HOW CAN CYBERSECURITY BE ENHANCED IN EXISTING SUBSTATIONS MINIMIZING IMPACT ON THE AUTOMATION AND CONTROL SYSTEM

Jérôme ARNAUD
Alstom Grid – France
jerome.arnaud@alstom.com

Jean-Michel REY
Alstom Grid – France
jean-michel.rey@alstom.com

ABSTRACT

Most of existing substations were commissioned in a time when the only communication link was a private telecontrol bus. Since then, DSO and utilities practices have evolved and require more connectivity to the substation. These new practices and the increasing threat of malware have raised cyber security awareness.
Even though a protection and automation control system is becoming more and more an IT system, it has its specific constraints (high availability, highly distributed, weak connectivity and a long lifecycle) and must be treated accordingly.
The authors have collected technical security practices from the IT world and selected those that can be applied to a commissioned substation and require no change to the substation automation core software.
While implementation of these techniques will not lead to full compliance to cyber security standards (such as NERC CIP) or recommendations (such as NISTIR 7628), the substation "attack surface" will be greatly reduced for a low cost.

INTRODUCTION

Security cannot be achieved at 100%, but can be it improved to an acceptable level.
Security strategies are numerous and cannot be reduced to what is covered in this paper. For example, this paper ignores internal processes and personnel training, which are essential to security. Also, in a typical 4 track Prevention-Detection-Response-Recovery) [5], this paper only addresses part of the Prevention.
The solutions proposed in this paper contribute to a low cost and easy to implement defence in-depth strategy but are by no mean an ultimate finite list of actions.

EVOLVING PRACTICES

The only communication link to a substation used to be the telecontrol bus. In an effort to improve network operation and reduce cost at the same time, DSO's set up a second communication link used to download disturbance recording files, upload relay settings [6][7].
Once this remote access is established, it opens a whole new world of possibilities: supervision, asset management, troubleshooting [8]… but it also opens new doors for attacks.

EVOLVING THREATS

In the past, virus and worms goals ranged from simply destroying their host to transforming their host into a spam or a DoS attack bot. But in the last few years, new stealth malware appeared that were specifically targeted at Industrial Control Systems, such as Stuxnet[1] [2] or Flame, making the menace more real.
Consequently DSOs, utilities and vendors now face the burden of securing the substation, from a cyber-security angle. Over the years, regulations such as NERC CIP, standards bodies such as IEEE [3] and IEC [4] and working groups [5] have published requirements, standards and recommendations to achieve better security.
All emphasize the concepts of AAA (Authentication, Authorization, and Auditability) and AIC (Availability, Integrity, Confidentiality, in that order of priority).

Many of these recommendations assume that the substation automation system was designed to support the security features, which is often not the case. Once in operation, modification of the substation automation system is a complex and costly process.

After listing some constraints specific to the substation, this paper explores 5 methods to dramatically increase the substation cyber security without having to change the substation automation core software.

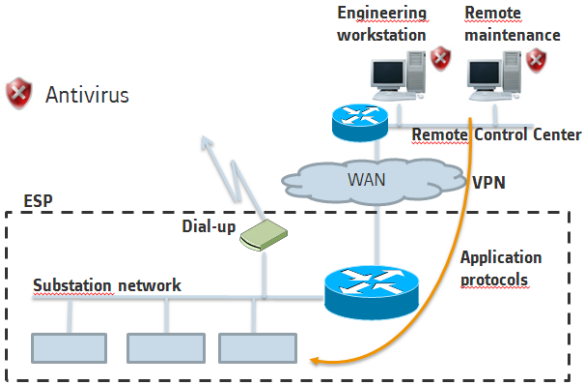

Figure 1: Current situation

SUBSTATION CONSTRAINTS

While we can consider a substation automation system as an IT system, it has its specific constraints:

- Availability is critical and must not be jeopardized by cyber security solutions;
- The automation system is deployed in hundreds of unmanned locations, impacting deployment process;
- Typical lifetime of a substation automation system is 12-15 years, while third party software vendors may support their software for a shorter period of time;
- Usually, after a system is commissioned, it is "frozen". Any change requires a lengthy qualification process.
- Vendors product development cycles and product qualification by DSOs are much slower than threat evolution;
- IT infrastructure is usually weak: there are no centralized patch deployment process, the network speed to the control center is low;

All these constraints make software updates a long and costly process.

SOLUTION REQUIREMENTS

The chosen solutions must restrict remote access to the substation to authorized users and deny malware propagation, without changing the substation automation system software and minimizing the management overhead.

OPERATING SYSTEM HARDENING

The first step in securing the system is operating system hardening.
Operating system hardening is the process of securing an operating system by reducing its surface of vulnerability.
A few examples of hardening operations include:

- Removing unused software and components
- Disabling unused user accounts
- Disabling USB ports
- Disabling unused services and daemons
- Applying the latest software patches
- Executing processes with the least amount of privileges
- Setting file permissions
- Configuring account, password and audit policies

Many organizations have created their hardening guide and made them publicly available: NSA [9], Center for Internet Security [10], DISA [11], NIST [12]. Some have released tools, checklists and templates to automate hardening.
Hardening is highly dependent on the system usage. Hence, any guide or tool need be tailored to the specific system it targets.

Hardening improves security by reducing the number of possibilities an attacker (a person or a process) has to disrupt or take control of the operating system on which the automation software is installed.

MALWARE PREVENTION: WHITELIST AND MEMORY PROTECTION

After the operating system is hardened, one can start adding security layers on top of it. The second step (or second security layer) is to protect the system from malware. Traditionally, antiviruses are used.
Antivirus software relies on a list of malware signatures to prevent malware execution (a "blacklist"). However, AV software has drawbacks:

1- The list of malware must be updated whenever new malware is discovered;
2- The update could break the system by detecting a false positive (i.e. identifying a legitimate software component as a malware);
3- Resource usage is significant (memory, CPU)

On the other hand, application whitelisting software relies on a list of authorized executable files (a whitelist). This approach is particularly adapted to the substation automation system where the system being stable, the whitelist seldom changes.
The result is that malware, which are processes, cannot execute on the protected system.

To be efficient, the application whitelisting software must:

1- Keep and protect a list of authorized executable files;
2- Prevent authorized executable file modification
3- Check executable file integrity before execution;
4- Provide a secure way to install new legitimate software (or software updates), other than by being temporarily disabled (which leaves an open window for malwares), for instance by authenticating install packages (dynamic whitelisting).

An application whitelist is using resources during the starting phase of a process only, whereas an antivirus is constantly scanning disks and memory. Hence the former has lower impact on the system resources.

However, malware is not just propagated through executable files. An attacker can exploit a buffer overflow vulnerability and dump code directly into memory, in which case the whitelist is ineffective.
To fill this hole, some vendors have associated a memory protection feature to protect against buffer overflow exploits and 0-day vulnerabilities.

The addition of all these features creates additional benefits:

1- The executable file integrity check guarantees that the file was not tampered with since installation;
2- The dynamic whitelisting together with installation package authentication guarantees the package integrity.

3- Software patch updates can be limited, reducing the deployment overhead.

Application whitelisting and control should also be installed on the control center engineering workstation to prevent the deployment of compromised configuration files and settings.

Whitelisting and memory protection together make a replacement for antivirus software, along with additional benefits.

FILE INTEGRITY CONTROL

To further increase the system security, configuration and settings files must be secured.

While application whitelisting focuses on executable files, file integrity control monitors, alerts and/or prevents all file changes.

The amount of data reported by a file integrity tool can be overwhelming so the authors have chosen to narrow file integrity control to a manageable scope: the protection of the automation system configuration files and settings.
The integrity control software should be set up to prevent automation system configuration and settings files modification except by an authorized process.
This guarantees that the only way new configuration files and settings can be deployed is by the expected process.

The installation of application whitelisting and control on both the substation system and the remote engineering workstation on the one hand, and the installation of file integrity control on the substation system on the other hand are an efficient protection against malware such as Stuxnet.

JUMP BOX

In a simple setup, the remote operator establishes a connection with the substation, usually using a VPN (either a site-to-site VPN or a remote SSL VPN) or a dialup access. In such a setup, once the connection is established, the remote operator workstation has access to the full substation network. So has any malware circulating on the corporate network or operator workstation.
A jump box is a computer, installed in the substation DMZ which has access to the substation network. The remote operator first logs into the jump box, then logs into other system components from there.

This is a better setup because:

- The jump box is not involved in the substation operation, so it can be protected by all kinds of hardening scripts, intrusive security software and automatic updates. It doesn't matter if a patch or antivirus signature update breaks the box;
- The only open communication port between the remote user and the substation is the remote desktop application port (plus a file transfer port, more on that later); this make the firewall configuration much easier and limit the doors open to an attack;
- The jump box is in a DMZ, so its traffic to the substation network can be tightly controlled by the firewall;
- Without a jump box, software programs necessary to work on the substation have to be installed and protected against malwares on all remote operator workstations. However, such software only needs to be installed on the jump box;
- The jump box is an opportunity to increase the activity audit trail as there is a single access point.
- The jump box should be the only box with an enabled USB port if removable storage is needed for local maintenance.

One weak point of a remote desktop application that must be mitigated is the "remote shared folder" feature which makes the substation system file system available to the remote machine, opening a door to malware. This feature must be disabled.
The main usage of a remote access being event log, disturbance recording files or setting files download, a secure file transfer service, such as SFTP, must be setup over the communication link to replace the remote shared folder feature.
The jump box is a solution to NERC CIP005-5 R2.1 which requires the use of "an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset" [13].

ACCESS POINT

The NERC CIP defines the notion of an Electronic Security Perimeter and of an Access Point to the ESP.
For the sake of simplification, we consider the Electronic Security Perimeter surrounding the whole substation automation system.
There should always be a single redundant access point, to protect substation access.
The access point can be:

- a modem in a dial up configuration;
- an Ethernet router/firewall if the transport layer is a private infrastructure;
- an Ethernet VPN capable router/firewall if the transport layer is a public infrastructure.

Modems should be configured with a callback feature: when contacted to establish a connection, the modem hangs up and calls back a preconfigured phone number. This limits the number of source connection points to a finite list. The modem should be connected either to a firewall (preferred) or the jump box.

The router/firewall is mandatory to separate the substation IP network from the rest of the world. It can be further enhanced with Intrusion Detection and Intrusion Prevention System at the expense of a significant increase in the required management overhead as IDS/IPS relies on signature updates.

The firewall can also act as an authentication and authorization proxy for all users trying to access the ESP. It can log authentication attempts to increase the audit trail. The authorization proxy can be used to restrict access to the file transfer protocol or the remote desktop protocol to the jump box.
The authentication and authorization service can either:

- use a users' account list stored in the firewall.
- query a central authentication service.

The former solution has a higher management overhead (user accounts have to be managed on each firewall) while the latter requires more complex infrastructure (central authentication services on the remote network).

CONCLUSION

In this paper, the authors have listed five methods to enhance the substation IP network security without changing the substation automation core software.

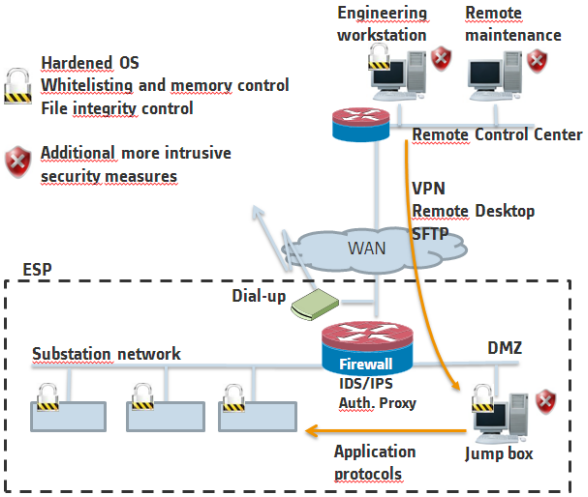

Figure 2: solution overview

The access point protects the substation access and restricts communication to the jump box only on specific protocols (remote desktop and secure file transfer protocol).
The jump box is a secure box which is used to access the critical elements of the operational network.
The critical elements are protected against exploits with hardening, whitelisting, memory protection and file integrity.
In addition, the engineering workstations are hardened and configured with file integrity to prevent compromised configuration and setting files to be deployed in the substation.

These technical solutions significantly increase substation cyber-security and can be implemented at reasonable cost in a reasonable timeframe.
They must be considered only as one of many necessary steps towards increased security.

REFERENCES

[1] Symantec, 2011, "W32.Duqu, The precursor to the next Stuxnet", http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

[2] N. Failliere, L. O. Murchu, E. Chien, 2011, "W32.Stuxnet Dossier v1.4", Symantec, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[3] IEEE, 2007, "IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities".

[4] IEC, 2007, "IEC/TS 62351 - Power systems management and associated information exchange – Data and communications security".

[5] SGIP, 2010, "NISTIR 7628 - Guidelines for Smart Grid Cyber Security", http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628.

[6] K.P. Brand, M. Herzig, W. Wimmer, 2012, "Remote Access to Substations: State, Possibilities, Challenges", CIGRE 2012, B5-211.

[7] K. Kuroi, H. Oshida, C. Komatsu, Y. Kawasaki, M. Toi, H. Nakatani, 2012, "Applications and developments for the remote access to protection relays", CIGRE 2012, B5-210

[8] D. Espinosa, C. Melendez, M.Manriquez, 2012, "PRESENT AND FUTURE FOR REMOTE ACCESS SOLUTIONS TO IEDs", CIGRE 2012, B5-209

[9] National Security Agency, USA, Security Configuration Guides, http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

[10] Center For Internet Security, Benchmarks, http://benchmarks.cisecurity.org

[11] Defense Information Systems Agency, DoD, USA, Security Technical Implementation Guides, http://iase.disa.mil/stigs/index.html

[12] S.D. Quinn, M. Souppaya, M. Cook, K. Scarfone, 2011, "Special Publication 800-70 Revision 2, National Checklist Program for IT Products—Guidelines for Checklist Users and Developers", http://csrc.nist.gov/publications/PubsNISTIRs.html

[13] NERC CIP005-5, 2012, "Cyber Security - Electronic Security Perimeter(s) ", http://www.nerc.com/files/CIP-005-5.pdf