SmartGridToday
The independent journal of the digital energy industry
MMi
Friday, June 8, 2012

EXCLUSIVE

Utilities urged to increase vigilance over meter firmware, upgrades

Utilities need to pay closer attention to firmware in smart meters to defray power theft and introduction of malicious worms into control systems, Gib Sorebo, chief cybersecurity technologist with consultancy Science Applications International Corp, told us this week in an exclusive interview. Though meter vendors have built up defenses against such intrusions, the utility is ultimately responsible for keeping systems and meters secure, he said.

Firmware is software that runs in chips and carries out instructions. Routine checks for firmware upgrades can be expensive for utilities, Sorebo said. The practice requires plenty of bandwidth, which is an expensive commodity in the communications network realm, he said. Many utilities have not developed operational processes to efficiently execute such tasks, he added.

CYBER inSECURITY
Seventh in an expanded series

Logistical costs may deter utilities from upgrading firmware if the perceived risk is low, Michael Stuber, engineering advisor in the office of the chief technology officer at Itron, told us this week in an exclusive interview. Vetting each new firmware update, paying employees to oversee downloads and occasionally rolling out trucks to force upgrades onto fussy devices all cost money in operational terms, he said.

Firmware upgrades might also occur during a period when the utility must focus all its operational capabilities on specific tasks, such as when a utility must run DR programs during peak events, he said.

QUOTABLE: Vulnerabilities are part of the world and we make risk decisions every day. I suggest you did not put on your bulletproof vest and did not get into your bulletproof car to go to work this morning.

Michael Stuber, engineering advisor in the office of the chief technology officer at Itron

Italian firm prepared

Enel centralized its Italian smart meter firmware upgrade operations when it completed its nearly 32 million meter AMI deployment, Giuseppe Michele Salaris, head of the remote management and metering system team with Enel Distribuzione, told us this week in an exclusive interview. The utility updates firmware when it wants to add functionality to the AMI system, whether through internal motivation or regulatory decree, he said.

That means the utility updates its firmware once every five years for each meter model, Salaris said. The utility uses Echelon meters along with meters from a handful of other vendors (SGT, 2010-Feb-23). The utility has a "number of protection mechanisms" to restrict unauthorized firmware downloads, he said.

QUOTABLE: Configuration management performed by Enel's automated meter management central system allows us to keep under control the firmware version installed on each meter. Any time a new firmware version is made available the system is able to detect on which meters it needs to be downloaded.

Giuseppe Michele Salaris, head of the remote management and metering system team with Enel Distribuzione

Meter vendors employed

Many utilities farm firmware updates out to the meter vendors with which they contract, for an added fee, Sorebo said. Utilities that prefer maintaining control over those updates, however, must be more dogged in their approach, he said.

"I don't doubt that the meter vendors are doing what they can in this area. However, it's ultimately up to each utility to ensure that the processes are being implemented correctly," Sorebo said.

For their part, smart meter vendors have sufficiently addressed firmware and security issues, Sorebo said.

Digital signature helps

Landis & Gyr, like Dept of Defense (DOD) and the banking and credit card industries, uses a digital signature and root of trust on all firmware commands and downloads. That means users cannot download malicious firmware, because the smart meter and other systems will refuse to accept that material.

"We believe that three key functionalities are required for security process best practices: first, firmware download integrity methods and verification; second, strong command authentication means; and finally, a clear audit capability," Heath Thompson, a VP and chief technical officer of North America with Landis & Gyr, told us this week in an exclusive interview.

Landis & Gyr's root of trust method – in which it keeps digital signatures locked away in a DOD-certified, hardware-based device – is an "ideal" defense, Sorebo said.

Some older smart meters lack this root of trust technique inside the actual devices, though vendors have also devised ways to mitigate some of the problems that would arise from this, Stuber said. That means, at least theoretically, someone with technical knowledge could manipulate the meter's firmware, he said. That would also require a counterfeit digital signature to mask that illicit activity, and that is difficult to create, he said.

But digital signatures alone are not enough to keep users from downloading firmware, Sorebo cautioned. Stuxnet was

an unauthorized firmware upgrade that used a legitimate digital signal, he noted.

Firmware upgrade no guarantee

Still, the likelihood of a full-scale cyber attack launched on a utility control system through the smart meter is limited, Stuber said. Those devices are connected to far fewer programs and software than the control systems software inside utilities, and attackers must successfully navigate a communications network security perimeter to even get into the utility nerve center, he said. That is why security and firmware upgrades are not necessarily one and the same. Stuber recommends one or two firmware upgrades each year after initial deployment, but just one every couple years after the five-year mark.

"I'm not saying that a meter is inherently more secure [than control system software]. I'm not saying that at all. But a meter is substantially simpler," Stuber said. "With this simplicity, there is less to attack and greater opportunity to get to full-scale coverage of the problem."

Hardware attacks usually occur one meter at a time, but there are known vulnerabilities in some AMI implementations from the complexity of implementing public-key infrastructure (PKI), a cryptographic mechanism that uses digital signatures to identify users on a network, Seth Bromberger, principal at NCI Security, told us this week in an exclusive interview.

Those implementation flaws are not unique to AMI, and can be exposed on control systems networks as well, Bromberger wrote in a DOE-backed white paper co-authored by Stan Pietrowicz, senior principal at Applied Communication Sciences and published in January. The "governance, protection and storage" of critical PKI material, such as private encryption and signing keys, are still "weak links" in the utility model, they said in the paper. Should an attacker ever compromise the root of trust for an AMI or control system, they said, the security protections afforded by PKI would be rendered meaningless.

Furthermore, common approaches to mitigate the risk of certificate compromise do not work well in closed environments, they wrote. Programming devices to systematically look up certificate revocation lists (CRLs), especially before any interaction with a previously unknown peer, would require constant connectivity to a CRL server, "which is not always feasible – especially in closed or low-bandwidth communications networks, such as AMI or control systems networks."

"The effect of a compromise of the manufacturer's private key or signing process can result in the attacker being able to impersonate components of the AMI system," Bromberger and Pietrowicz added.

Utilities resisting

Utilities could guard against this and other vulnerabilities if willing to pay for it, but so far the industry has resisted expensive smart meter security elements, Bromberger told us.

> **QUOTABLE:** The larger general issue is one that we haven't really figured out yet: How to secure a device that's under the physical control of an adversary without making it cost-prohibitive to deploy in the first place. There's an interesting dynamic at play with smart meter deployment between the cost per device and the device's security features. This causes tension not only between utilities and manufacturers, but in some cases between different groups within the utility itself.
>
> *Seth Bromberger, principal at NCI Security*

Power theft focus challenged

Cost has always been an issue with utilities and smart meters, and people have begun questioning whether one of the technology's main benefits – reducing power theft – is as foolproof as marketed.

A recent KrebsOnSecurity.com report of smart meter hacks at a Puerto Rico utility in 2009 showed that utility anticipated up to $400 million/year losses from power theft from smart meters. The security blog obtained a 2010 FBI report that showed the hacking may have been simple: people used either a magnet or infrared lights to hack meters and then changed the software that communicated with them, the FBI posited.

"The best solution for that is to periodically query each meter to verify its hash value and ensure that no unauthorized changes have taken place," Sorebo said of such attacks, though he was unsure of the credibility of the infrared assertion. "You can never assume that your defenses will be sufficient from something being compromised."

The incentive to steal power from smart meters and the inability to manage that at the utility level are the greatest in low-income countries or those with a high crime rate, Sorebo noted. Utilities in those nations often lack the technical and security knowhow, as well as the money, to keep firmware updated and meters strongly secured, he added.

Predictably, utilities in developing nations commonly cite cutting power theft as a significant factor for deploying smart meters. That certainly was the case, Sorebo noted, in Southern Italy, a hardscrabble region nurtured on mafia culture.

The main push for AMI in Italy was reducing costs, Salaris said.

"Localizing energy theft and fraud was a side benefit of the automated meter management system installed in Italy," he added. "In any case, fraud and theft did not impact the electricity distributed by Enel significantly."

Dozens on case

At least "several dozen researchers" in the US are looking into how people might remotely take advantage of smart meter vulnerabilities, Bromberger told us.

"If you know what you're doing and have access to some specialized equipment, you'd be able to take advantage of software flaws in the meters as well, possibly leading to something that's remotely exploitable," he added.

[Comments]