Abstract
A smart grid is an electricity network that has been infused with information and digital communications technology to provide greater control, stability, reliability, and flexibility of the power grid. Technology has been added from the consumer premise which includes appliances, thermostats, home energy managers, and load control switches all the way back to the generation facilities. The combination of these technologies could potentially optimize demand management, save energy, reduce costs, increase reliability, connect alternative and home-generated energy sources to the grid (i.e., transmitting a bi-directional flow of energy), and evolve into a powerful platform for new business opportunities. In order for smart grids to achieve all objectives, cyber security and privacy concerns must be overcome.

The smart grid adds new entry points to the older technologies that are already vulnerable but were previously protected from exploit by physical isolation. Theoretical concerns have become practical realities as a number of vulnerabilities in the smart grid and power complexes have been exploited. After a general introduction to smart grids and smart grid security, this article analyzes security (control) and compliance (visibility) requirements for smart grids. In order to justify the need for security policy automation, the article focuses on the hard-to-implement least privilege, information flow enforcement, and security incident monitoring/reporting/auditing requirements. The article then presents “model-driven security policy automation” (control) and “model-driven security incident monitoring/analysis automation” (visibility) within the context of smart grids, and explains how alternative approaches such as identity and access management and authorization management are necessary but not sufficient on their own. The presented “model-driven security” policy automation solution uniquely helps solve the challenge of capturing, managing, enforcing, and monitoring/analyzing fine-grained, contextual technical authorization policies for small to large-scale smart grids.

Smart grids
Smart grids are being promoted by many governments as a way of addressing energy independence, global warming issues, emergency resilience issues, and the attempt to phase out nuclear power in several countries. A smart grid is a form of electricity network combined with...
information technology – across generation at power plants, distribution and transmission along electrical lines, and delivery and consumption at the customer homes or businesses of a utility. A smart grid transmits electricity intelligently using two-way digital communications to continuously monitor the bi-directional flow of electricity and to control a number of devices across the grid, including appliances at consumers’ homes; this could potentially optimize demand management, save energy, reduce costs, increase reliability, and connect alternative energy sources to the grid – if the risks inherent in executing massive information technology projects are mitigated.

The smart grid is envisioned to integrate today’s electrical grid with large-scale deployments of Information and Communications Technologies (ICT) and smart meters. Smart meters support quick and precise measuring and information gathering to allow easy, real-time control of electricity consumption (e.g., power, heating, and cooling devices and appliances). One of many examples for the use of smart grids is that new technologies (e.g., electric vehicles, air conditioning, and household appliances) will require more intelligent energy demand management, as well as involvement of users (e.g., through home automation). Because the final end-state is still unknown, today’s smart grid rollouts can be viewed as the deployment of a general energy ICT platform that forms the basis for future energy-related applications. Because smart grids can potentially mitigate growing energy and environmental concerns, significant investments are being made. For example, the worldwide smart grid market in 2009 was $69 billion, with tens of millions of smart meters installed across the world. By 2014, it could reach about $170 billion. In the US, a chunk of the federal stimulus spending in 2009-10, some $3.4 billion, was directed to investment in, and modernization of, smart grids.¹

Relevant for this article, from an IT perspective, the authors expect that smart grids will have several unique features compared to “normal” IT environments, including critical infrastructure reliability expected; extremely large scale/distribution/interconnectedness; many embedded devices (e.g., smart meters, SCADA-based devices); many stakeholders involved; dynamic stakeholder roles (e.g., buyer, seller); and increasingly dynamic/agile interactions between stakeholders. In addition, many utilities have very immature security practices or security practices that are not being included in the solutions development processes. This is mostly due to the lack of need prior to the incorporation of technology and network connectivity. Many projects are advancing through the life cycle to the point of deployment before security is aware of what has happened.

Smart grid cyber security

The smart grid vision can only become a reality if cyber security risks are sufficiently mitigated. This is because power grids are absolutely critical infrastructure – if power goes down for extended periods, the affected geographic area stands still. New cyber security challenges (e.g., cybercrime or cyber warfare) become a major risk factor due to the convergence of the information technologies (IT) with the electric power grid, the critical reliance on IT for smart grids, and the fact that parts of the smart grid will be connected to the Internet, which makes them susceptible to many of the same malicious attacks that regularly occur against computer networks outside the electrical and energy sectors. The smart grid technologies are introducing in many cases millions of new points of entry into the electric grid by placing meters on every home that have connectivity back to the corporate network and its infrastructure. Some organizations are making attempts to ensure that the paths to the critical cyber assets are separated from the advanced metering infrastructure (AMI) networks, but others just do not appear to understand the risks.

There are also increased privacy concerns, as smart meters and other tools could leak personal and financial data on a consumer to utilities and attackers alike. Many organizations are not transmitting the account information over the networks, when the major issues lie in the usage information itself. Usage information could lead someone to be able to identify patterns that may lead him to know when the consumer is present or away from the premise. However, because of a potential of lack of understanding of how their networks may be interconnected, a utility could potentially expose its entire network to the AMI environment, creating a vector to their critical infrastructure.

This changing environment poses a major challenge to power utility IT departments, which are not ICT/Internet focused and currently mostly operate closed tried-and-tested legacy mainframe/server systems. In general, there is often a “culture gap” between the employees of IT shops and those of electrical and other infrastructure facilities and government regulators.

A few examples of potential risks associated with the evolution of the smart grid include:²

- Greater complexity and interconnectedness increases exposure to potential attackers and unintentional errors.
- Previously closed networks are now opened up and may span multiple smart grid domains (“system of systems”), which increases the attack surface and the risk of cascading attacks.


• More interconnections increase “denial of service” and malware-related attack risks.
• Increasing number of attacker entry points and paths as the number of network nodes increases.
• Increased potential for data confidentiality and privacy breaches due to more extensive data gathering and two-way information.
• In deregulated areas the utility may not have control over the devices being utilized on the AMI or Home Area Network and therefore do not control the security requirements for those devices or even the kinds of devices that may be introduced to the environment.
• Unauthorized privileged access to AMI could provide the opportunity to send control commands or create denial-of-service in order to prevent the utility from issuing control commands.
• Unauthorized access to meters could be exploited in many ways, e.g., readings could be altered for monetary benefit, spoofing the meter and injecting bogus responses to utility command as in denial-of-service attacks, forging meter readings to gain monetary benefits.

Vulnerabilities might allow an attacker to penetrate a network, gain access to control software, and alter load conditions to destabilize the grid in unpredictable, potentially safety-hazardous ways. A cyber attack aimed at energy infrastructure “could disable trains all over the country and it could blow up pipelines. It could cause blackouts and damage electrical power grids so that the blackouts would go on for

@ RSA 2012

Editor: While David was as RSA, presenting and taking in the talks and discussions, we asked if he would share some of his observations.

Cyberwar and Active Defense
Major Themes at RSA

By David L. Willson — ISSA member, Colorado Springs, USA Chapter

RSA 2012 in San Francisco was a great conference, learning experience, and social event all in one. Many topics were discussed, but major themes seemed to be whether we are in a cyberwar and implementing active defense, mitigative counterstrike, or taking the fight to the hackers.

It seems the first salvo began with a panel titled, “Special Forum on the Future of Cyber Security and Active Defense,” that included Gen. Michael Hayden, Lt. Gen. Kenneth Minihan, Jim Dempsey, and Professor Ron Deibert. The group agreed something must be done as attacks are ever increasing. Exactly what actions and to what degree was a definite point of discussion. Generals Hayden and Minihan both advocated government taking on the mission of defending all networks, public and private, in cyberspace. Certainly private industry is not prepared to cede that much power and authority over cyberspace to the government, but the message came through loud and clear: figure something out quickly or it may come to that.


—Ben Tomhave (ISSA member, Northern Virginia, USA Chapter ) and I presented “Legal and Ethical Considerations of Offensive Cyber-Operations,” which was structured along the lines of my recent article in the ISSA Journal, “Hacking Back in Self-Defense.” We discussed the legal and ethical issues of nations, but mostly corporations, using offensive cyber weapons to defend their networks.

—Paul Dot Com pursued a similar theme in “Offensive Countermeasures: Making Attackers’ Lives Miserable,” discussing active defense and technical techniques for traceback and bringing the fight back to the hacker.

—FBI Director Robert Mueller emphasized in his keynote that there are two types of companies: those that have been hacked and those that will be hacked. The days of hackers merely stealing credit card numbers is over. Organized crime has gotten into hacking, and they are taking everything.

Regardless of where you stand on these issues, they cannot be ignored. We can no longer sit back and hope our defenses are good enough. It is common knowledge that attacks have increased significantly and are becoming more sophisticated. They are costing much in time, resources, money, and the loss of proprietary information, intellectual property, and national security secrets.

About the Author
David L. Willson, JD, LLM, CISSP, Security+, is currently owner of Titan Info Security Group, LLC, providing enhanced cyber security and liability reduction or elimination. David is a licensed attorney in Colorado, New York, and Connecticut and is a VP of his local ISSA chapter. He may be reached at david@titaninfosecuritygroup.com.
a long time.” A hacker with a basic knowledge of electronics and a few hundred dollars in hardware could interfere with, and get control over, the smart meters that are essential to managing the two-way interaction.

Theoretical concerns have become practical realities, as a number of exploits involving smart grids and power complexes have taken place. In particular in 2010, Stuxnet, a sophisticated malware attack that targeted Siemens WinCC, industrial control software popular in the utility sector and other industries, via a Microsoft Windows vulnerability, infected at least a dozen systems worldwide (and specifically suspected nuclear weapons facilities in Iran), and represents the first publicly-known rootkit to specifically target industrial control systems. There are many other reported attacks on industrial control systems. Electric Power Research Institute (EPRI) has compiled a database of more than 170 infrastructure cyber incidents.

But as illustrated by a 2003 blackout in the US, cyber security must address not only deliberate attacks, but also inadvertent compromises of the information infrastructure due to user errors, equipment failures, and natural disasters. Another classic failure example was the 1999 explosion of a pipeline in Bellingham, WA, USA, where the computer monitoring systems failed to detect the build-up of pressure within the fuel line – the resulting explosion killed three, and the busted line spilled gasoline into nearby creeks, resulting in $45 million of damage. Another challenge is that it is also not always easy to apply traditional IT security tools and processes such as routine software patches or upgrades to control systems. For example, penetration testing has been known to destroy the firmware or disrupt the control systems of infrastructure facilities, and maintenance of antivirus software on such facilities has disrupted control devices and triggered denials of service. Installation of software patches has prevented shutting off the pumps of water utilities, while software for other infrastructure cannot be patched while the facilities are in operation. Inadvertent incidents have even forced nuclear power plants to fall back on auxiliary power. Fortunately, despite the exploits that have occurred and can occur, malicious or inadvertent, cyber threats to the electrical grid and other infrastructure elements are still at early stages. This fact hopefully will allow companies and government agencies the time to take countermeasures to minimize the threat. Most of the steps that have been proposed mirror those that have been taken to better secure the IT industry against malicious attack.

However, the introduction of these technologies to the electric sector also presents opportunities to increase the reliability of the power system, to make it more capable and more resilient to withstand attacks, equipment failures, human errors, natural disasters, and other threats. Greatly improved monitoring and control capabilities must include cyber security solutions in the development process rather than as a retrofit.
Governments around the world are working on standards and best practice guidance to educate, guide, and to raise awareness. For example, the North American Electric Reliability Corp. (NERC)\(^8\) is a non-profit organization of industry working groups and utilities. It is formulating some Critical Infrastructure Protection (CIP) standards to ensure reliability of power systems in North America. The Federal Energy Regulatory Commission (FERC),\(^9\) an independent agency that regulates transmission and transport of electricity and energy commodities, provides oversight for NERC. NERC currently only focuses on generation and transmission (for North America). There is conversation about setting standards for distribution, but they have not been concluded yet.

As a consequence of these security- and privacy-related challenges, the market for security-related expenditures on smart grids is growing fast, by about one-third a year, and is forecasted to reach $4 billion annually by 2013. A report released in 2010 by Pike Research\(^{10}\) estimated that utility companies worldwide will spend $21 billion by 2015 on smart grid cyber security. As a relatively new field, infrastructure cyber security must begin to embed state-of-the-art security (adapted from other industries with more mature cyber security) into its architecture as part of the design and development process.

**Smart grid security and compliance requirements**

This section analyzes the main security and compliance requirements presented in guidance documents for smart grids related to security policy automation. In particular, as the smart grid emerges, it will be necessary to improve control and visibility in line with recommended guidance (e.g., US NERC CIP and US NIST IR 7628):

- **Control**: Enforce technical security policies across the millions of devices (including many control systems, meters, substations, etc.) across an ever-changing, interconnected IT landscape
- **Visibility**: Show that the technically enforced security policies support compliance with recommended guidance

Smart grids have some unique security and compliance requirements compared to most traditional IT environments, including the need for:

- Message authentication and authorization to millions of devices.
- Tamper resistance and physical device security due to the large number of devices in uncontrolled environments.
- Least privilege access controls between interconnected devices to prevent attack points from scaling across a large number of devices and to compartmentalize distributed attacks.
- Mechanisms to meet power utility-specific legal security and privacy requirements.
- Auditability and metering without compromising privacy regulations.
- Highly secure and automated policy update, certificate management, and configuration management across the network, even for embedded devices, because there will be too many devices to manually manage.
- High availability, which rules out a number of slow or CPU/network performance-hungry security mechanisms.
- High reliability and assurance because smart grids will be critical infrastructure and an attractive attack target.
- Security beyond the network layer to cover all layers (including the application layer) because fine-grained, contextual least-privilege access control and information flow control cannot be effectively implemented purely on the network layer.
- Prevention of social engineering attacks, e.g., through security policy and configuration automation that takes humans out of the loop.
- Security of consumer usage information on millions of devices.

To achieve these complex requirements, security will need to be designed into the smart grid architecture right from the beginning – because retrofitting security after the system has been designed and built will be more costly and less effective.

Unfortunately, many of the companies that are producing the solutions for meter management have not incorporated security messages in their products beyond simple physical breaches of the equipment. Utilities will have to request modifications of the products to be able to capture security information that would provide sufficient forensic value.

**Security requirements guidance for smart grids**

In the US, North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) is the

Continued on page 30.
foremost recommended guidance for protecting power grids against cyber attacks. It is soon expected to fully apply to all aspects of smart grids.

This article will focus on another major publication, US NIST’s 537-page, “Guidelines for Smart Grid Cyber Security,” NIST IR 7628, security requirements and risk assessment framework.

The guideline includes high-level security requirements, a framework for assessing risks, an evaluation of privacy issues at personal residences, and additional information for businesses and organizations to use as they craft strategies to protect the modernizing power grid from attacks, malicious code, cascading errors, and other threats. Its reference architecture with six functional priority areas across seven domains and 46 actors identifies 137 interfaces – points of data exchange or other types of interactions within or between different smart grid systems and subsystems. These are assigned to one or more of 22 categories on the basis of shared or similar functional and security characteristics. In all, the report details 189 high-level security requirements, which are grouped in 19 families, applicable either to the entire smart grid or to particular parts of the grid and associated interface categories.

The report also includes a description of the risk assessment process used to identify the requirements, a discussion of technical cryptographic and key management issues across the scope of smart grid systems and devices, and initial recommendations for addressing privacy risks and challenges pertaining to personal residences and electric vehicles. It also includes an overview of the process that the Cyber Security Working Group (CSWG) developed to assess whether existing or new standards that enable smart grid interoperability also satisfy the high-level security requirements included in the report, and summaries of research needs.

Several controls recommended in NIST IR 7628 directly relate to security policy automation for smart grids, particularly relevant least privilege and information flow enforcement.

**Least privilege**

The recommended control, Least Privilege (NIST IR 7628 - SG.AC-7), requires that “the organization assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks,” and that “the organization configures the smart grid information system to enforce the most restrictive set of rights and privileges or access needed by users.” In other words, a caller should only be granted access to a resource if that caller has a need to do so in the specific context, for example, a particular step in a business process, or a particular system situation such as emergency level.

What this specifically means is that a dynamic access control “whitelist” (i.e., stating what is allowed vs. “blacklists” that state what is not allowed) needs to be available that enforces that policy requirement. Static access control models such as identity-based access control (IBAC) or role-based access control (RBAC) are not sufficient access mechanisms because they do not capture such context in the policy. As a result, virtually all IBAC/RBAC implementations, including traditional Identity and Access Management (IAM) technologies, are insufficient on their own. Attribute-based access control (ABAC), as for example standardized in OASIS Extensible Access Control Markup Language (XACML), help add this missing context and other additional expressions to the policy. The flipside of ABAC is that those fine-grained contextual authorization policies are extremely difficult, time-consuming, and error-prone for human administrators to manually author and maintain.

**Information flow enforcement**

The recommended control Information Flow Enforcement (NIST IR 7628 - SG.AC-5) requires that the smart grid information system enforces assigned authorizations for controlling the flow of information within the smart grid information system and between interconnected smart grid information systems in accordance with applicable policy. Information flow control regulates where information is allowed to travel within a smart grid information system and between smart grid information systems. As example implementations, the document mentions boundary protection devices that restrict smart grid information system services or provide a packet-filtering capability.

---

13 The section of the document also offers the additional considerations relevant to this discussion, in particular that “the organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system,” and “the organization authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.”


This section of the document also offers a number of supplemental considerations. Particularly interesting for this discussion, the guidance recommends “dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations.”

As already mentioned in the previous section, IBAC and RBAC are insufficient on their own, and due to the inherent changing (“agile”) nature of today’s interconnected IT landscapes (“system of systems”), ABAC policies would need to be constantly manually updated to be correct after “system of systems” changes, resulting in a policy management nightmare. There are a number of other problems with ABAC, e.g., challenges around authorization delegation across service chains and impersonation, which can be solved using authorization-based access control (ZBAC), which uses authorization tokens and federated authorization token servers.

Security incident monitoring, reporting, and auditing

Related to achieving visibility, numerous recommendations for incident monitoring, incident reporting, and auditing are spread throughout the NIST IR 7628 document. For example:

- **Smart Grid Information System Monitoring Tools and Techniques** (SG.SI-4) requires that “the organization monitors events … to detect attacks, unauthorized activities or conditions, and non-malicious errors” based on the organization’s “monitoring objectives and the capability of the smart grid information system to support such activities.” The supplemental guidance states that this can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools), and can include real-time alerting.

- **Incident Monitoring** (SG.IR-6) requires that “the organization tracks and documents … security incidents,” maybe using “automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.”

- **Incident Reporting** (SG.IR-7) requires incident reporting procedures about what is an incident, granularity of incident information, who receives it, etc., again potentially employing “automated mechanisms to assist in the reporting of security incidents.”

- **Auditable Events** (SG.AU-2) requires identifying events that need to be auditable as significant and relevant, and requires the development and review of a list of auditable events on an organization-defined frequency, including execution of privileged functions.

- **Audit Monitoring, Analysis, and Reporting** (SG.AU-6) requires audit record reviews and analyzes to find and report inappropriate or unusual activity, potentially employing automated, centralized analysis tools.

- **Audit Reduction and Report Generation** (SG.AU-7) supports near real-time analysis and after-the-fact investigations of security incidents, e.g., by automatically processing audit records for events of interest based on selectable event criteria.

- **Audit Generation** (SG.AU-15) recommends audit record generation capability, potentially from multiple components into a system-wide audit trail that is time-correlated.

- **Remote Access** (SG.AC15) mentions automated mechanisms to facilitate monitoring and control of remote access methods.

In the context of the fine-grained contextual authorization mentioned earlier, incident monitoring, reporting, and audit are intrinsically intertwined with authorization. Monitoring, reporting, and audit tools will need to know the specific authorization policies in order to decide whether behavior is in fact suspicious or not. This differs dramatically from traditional monitoring approaches which mainly monitor for generic vulnerabilities (i.e., the same vulnerabilities occur for a particular technology, rather than for a particular business) and thus do not need to know any specifics about the organization’s business processes in order to flag an incident. The
author call control and visibility for generic vulnerabilities “security hygiene” to distinguish them from organization-specific policy enforcement and monitoring.

Model-driven security policy automation for smart grids

This section describes how authorization policy implementation can be automated using model-driven security.

Model-driven security

Since 2002, the authors have implemented “model-driven security,”20 the use of model-driven approaches to automate the generation of technical security policy implementation from generic security requirements models. Numerous publications are available.21 Model-driven security solves the challenge that manually translating security policy and compliance requirements into effective technical implementation is difficult, expensive, and error-prone — especially for inter-connected, agile, large-scale software application landscapes such as smart grids. The main challenges are:

- Where do concrete policy requirements (based on the rather vague guidance documents) come from?
- Who can reliably write the matching technical policy rules?
- Who can reliably and cost-effectively maintain them despite dynamic changes?
- Who can verify policy correctness and compliance?

The authors’ definition of model-driven security (MDS) is as follows:

MDS is the tool-supported process of modelling generic, human-understandable security requirements at a high level of abstraction, and using other information sources available about the system produced by other stakeholders (e.g., mashup/orchestration models, application models, network topology models). These inputs, which are expressed in Domain Specific Languages (DSL), are then transformed into enforceable security rules with as little human intervention as possible. It also includes run-time security management (e.g., entitlements/authorizations), i.e., run-time enforcement of the policy on the protected IT systems, dynamic policy updates, and the monitoring of policy violations. MDS helps develop, operate, and maintain secure applications by making security proactive, manageable, intuitive, cheaper, and less risky.23

This model-driven security policy-automation approach forms a critical part24 of any authorization management, entitlement management, and identity and access management strategy. Through its integration with system/application-specification tools (e.g., modelling, orchestration, and development tools), it also enables a secure application development life cycle at development time right from the beginning — dealing with policy abstraction, externalization, authoring, automation, enforcement, audit monitoring and reporting, and verification.

The authors have developed a full-fledged model-driven security framework, Open Policy Management Framework (OpenPMF), which automates application security policies for access authorization and incident monitoring. OpenPMF automates the process of translating human-understandable security and compliance requirements into the corresponding numerous and ever-changing technical authorization policy rules and configurations. In addition, it proactively enforces (“whitelisting”) decentralized access decisions and continuously monitors for security incidents (including at the application layer). OpenPMF involves five steps:

1. **Configure intuitive business security requirements:**
   Security professionals can configure and audit generic application security requirements, including access and monitoring policies. No need to be an application specialist. The Human-Machine Interface (HMI) to configure model-driven policies is similarly intuitive and visual as process modelling and enterprise architecture tools.

2. **Generate matching technical security policies automatically:**
   Application developers can implement application-specific technical application security at the click of a button. OpenPMF automatically analyzes your software as it is being written or updated, and generates fine-grained access and audit policies. No need to be a security specialist.

3. **Enforce technical security policies transparently:**
   At runtime, local protection agents underneath all applications automatically intercept and check all application communications before they are forwarded to the application.

4. **Audit technical security policies transparently:**
   At runtime, automatically monitor and collect incident alerts and analyze them for compliance purposes. The collected information can be configured through fine-grained audit policies. In large-scale deployments, analyzed alert information is provided to third-party monitoring tools, to ensure there is a single HMI for operators to be concerned with. There is also a basic built-in HMI for incident moni-

22 Asset tracking tools can replace modeling/orchestration tools for the purposes of model-driven security.
24 Other important aspects to consider are network segmentation, incident monitoring, vulnerability analysis and testing.
26 For scalability, availability, and robustness reasons, OpenPMF’s Policy Decision Points (PDPs) are typically deployed decentralized and collocated with the Policy Enforcement Points (PEPs) on each protected systems.
New opportunities abound in the midst of amazing transformations in technology, business, and culture. Inspired by Disney’s innovative vision, the cybersecurity community will gather at the Magic Kingdom on October 25-26 to look at change as a chance to achieve excellence. Disruptions like "big data," "cloud computing," massive collaboration, and business transformation make it possible for us to blaze new trails and build effective foundations. We are enabling our work forces to be mobile and productive while protecting sensitive data. We build systems and policies that impede our foes and guard our constituents. This is an exciting time to be in the information security field as we are all vital in making our businesses faster, better, smarter and, most importantly, safer. Imagine the possibilities. Sessions will include:

- Cloud
- Infrastructure
- Mobile Security
- Threat Updates
- Big Data
- Business Skills
- Application Security
- Legal Updates
- Critical Infrastructure
- Securing the End Users
- Incident Response
- Governance and Compliance

Visit www.issaconference.org to be notified when registration opens.

**Special Events:**

- Calling all Chapter Leaders: Chapter Leaders Summit® – October 24
- CISO Executive members and guests: 4th Quarter CISO Forum® – October 27
  immediately following the International Conference.

*Open to qualified attendees only.*

Mark your calendar for the 2012 ISSA International Conference

for more information visit:
www.issaconference.org
toring for small-scale or development purposes.

5. Update technical security policies automatically: agile policy automation uniquely makes policy management and implementation manageable for today’s rapidly evolving interconnected applications (e.g., agile SOA with business process modelling [BPM], agile cloud infrastructures).

OpenPMF is based on open standards where possible (e.g., Eclipse EMF, and web app server security APIs, XACML, syslog), and because it is designed as a customizable, future-proof toolkit, it can be easily expanded to both legacy devices and new kinds of devices from different vendors.

OpenPMF automates policy management even for complex, large-scale environments such as smart grids, as well as agile service-oriented architecture (SOA) and cloud application platforms. Developed since 2002, OpenPMF is useful for protecting smart grids because it has already been successfully used in other highly regulated, critical, large-scale sectors such as defence, healthcare, air traffic management, and telecoms. Thanks to its decentralized architecture, it supports authorization management and enforcement across several trust domains (e.g., across multiple companies’ networks, or intra-company network segments), and across multiple devices. As mentioned earlier, ZBAC should be used to achieve scalable and manageable cross-domain authorization management.

MDS is well suited to implement authorization policy implementation for smart grids in an automated, flexible, reliable, and cost-effective way. Figure 1 shows how smart grid system models (e.g., from asset tracking/monitoring tools, development tools, deployment/orchestration tools) and security requirements models (captured within OpenPMF) are used to generate fine-grained, contextual technical access rules. These technical rules are then distributed to local policy decision and enforcement points, where they are automatically enforced at runtime on all traffic.

Model-driven security incident monitoring and analysis automation

As authorization becomes increasingly fine-grained and contextual, authorization incident monitoring and analysis also need to be policy-driven. This is because the authorization policy determines to a large extent what behavior is deemed to be an incident.

In the simplest case, any blocked access requests should trigger an incident alert in real time. Furthermore, customized incident monitoring policy rules can be specified to trigger customized incident alerts. But just creating such incidents is not enough. This is because security administrators typically get flooded by an unmanageably large number of irrelevant alerts and cannot prioritize and filter alerts based on the policy requirements to find and respond to the truly important situations.

To solve this problem, the authors have implemented an automatic model-driven correlation engine called Model Driven Security Accreditation (MDSA), originally developed for automating large parts of the compliance and assurance accreditation management processes (e.g., Common Criteria) to achieve reduced cost/effect, and increased reliability/traceability. MDSA automatically analyzes and documents two main compliance aspects:

- Does the actual security of the system of systems at any given point match with the stated requirements? MDSA is a system and method for managing and analyzing security and information assurance requirements in reusable models, and for (mostly) automating the verification of the traceable correspondence between incident alerts, functional models, security models, and requirements models.
- Do any changes to the system of systems impact the current accreditation? MDSA automatically identifies changes to any aspect of the system of systems, and evaluates whether changes impact the current accreditation and whether manual corrections and re-accreditation are required.


28 Based on the authors’ experience gained from being part of several smart grid alliances and centers of excellence, and from informal knowledge exchange with security staff at power utilities and smart grid vendors.

29 Background images for Figure 1+2 top: © ObjectSecurity, bottom © GridWise Alliance

toring for small-scale or development purposes.

5. Update technical security policies automatically: agile policy automation uniquely makes policy management and implementation manageable for today's rapidly evolving interconnected applications (e.g., agile SOA with business process modelling [BPM], agile cloud infrastructures).

OpenPMF is based on open standards where possible (e.g., Eclipse EMF, and web app server security APIs, XACML, syslog), and because it is designed as a customizable, future-proof toolkit, it can be easily expanded to both legacy devices and new kinds of devices from different vendors.

OpenPMF automates policy management even for complex, large-scale environments such as smart grids, as well as agile service-oriented architecture (SOA) and cloud application platforms. Developed since 2002, OpenPMF is useful for protecting smart grids because it has already been successfully used in other highly regulated, critical, large-scale sectors such as defence, healthcare, air traffic management, and telecoms. Thanks to its decentralized architecture, it supports authorization management and enforcement across several trust domains (e.g., across multiple companies' networks, or intra-company network segments), and across multiple devices. As mentioned earlier, ZBAC should be used to achieve scalable and manageable cross-domain authorization management.

MDS is well suited to implement authorization policy implementation for smart grids in an automated, flexible, reliable, and cost-effective way. Figure 1 shows how smart grid system models (e.g., from asset tracking/monitoring tools, development tools, deployment/orchestration tools) and security requirements models (captured within OpenPMF) are used to generate fine-grained, contextual technical access rules. These technical rules are then distributed to local policy decision and enforcement points, where they are automatically enforced at runtime on all traffic.

Model-driven security incident monitoring and analysis automation

As authorization becomes increasingly fine-grained and contextual, authorization incident monitoring and analysis also need to be policy-driven. This is because the authorization policy determines to a large extent what behavior is deemed to be an incident.

In the simplest case, any blocked access requests should trigger an incident alert in real time. Furthermore, customized incident monitoring policy rules can be specified to trigger customized incident alerts. But just creating such incidents is not enough. This is because security administrators typically get flooded by an unmanageably large number of irrelevant alerts and cannot prioritize and filter alerts based on the policy requirements to find and respond to the truly important situations.

To solve this problem, the authors have implemented an automatic model-driven correlation engine called Model Driven Security Accreditation (MDSA), originally developed for automating large parts of the compliance and assurance accreditation management processes (e.g., Common Criteria) to achieve reduced cost/effort, and increased reliability/traceability. MDSA automatically analyzes and documents two main compliance aspects:

- Does the actual security of the system of systems at any given point match with the stated requirements? MDSA is a system and method for managing and analyzing security and information assurance requirements in reusable models, and for (mostly) automating the verification of the traceable correspondence between incident alerts, functional models, security models, and requirements models.
- Do any changes to the system of systems impact the current accreditation? MDSA automatically identifies changes to any aspect of the system of systems, and evaluates whether changes impact the current accreditation and whether manual corrections and re-accreditation are required.
Figure 2 shows in simplistic terms how local policy monitoring points generate incident alerts based on the policy (implemented in the same piece of software that contains the policy decision and enforcement logic). These alerts are centrally collected and automatically correlated with the various system and security models, as well as with other information. The result is a consolidated report that correlates each incident to the affected security requirements and parts of the system.

**Example use-case scenario**

This section outlines a basic use-case scenario to illustrate how the described solution works. Assume the following policy statement that includes least privilege, information flow control, and incident monitoring/analysis:

A power utilities’ customer service staff should only be able to initiate the electricity shutoff at a smart meter (by sending a web service request to a web service that deals with the shutoff) if the corresponding customer requested termination of service or has not paid for electricity usage, and an incident alert detailing the shutoff should be automatically generated by the meter and analyzed by the operator.

Also assume a service-oriented architecture where the customer service staff uses a browser-based web application that is orchestrated from numerous web services using business process modelling (BPM) orchestration tool. While on the phone to the customer, the BPM tool guides the staff through a defined multi-step business process through several web pages. The steps are: get customer information, verify balance or shutoff request, verify meter correctness, instruct smart meter infrastructure to shut off electricity. Note that it is intended that this workflow could change frequently to reflect changes in the way the business is run.

The five steps of model-driven security now look as follows:

1. **Policy Model Configuration**: When the system is designed, built, and deployed, security specialists capture the security requirements in a domain specific language, a modelling language that uses the concepts configured specifically for the requirements of power utilities (e.g., smart meters, smart meter shutoff service, customer payment information). This can be done using a visualization or a model editor. It is important that these policy models are specified generically and close to human thinking (i.e., close to the policy description above).

2. **Technical Policy Generation**: Next, the model-driven security tool automatically analyzes the security policy model, the BPM orchestration model, and other information, and automatically generates the policy rules for each node. For example, the rules generated for the shutoff web service will include, e.g., “only accept the shutoff request if it is secured and comes from a known customer service system node and from the correct network segment, and from an authenticated and authorized customer service staff, and only if that staff’s web application is currently going through the business process involving the customer whose meter is going to be shut off, and only if there is a shutoff request or non-payment notice on that customer’s account, and only if the business process is currently at the 5th (example!) step (the shutoff step) in the business process, and only if there is no emergency or crisis situation on the network; in this case an incident alert should be generated for analysis and auditing purposes,” etc. As opposed to authentication-based or role-based access control, such a contextual, fine-grained authorization rule implements real least privilege access control. Once all the rules have been generated, they get automatically distributed to policy decision points (PDPs) on each protected system for localized decision making.

3. **Technical Rule Enforcement**: Whenever a message arrives at a protected system, the PDP automatically evaluates the policy and makes a decision whether to grant or deny the request. The PDP then preventively enforces that decision by potentially blocking the message.

4. **Incident Monitoring and Analysis**: A policy monitoring point (PMP) also generates alerts if needed, based on the policy or based on incidents (such as unauthorized blocked requests). Using model-driven approaches, alerts information can now be automatically analyzed and correlated with the specific requirements in the model – this minimizes irrelevant information and enables more accurate decision-making in near real time.
5. **Automatic Updates**: Whenever the system changes, the rules can automatically be updated. For example, if the business process for the customer service staff changes to include an extra step where the supervisor authorizes each shutoff request, or if the customer service staff has to get authorization before viewing customer payment information, then the BPM service orchestration will change and the shutoff step in the business process may now be somewhere else in the workflow. The technical policy on the shutoff web service should then, for example, be automatically configured so that the correct step is not step 5 anymore but, say, step 9 in the process sequence, and that, for example, a valid delegated authorization token from the supervisor must be attached to the request. Because model-driven security generates technical rules automatically from generic models, these rules can be updated and deployed automatically if such changes occur, which minimizes security policy management.

While this example is deliberately simplistic and hypothetical, model-driven security is being implemented in several critical sectors with security requirements similar to smart grids, such as defence, air traffic control, and crisis management, and is being considered for health IT and government cloud computing.

**Conclusion**

This article explains why smart grid architectures need to be designed to include state-of-the-art model-driven security approaches to control and visibility. Recommended controls such as least privilege, information flow enforcement, and policy-driven monitoring/analysis can only be effectively implemented at the very large scale of a smart grid by using a combination of MDS with fine-grained, contextual authorization management and identity and access management and explains why on their own they are insufficient mechanisms. MDS needs to be designed into the architecture right from the start to ensure that the architecture is geared to support it. The actual deployment road map can then be implemented gradually based on a low-risk “start small, think big” approach (similar to how the smart grid itself is rolled out). While some degree of customization is to be expected due to the uniqueness of smart grid technology platforms (e.g., many embedded and legacy devices, unique security requirements), the authors have proven the approach in other critical infrastructure projects.

**Acknowledgements**

The authors would like to thank the following individuals for their comments and suggestions on the final draft of this article (in alphabetic order): Christine Hertzog (Smart Grid Library), Amir Khan (consultant for Portland Gas & Electric), John Reynolds (Integrated Architectures), and Jeffrey J. Sweet (American Electric Power).

---

**About the Authors**

Dr. Ulrich Lang, Object Security CEO and co-founder, received his Ph.D. from the University of Cambridge Computer Laboratory (Security Group) on conceptual aspects of middleware security in 2003 and a Master’s Degree (M. Sc.) in Information Security with distinction from Royal Holloway College (University of London) in 1997. Ulrich is a renowned thought leader in model-driven security, access control policy, and Cloud/SOA/middleware security and is responsible for the business and technical strategy, architecture and direction of ObjectSecurity and the OpenPMF product. He may be reached at ulrich.lang@objectsecurity.com.

Rudolf Schreiner, Object Security CTO and co-founder, received his Master’s (Dipl-Phys.) in physics from University of Munich in 1993. He is currently the main software architect for the OpenPMF product and is also the principal architect behind MICO-Sec Secure CORBA and the ObjectWall IIOP firewall. His main interest is the modeling and development of mission-critical and secure applications, the development of secure distributed systems in the air traffic management domain for one. He may be reached at rudolf.schreiner@objectsecurity.com.