



Security in the smart grid

Security in the smart grid

It's hard to avoid news reports about the smart grid, and one of the media's favorite topics is security, cyber security in particular. It's understandable—the grid as we know it today already relies on a wide variety of digital devices and computerized controls to keep the lights on. The grid of the future will only be more “wired” (or wireless, as the case may be), and the combination of those systems with public communications infrastructure creates the potential for unauthorized access.

The question then becomes, how do we protect such a vast system from hackers, criminals, disgruntled employees and others who would do harm to the grid?

Security is primarily about people, processes and technologies working together to prevent an attack. It is not just technology, or a set of procedures, and it is not a one-time investment. There is no single solution that is effective for all organizations or applications, but effective solutions can be realized through the cooperation of vendors, systems integrators and end users.

Gauging the threat

Ultimately, security is about managing risk, but the task of defining security threats to power utility systems is a difficult one, in part because there is relatively little statistical data on security breaches. These have been (thankfully) rare as compared, for example, to natural disasters like hurricanes, ice storms and the like. Nature is also fundamentally random, and as such lends itself to statistical analysis. Cyber threats, on the other hand, are posed by human beings who are able to learn and change their methods over time. Security in this context is by nature a dynamic and ever-changing process. It is never “done.”

Security threats also do not know technical limits (i.e., there are many potential vectors of attack that might be used to circumvent security measures). This is why security experts often refer to the need to have “defense in depth,” a combination of policies, procedures and technologies that are mutually reinforcing.

Another distinction that should be made with regard to security in utility systems is the relationship between security and reliability. These two objectives are not always aligned, given the priorities behind each of them. For example, the increasing amount of data flowing out of substations back to utility control centers is highly useful for managing reliability but it presents additional challenges from a security perspective. Modern “routable” communication protocols are seen as vulnerable, and with the proliferation of intelligent electronic devices (IEDs), the utility's exposure to cyber attack seems to grow by the day.

However, a return to older “serial” protocols would not allow the bandwidth required to run advanced applications like wide-area monitoring, and would also not offer nearly as much as IP-based protocols in the way of security tools to harden utility systems. Ultimately, though, reliability and security are on the same team. If a security breach allows an intruder to disrupt the utility's operations and cause a blackout, then clearly reliability has also been compromised.

Today of course, utility systems have not only grown more extensive and more numerous, they have also forged connections between one another and with remote facilities like substations. In addition, interoperability of utility systems has emerged as a priority, as demonstrated for example by the rapid adoption of open communication standards like IEC 61850. Vendors must therefore ensure their security measures do not come at the expense of interoperability.

Meeting utility security requirements in the current environment is a multi-faceted and ever-changing challenge. From the system vendor's perspective, one of the first hurdles in addressing security lies in meeting the different and sometimes contradictory requirements of utility users, regulators and various industry working groups and standards. Requirements from these sources were developed within a certain context and with specific objectives, and are not likely to account for concerns outside of that scope. For example, NERC's CIP requirements address operators, not vendors, but system users will likely still expect vendors to support their compliance efforts.

This presents a moving target for systems vendors as they develop new product and service offerings. Defining product requirements, then, takes on an even more vital role. Similarly, security issues must constantly be revisited throughout the development process with a heavy emphasis placed on security assessments and testing.

Challenges for utilities

While system vendors are vital in their role of developing fundamentally secure products, after the sale it is primarily the job of the user, the utility, to ensure ongoing security. Ultimately, it is the utility that is accountable. For that reason, security within the modern utility organization is by necessity a complex and high-visibility function.

Utilities must assess the security of their existing systems, evaluate and plan for new costs associated with security, craft security policies and procedures, train their employees on those policies and procedures, and establish a management mechanism that ensures all of these things get done in a thorough and timely fashion.

From an organizational perspective, security is an interesting function in that power engineers are not security experts by training. Their focus is on operating the network to maximize reliability. Likewise, security professionals typically are not operations people, and their focus is on preserving the integrity and functionality of the system rather than actually using it on a day-to-day basis.

Managing security as a corporate function requires balance in order to draw on the skill sets of the user and the security professional alike. It also takes a good deal of basic vigilance in terms of monitoring the security infrastructure (e.g., regularly analyzing system log files, reevaluating threat models, updating security policies and processes), a concept we will return to later.

Improving security

For the utility, security begins with policies that address human behavior, which is the basis for all security whether technical, procedural or organizational. Relatively few security breaches can be attributed solely to a technological failure. What is far more likely is that a technological weakness will be exploited through the application of “social engineering” on the part of the intruder, or through a seemingly innocuous oversight on the part of the system operator.

Monitoring log files is an important, if unglamorous, way for utilities to keep track of the nature and frequency of attempted security breaches their systems are facing. If all goes well, the policies, systems and procedures in place will deter the garden-variety threat, but log files provide valuable information on unsuccessful attacks that may be applied to preventing more sophisticated ones.

There are many simple things that utilities already do to maintain IT system security. They may seem obvious, but the key to their successful application lies in the organization’s ability to stick with them. Some examples of such basic but vital practices include:

- Using and listening to alarms
- Removing unused software from servers and workstations
- Disabling unused services
- Removing unused accounts
- Changing default passwords regularly
- Verifying system setup on a redundant or test system, not the production server
- Using host-based firewalls
- Regularly updating antivirus software
- Using a vendor’s patch management process

This last item points to the importance of cooperation between vendors and utilities over the entire system lifecycle. It also highlights maintenance of security systems, which are as vital as the control systems they protect. The maintenance phase is by far the longest in the lifecycle of any security regimen. The vendor addresses security during product development and an integrator will handle it during installation and major upgrades, but over most of the system’s life, the “care and feeding” of security falls to the utility.

This brings us back to the organizational character of the security function. To be successful, security must be formally established within the utility and that can sometimes present a problem in terms of who “owns” security within the company. Cross-functional teams are vital because security spans the entire organization (and because similar challenges are faced in different departments), but the lines of responsibility should be well defined and a security “czar” or stand-alone department should coordinate the various activities.

Legacy systems also present a particular security challenge. In most cases, it simply is not practical to replace systems that are otherwise perfectly functional simply to apply the latest in security technology. However, depending on the age of the system in question, it’s also conceivable that the security inherent to it is not at all adequate for current requirements. Fortunately, there are several approaches that can secure legacy systems without replacing them.

One option is to encapsulate the given system within a secure zone of cyber protection so that it is isolated from direct contact with other systems, both within the utility firewall and outside it. Communication channels can also be secured by upgrading to modern protocols that support encryption, authentication and authorization mechanisms. Access to the legacy system can also be controlled by bolting on a new user interface layer along with the application of appropriate procedures for authorization.

Finally, if remote access to the legacy system is required, that can be achieved using a secure virtual private network to connect to a terminal server rather than the operation system itself. As with any system, new or old, non-essential applications should be hosted from hardware that is physically separate from the main system.

Security best practices for the vendor

While suppliers of critical utility IT systems take security seriously, it’s almost impossible to overstate the importance of having a pervasive security culture across the development process. Developers themselves should be trained in security strategies and development tools, and system vendors should build development methodologies to model the ever-changing array of potential threats. Security requirements also need to be addressed as early as possible in the development process as they may have far-reaching implications for the product.

Testing, as mentioned earlier, is also vitally important. At the device level, a formal testing methodology should be created that leverages current state-of-the-art commercial and open source testing tools in the development life cycle. Multiple approaches should be employed. Profiling tools can help to determine vulnerable services; known flaw testing can check for the latest identified threats; resource starvation testing (which looks at denial-of-service attacks) and negative testing can be used to examine departures from a protocol’s specifications and operating parameters.

At the system level, thorough preparation, strict follow-up and clarity in who will receive test results can streamline the testing process. However, this is one area where time and money will be required, and wise investments of both are likely to produce a superior end product.

The complete system delivered to a utility user should address security from several vantage points. It should be secure by design (secure architecture and code, robust threat analysis, reduction of vulnerabilities), secure by default (reduced attack “surface area”, minimum privileges used, unused features turned off by default), and secure in deployment (training and documentation for users; management of detection, defense and recovery). Finally, the vendor should strive to maintain an open communication process with users regarding security. No system is perfect, and the ease with which fixes can be applied will directly impact the overall security of the system.

Conclusion

When we look at the organizations involved in maintaining utility system security—vendors, integrators, end users—it’s fair to say that security is “everybody’s business.” To the extent these groups cooperate with one another throughout the system lifecycle, security will be enhanced. At the same time, perhaps the most important aspect of security for the various players to keep in mind is that it is a journey and not a destination. There will always be new threats. Likewise, there will be new methods and technologies for meeting those threats. Vigilance, cooperation and technical expertise, when applied in unison, offer the best defense.

Contact us

ABB Inc.
North America Corporate Headquarters
12040 Regency Parkway
Suite 200
Cary, NC 27518
www.abb.com

©ABB Inc. 2009 3BUS094984