Shielding the substation against cyber-attacks

A joint development effort helps ward off cyber threats to substation control systems

09/30/2014 - 11.03 am

CLIMATE CHANGE GRID SUSTAINABILITY
NETWORK MANAGEMENT OPEN INNOVATION

As substations become increasingly digital and huge quantities of data are transmitted in real time, utilities are becoming vulnerable to cyber-attack. Consequently, up-to-date cybersecurity defences are crucial to the health and reliability of the digital substation.

Post a comment

[Source: GETTY/ThinkStock]

Most of today's substations were commissioned at a time when the only communications link was a private control line using proprietary protocols. Since then, technology has moved on. So, in tandem, have the needs of transmission and distribution system operators for increased connectivity to the substation. "In an effort to improve network operation and, at the same time, reduce costs, utilities set up a second communication link used to download disturbance-recording files and upload relay settings," explains Jérôme Arnaud, Upstream Marketing Engineer at Alstom Grid. "Once this remote access is established, it opens a whole new world of possibilities: supervision, asset management, troubleshooting, etc. But it also opens the doors to attack."

Threats to control systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, malicious intruders, accidents, natural disasters, and so on. In the past, the purpose

of viruses and worms ranged from simply destroying their host to transforming it into a spam or a DoS attack "bot"[1]. "However, new stealth malware like Stuxnet[2] or Flame has appeared, specifically targeting industrial control systems and making the menace more real," points out Arnaud. "Consequently, utilities and vendors now face the burden of securing the substation from a cybersecurity angle."

Over the years, numerous regulations, standards and recommendations have been published to aim for better security. Many of them assume that the substation automation system is designed to support the security features. That is often not the case. Furthermore, once in operation, modifying the substation automation system is a complex and costly process. While a substation's protection and automation control system looks increasingly like an IT system, it nonetheless has its specific constraints. These include mandatory high availability, a highly distributed system, weak connectivity and a long life cycle. These have to be treated specifically, and that is exactly what the enhanced cybersecurity of the new 5.1 version of the DS Agile substation control system does.

[1]A bot is a software application that runs automated repetitive tasks over the Internet. The largest use of legitimate bots is in web spidering to index content.

[2]The Stuxnet worm reportedly ruined almost one-fifth of Iran's nuclear enrichment centrifuges in 2009-2010.

1 Providing defence in depth

"The chosen solutions must therefore restrict remote access to the substation to authorised users and deny malware propagation without changing the substation automation software while, at the same time, minimising the management overhead. This can be done with a series of security layers that combine into a 'defence-in-depth' strategy," says Arnaud. "This layered arsenal is

capable of withstanding or minimising the impact of a failure in any one layer," he adds.

The first step in cyber-securing is to harden the operating system by reducing its surface of vulnerability. This means removing unused software and components, disabling USB ports and unused user accounts and services, applying the latest software patches, executing processes with the least amount of privileges, and so on. Hardening improves security by lessening the number of possibilities an attacker (whether a person or a process) has to disrupt or to take control of the operating system on which the automation software is installed.

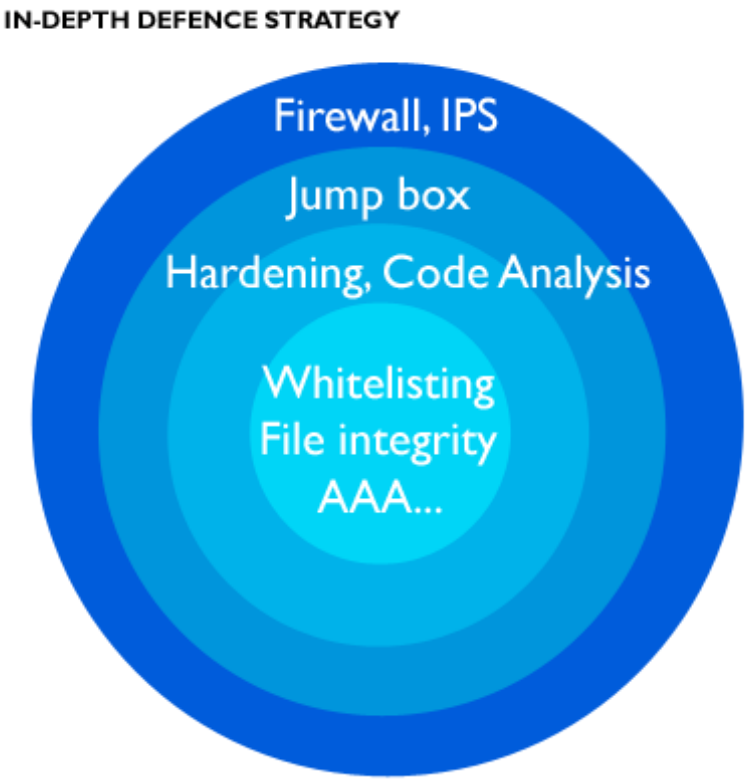
2__Malware prevention: whitelisting and memory protection

After hardening the operating system, security layers can be added on top. The second step (or second security layer) is to protect the system from malware. Traditionally, antiviruses are used. They rely on a "blacklist" of malware signatures to prevent malware execution. However, they have drawbacks: the blacklist must be updated whenever new malware is discovered, and this update may break the system by triggering a "false positive", i.e. identifying a legitimate software component as malware. "A more appropriate approach is whitelisting. This relies on a list of authorised executable files (the whitelist). This kind of software is particularly well adapted to a substation automation system because, since the system is stable, the whitelist seldom

changes," says Arnaud. The result is that malware processes cannot execute on the protected system. Also, whereas an antivirus is constantly scanning disks and memory, a whitelisting technology uses resources only during the starting phase of a process, and so consumes negligible system resources during runtime.

However, malware may propagate not just through executable files – an attacker can exploit buffer overflow vulnerability and dump code directly into the memory, in which case the whitelist is ineffective. To fill this hole, memory protection features are added to protect against buffer overflow and "0-day" (i.e. not-yet-discovered) vulnerabilities.

DS Agile 5.1 has integrated whitelisting technology specially designed by McAfee, the McAfee Embedded Control Solution (see sidebar). "Another far-reaching innovation with DS Agile 5.1 is that this solution is also installed on the control centre engineering workstation to prevent deployment of compromised configuration files and settings." Whitelisting and memory protection together deliver significant advantages that antivirus software cannot offer.



3 __ File integrity control

To further improve system security, configuration and settings files have also been secured. “While application whitelisting focuses on executable files, file integrity controls monitors, alerts and/or prevents all file changes,” explains Arnaud. “The integrity control software is set up to prevent any automation system configuration and settings files from being modified except by an authorised process. This guarantees that the only way new configuration files and settings can be deployed is by the expected process.” Installing McAfee Embedded Control on both the substation system and the remote engineering workstation combined with the installation of file integrity control on the substation system represent efficient protection against malware such as Stuxnet.

There are several other security layers implemented in DS Agile 5.1. One is the “jump box”, a computer installed in the substation DMZ that has access to the substation network. The remote operator first logs on to the jump box, then logs on to other system components from there. “This is a better setup, notably 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,” explains Arnaud. Last but not least, DS Agile 5.1 also comes with organisational measures covering internal processes and personnel training, as well as full and reliable documentation, all of which are essential to security.

These solutions are effective today. However, since cyber threats are a constantly shifting landscape, DS Agile’s security will be continuously evolved to ward them off.

4 __ Collaborative work on cybersecurity with McAfee, part of Intel Security

Three questions to Jan Krüger, Senior Sales Systems Engineer OEM, Embedded EMEA

What expertise does Intel Security bring to cybersecurity in the T&D world?

Jan Krüger: McAfee has been delivering solutions to the critical infrastructure market for decades to build reliable computing platforms. Adding the McAfee portfolio to these platforms enables our customers worldwide to improve the reliability of substation systems – such as those developed by Alstom – as well as to secure the electricity T&D networks.

Did the implementation of McAfee's protection solution in DS Agile imply modifications to the platform?

J.K.: DS Agile has been secured with "McAfee Embedded Control", which includes our patented "Whitelisting Technology" and "Memory Protection". Our collaboration with Alstom Grid is a long-term partnership, benefitting both companies. This enabled us to adapt and refine our solution to DS Agile applications and requirements. On the other hand, we made some suggestions about how to make DS Agile communication stronger and more "intelligent". Alstom Grid's feedback was also a very useful source of information for us to improve our offerings to the T&D world.

Is there a trend towards standardised cybersecurity functionalities in the electrical industry?

J.K.: McAfee as well as Alstom Grid actively participates in standardisation working groups at European and national levels on the theme of "Cyber Security of the Smart Grids". The objective is to define the best cybersecurity standards and practices that should be implemented to secure the smart grid and make it more reliable.

RATE THIS ARTICLE

COMMENTS

SIGN UP FOR OUR NEWSLETTER

LEARN MORE

EXPERTS

Jan Krüger
Senior Sales Systems Engineer OEM, Embedded EMEA, McAfee

Jérôme Arnaud
Upstream Marketing Engineer

SEND A MESSAGE TO OUR EXPERTS