in place, the BDEW white paper considers exceptions from patching as acceptable.

Encryption of Sensitive Data / Cryptographic Standards
Encrypted transmission of sensitive, confidential data between subsystems which do not support cryptographic protection by themselves can be achieved through VPN connections (virtual private network "tunnels") between two security appliances at the communication endpoints. The well-proven open Internet standard IPsec (Internet Protocol security architecture) and hardware-accelerated standard algorithms such as 3DES or AES-256 encryption and MD5 or SHA-1/2 signatures can provide state-of-the-art crypto security. Authentication should be performed by X.509v3 certificates with RSA key pairs and full support for public key infrastructures (PKIs).

Integrity Checking and Anti-Malware Protection
Another general requirement asks for the possibility to verify the integrity of system and application files and executables, for example through the use of check sums. The mGuard Integrity Monitoring method for example provides exactly such a solution, in particular for program and system files on Common Internet File Systems (CIFS) as used, e.g., by Microsoft Windows and other operating systems. This method also provides an excellent, industry compatible alternative to conventional anti-malware protection. As with patching, conventional antivirus scanning software turns out to be inappropriate for use on most industrial PCs. Typical problems include limited CPU and RAM resources, uncertain real-time behaviour, and the permanent need for updates to the virus patterns or malware signatures and scan engines. Plus, there may not even exist any known signatures for the most critical malware.

The Stuxnet Worm Revisited
In retrospect for example, analysis of the now widely known Stuxnet worm [7] has shown that this malware had been out in the wild unnoticed for at least 12 months before its discovery in June 2010 and had not been detected by antivirus programs during that period. Therefore, alternative techniques of integrity assurance such as the integrity monitoring method above are gaining relevance and acceptance for the protection of industrial systems. When initialized, it computes a baseline of signatures for all monitored objects and then periodically checks them for any deviations. This process works without any external provision of malware signatures, without the risk of disrupting operations through "false positives", without installation of software, and with moderate load on the monitored PCs, by utilizing the processing resources of a security appliance. In this way, suspect modifications are reliably discovered and promptly reported via SNMP and E-mail to network management systems or responsible administrators. As for the Stuxnet example again, vendor-independent tests have been able to verify that mGuard Integrity Monitoring would have recognized infections with Stuxnet on day zero. It would have unveiled the unexpected manipulations by the worm and warned asset operators about them long before any commercial antivirus product. Both the device drivers installed by Stuxnet as well as the modifications performed by the worm on the pivotal SIMATIC Manager DLL were discovered in the process.

Network & Communication Requirements

Secure Network Design and Communication
The requirements expressed by BDEW on secure network design exactly correspond one-to-one to the motives and defence-in-depth philosophy underlying the industrial security appliance concept. The security routers allow for a distributed deployment as firewalls and VPN gateways to achieve both the vertical and horizontal segmentation of networks into zones with filtering of communication protocols between those zones. They also support flexible, centrally controlled rollout and administration processes.

The authentication, integrity, and confidentiality (encryption) of communication can be ensured through IPsec VPN connections, in particular for all kinds of remote access. Subsystems can be flexibly integrated with the overall network concept of the utility through routers with NAT and 1:1 NAT network address translation functions. IP routing and VPNs are provided for wide area network (WAN) connections. And an effective firewall performs stateful packet inspection of IP connections (OSI layer 3) as well as Ethernet filtering mechanisms (OSI layer 2) including VLAN support.
Appropriate product portfolios provide hardened network devices with administration and monitoring via secure protocols (HTTPS, SSH, and SNMPv3) and ACL-protected management interfaces (Access Control Lists) as requested. They also support centralized device management and the integration with SNMP-based network management systems.

Secure Maintenance Processes and Remote Access
The requirements described in this section of the BDEW whitepaper represent essential aspects of remote maintenance solutions with security appliances in use today. Asset operators demand to always stay in control of potential remote access connections. Advanced security appliances provide that control via both hardware and software interfaces for the activation, supervision, and deactivation of VPN connections. Remote access can be restricted to defined target systems and remote service technicians can be virtually locked into those target systems to provide their service in a sort of quarantine situation

thanks to a combination of VPN and firewall functionalities. On site, for local connections of maintenance contractors' hardware to the process network, the security appliances can be used to enforce a restricted access to necessary connections and target systems only.

Demilitarized Zone (DMZ) structures and the necessary isolation of the process network can both be implemented with industrial firewalls. As part of the concept, secure remote access is generally provided through VPN gateways instead of a deprecated direct dial-in to endpoint devices. Strong 2-factor authentication of remote service staff, e.g., requiring possession of a device and knowledge of a pass code, is feasible. Thanks to these technical and conceptual ingredients, mGuard-based remote services solutions have been field-proven and are in daily use with many customers from the machine building and plant engineering industries.

SUMMARY AND CONCLUSION

Industry compatible network security appliances with appropriate firmware and management capabilities can provide significant contributions to security solutions for utilities in both retrofit and new construction situations. In particular in the areas of general system hardening, networking, and communication they can help integrators to implement many of the typical security requirements for control and communication systems in the power industry as compiled, e.g., by the BDEW working group. While even more advanced security technologies such as application whitelisting or intrusion prevention may become available in forthcoming generations of process automation equipment, all of the methods presented in this paper lend themselves perfectly for retrofitting into existing installations today.

REFERENCES

[1] North American Electric Reliability Corporation (NERC), 2006-2011, *Critical Infrastructure Protection Cyber Security Standards (NERC CIP-001 - CIP-009)*, Princeton, NJ, USA (available from http://www.nerc.com/page.php?cid=2%7C20).

[2] Federal Ministry of the Interior, 2009, *National Strategy for Critical Infrastructure Protection (CIP Strategy)*, Federal Republic of Germany, Berlin, Germany (available from http://www.bmi.bund.de).

[3] Federal Ministry of the Interior, 2009, *CIP Implementation Plan of the National Plan for Information Infrastructure Protection*, Federal Republic of Germany, Berlin, Germany (available from http://www.bmi.bund.de).

[4] B. Becker, H.-W. Benke, I. Jensen, R. Kasper, et al., 2008, *White Paper Requirements for Secure Control and Telecommunication Systems*, BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., Berlin, Germany (available from http://www.bdew.de).

[5] T. Rössel, 2007, "Applications and Efficient Management of Industrial Network Security Appliances", *Proceedings of the SPS/IPC/DRIVES 2007*, VDE Verlag, 269-278 (in German).

[6] T. Rössel, 2009, *Innominate mGuard Firmware – Major Release 7: The Embedded Secure Linux System for all mGuard Appliances*, Innominate Security Technologies AG, Berlin, Germany (available from http://www.innominate.com).

[7] N. Falliere, L. O Murchu, E. Chien, 2010, *W32.Stuxnet Dossier Version 1.3 (November 2010)*, Symantec Corporation, Cupertino, CA, USA (available from http://www.symantec.com/stuxnet).