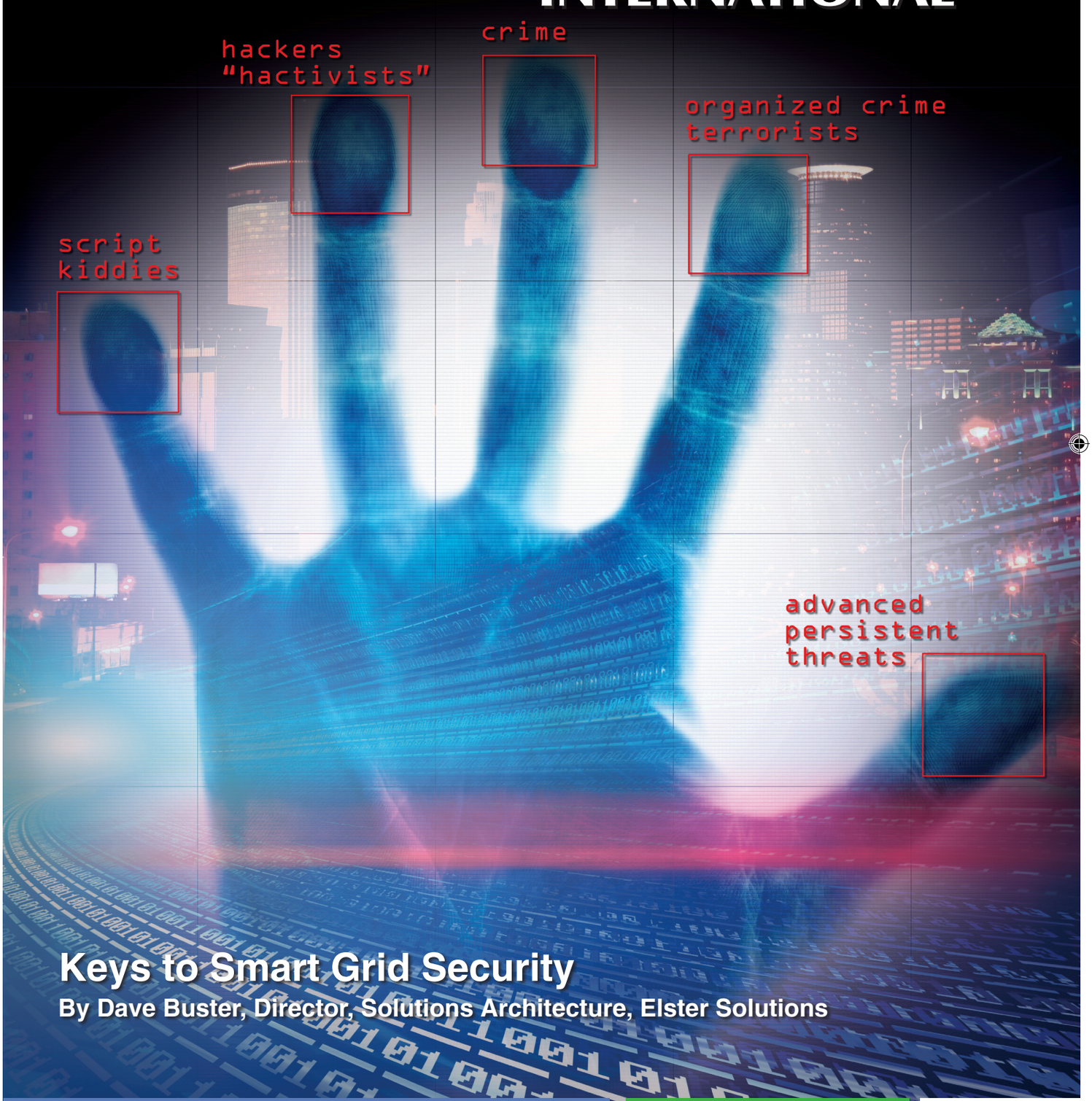
METERING INTERNATIONAL Issue 4 2012 Where business begins www.metering.com

ISSUE 4 | 2012

WHERE BUSINESS BEGINS

METERING.COM

METERING INTERNATIONAL



Keys to Smart Grid Security

By Dave Buster, Director, Solutions Architecture, Elster Solutions

Smart grid innovation • Data analytics • Empower Demand

Smart Energy International

spintelligent CLARION

KEYS TO SMART GRID SECURITY

By Dave Buster, Director, Solutions Architecture, Elster Solutions

The topic of smart grid security continues to mature in the industry, especially as the underlying technologies evolve. Utilities are becoming much more sophisticated in the approaches they take to smart grid security as new threats and new technologies continue to emerge. In addition to supporting standards and reviewing security policies, utilities are beginning to analyze smart grid threats, applying proactive solutions to the problem of technology attacks.

Outlined below are the most common threats to the smart grid and recommended solutions to help ensure proper protection and security.

SMART GRID ADVERSARIES

Script kiddies

These attackers are typically young and pursue hacking of computers and communications systems as a hobby. They are called "script kiddies" because they usually download Java scripts and other attack exploits from the internet, but lack resources and experience. Therefore, most attacks make use of free downloaded probes and code, which typically search for known exploits in common operating systems (Windows, Linux, Unix, etc.). The goal of script kiddies is notoriety with their friends, so they have little interest in attacking the system as a whole, or hiding their presence.

Solution: Elster and other prudent systems manufacturers use micro-kernels, often with proprietary extensions, and carefully check for weaknesses before employing them in a meter. From a hardware standpoint, "script kiddies" may try to steal a device to hack it, but they usually only have basic electronic tools at their disposal. Elster meters are equipped with tamper sensors, designed to alert the utility of possible physical tampering with the devices. Meters that show a pattern of power outages that do not match neighbouring meters also cue the utility to schedule a site visit or look for other evidence of theft. Finally, the hardware itself is also hardened against tampering by obfuscating communications between chips on the board.

Hackers/hactivists

More sophisticated attackers with formal training and tools, hackers and hactivists have a political motivation and are seeking notoriety. They want to attack more than one meter and they want to do it in a way that makes a successful attack evident to outsiders. Hackers and hactivists want to create controversy and try to embarrass the utility, if possible. They need to hack into a system and leave clear evidence that they were there, either by leaving "fingerprints" on a display or changing system behaviour. They attack at the meter level, but are capable of writing their own code and building more advanced probes and tools to hack into the hardware.

Solution: Smart grid vendors such as Elster employ obfuscation of information in memory, lock processors to prevent register reads and memory dumps, and avoid storing passwords in ROM. Elster stores encryption seed values in distributed memory locations (through a patented process) and Elster's software does not generate an encryption key until it is actually needed.

Crime

These attackers have a goal of financial gain. Unlike hackers, they take great care to keep their activities undetected, if possible, since some are attempting to defraud a utility by paying lower or zero rates, while others are trying to steal power for nefarious activities. With the goal of financial gain, they may try to hire experts, such as hackers with expert skills or by bribing utility employees. The typical approach is to try to use physical access to bypass a meter or tamper with it to reduce measured kilowatt-hours.

Solution: In addition to tamper alarms and meter passwords, Elster integrates theft detection systems which compare measurements from low voltage sensors on transformers to the measurements recorded by meters on the house. Any discrepancy between the power that leaves the transformer and what is measured at the residence can be investigated.

Organized crime, terrorists

Organized gangs and/or terrorists are interested in more widespread effects, with the goal of creating outages, either for financial gain (by shorting stocks) or political gain (terrorism). They are better funded and are able to outsource significant components of the attack, including writing code, testing and introducing the attack. They also have the goal of mounting an undetected attack, and are willing to spend extraordinary amounts of time, energy and money to keep the attack secret. These attackers are much more likely to use bribery, phishing, and other "carbon-based" attack modes. In addition to simple bribery

	Script Kiddies	Hackers, "Hactivists"	Crime	Organized Crime, Terrorists	Advanced Persistent Threats
Goals	Vandalism "LOLs"	Vandalism Extortion Eco-terrorism	Theft of service, fraud	Disruptions, panic (FUD), stock manipulation	Broad grid disruptions
Scope	Single-end-point	Multiple end nodes in an area	Local meters and distribution sensors	Widely separated targets	Nation-state funded, broad scale coordinated attacks
Methods and Tactics	Download code for probes and common exploits	Author zero-day exploits	Physical tampering and hacks	Outsourced multi-component attacks	Modelling of target networks with advanced testing

for passwords, they even have sufficient resources to recruit ongoing spies in an organization.

.

Solution: Because the goal is system-wide disruption, these attackers need to attack the head-end of the system. Therefore, an employee education program to mitigate phishing and bribery exploits is recommended. In addition, vendors like Elster assume handheld devices in the field may be compromised, and limit the time-to-live credentials in each device, and encrypt authentication in the field.

Advanced persistent threats (APTs)

These threats represent the highest level of attack on the smart grid. A euphemism for state-sponsored attacks, the APT is extremely well funded, persistent and sophisticated. APTs are interested in wide scale, national disruption, possibly as an economic attack or even prelude to military attack. The adversaries can infiltrate a system and then wait for years before activating an attack. In theory, an APT may actually have access to more resources to attack a smart grid target than the utility itself could possibly mount to defend it. Please note: APTs consider the smart grid as only one of several potential targets (e.g. other utilities like water, transportation, infrastructure) to meet their goals and will make an economic decision based on return on investment to attack the grid.

Solution: The utility needs only to make the attack more expensive than the benefit in order to reduce the attraction of the smart grid target. To that end, utilities can take steps to compartmentalize information from employees, as well as using a smart grid architecture that has been designed for compartmentalization itself. Elster and other vendors utilize advanced protocols carefully designed to limit interactions between devices that have no normal reason to communicate. The EnergyAxis protocol prevents Elster meters from terminating communications with each other. They can only forward messages without reading them, protecting them from unauthorized commands.

SMART GRID SECURITY APPROACHES

Given the threats outlined, protection of the smart grid seems to be a daunting task; however, there is a series of philosophical approaches that utilities and smart grid designers can use to lay out a protection plan.

Formal risk management process and policy

Similar to approaches used in other industries such as the financial industry, this includes a detailed analysis of the value of the information to be protected and the costs associated with loss and disruption. Without this necessary step, system designers can only provide anecdotal evidence about potential threats, and the business case for investment in protection is weak. However, armed with the information from a formal risk management study, a budget and timeframe for implementation, remediation becomes possible.

Trust management

Utilities should review and study the use of the latest trends in technology, since it is difficult to protect a system without indication of friend or foe. This includes identity management for humans such as user profiles and role-based access control as well as authentication for devices on the network. It should be engineered to be robust in the face of distributed attacks, with a way of distributing not only validated credentials but also revocation lists quickly and efficiently.

Physical tamper resistance

Product manufacturers should reduce the potential for meter tampering, including locking the processor, and obfuscating information in memory and on interfaces between components. This type of tamper resistance is effective against logic probes and attempts to reverse engineer or decompile software.

Ongoing employee training

It is also essential to provide ongoing employee training for security. Employees should be trained not only on standard procedures, but also a high level explanation of why some of those processes and policies exist. For example, employees need to be educated on the risks of sharing password information even with trusted co-workers. In addition, employees can learn from role play of phishing attacks and other social engineering type of exploits.

Compartmentalization

At a high level, a secure system is designed with a philosophy of protocols and system interfaces to limit information and access to the smallest possible number of local devices. Information that is not needed by a particular device is not available to that device. In the same way, compartmentalization of personnel can help safeguard against attacks. Security information including passwords, profiles, and even the architecture itself should only be distributed on a need-to-know basis.

"Standards are necessary but not sufficient to protect systems."

Intrusion detection systems (IDSs)

Modern IDSs use sophisticated heuristics to detect, isolate and remove threats. Since the threat landscape is constantly changing, it is necessary to ally with a vendor who specializes in this type of protection. Elster Solutions has partnered with industry leader Industrial Defender to provide an advanced IDS with the EnergyAxis system, which integrates an IDS agent in the server to monitor and analyze approved processes, as well as event logs and status alarms. Taken together, this system provides strong security against even APT attackers.

Finally, compliance with industry recognized security standards, policies, and processes is critical. Security standards around trust management, encryption, and policies have been carefully analyzed and validated by experts and can provide significant value and speed to deployment.

The security of smart grid networks is a vital part of protecting our shared critical infrastructure. As new technologies and threats continue to emerge, as outlined above, utilities need to ensure proper protection to defend themselves against these adversaries. Not only do utilities need to support standards and review security policies, they also need to analyze security threats and apply proactive solutions. As a leader in secure smart grid systems, Elster is taking an active role in advancing these areas. MI

ABOUT THE AUTHOR:
Dave Buster is an industry veteran with over 30 years experience is designing, building and operating communications systems in the telco world and vendor community. Recently, he joined Elster Solutions as a Customer Solutions Architect, with a special focus on security. He has a BS Engineering and MBA from North Carolina State University.
www.elster.com