North American Policies and Technologies

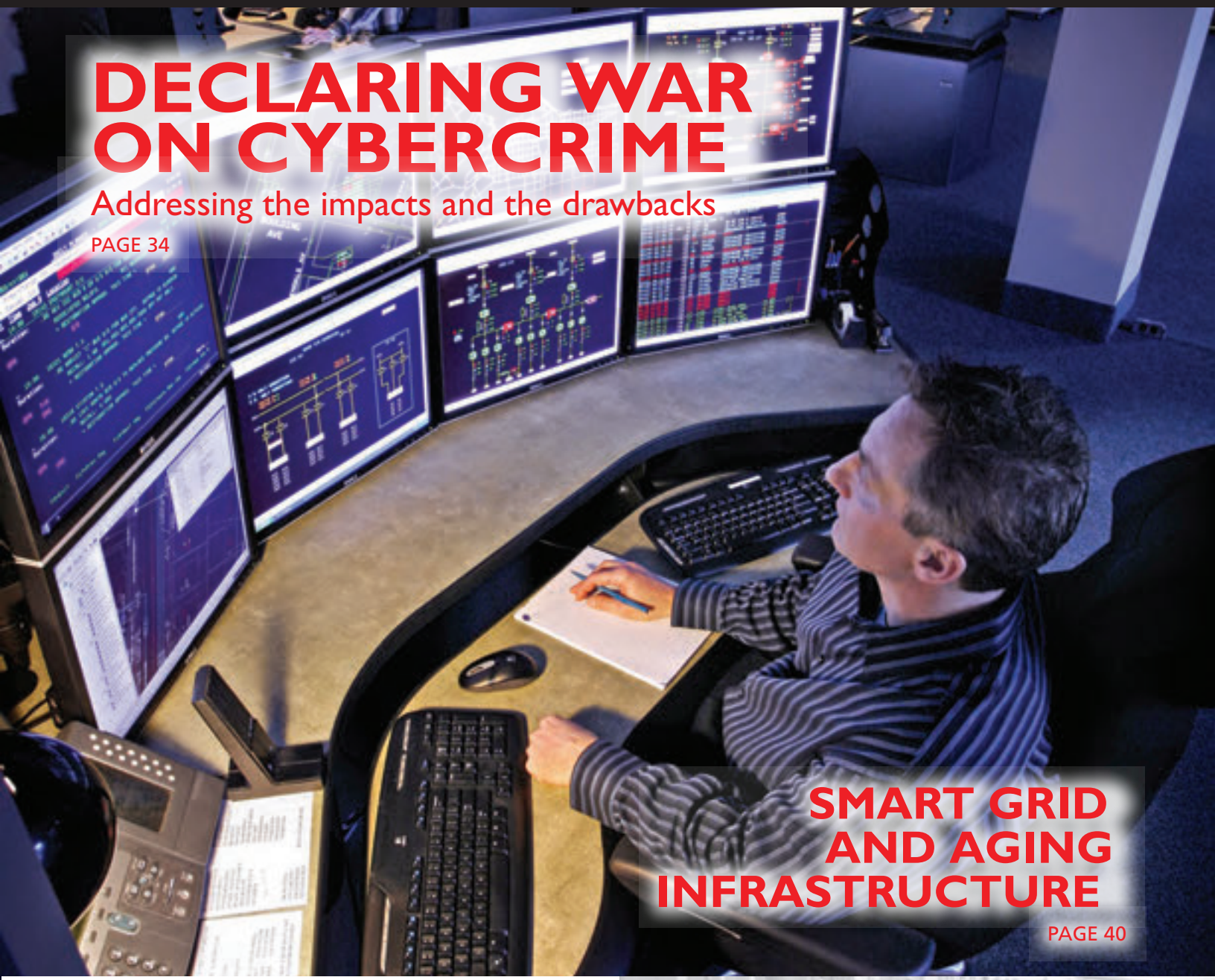
ELECTRICITY Today

Transmission & Distribution

Est 1986

Expanded Digital Magazine

June 2013 Volume 26, No. 5



DECLARING WAR ON CYBERCRIME

Addressing the impacts and the drawbacks

PAGE 34

SMART GRID AND AGING INFRASTRUCTURE

PAGE 40

Protecting sensitive customer and utility data

BY JOHN CHOWDHURY, Fujitsu Network Communications, Inc.

Smart meters, and the advanced metering infrastructure (AMI) on which they depend, collect and transport vast amounts of data. While the data provides more precise energy billing, as well as valuable insight into energy demand and usage patterns, consumers expect that utilities will keep that data secure and that their privacy will be protected.

Security and privacy are prerequisites to increased AMI adoption, and more broadly, Smart Grid implementations. Recognizing this, multiple U.S. federal agencies, including the Government Accountability Office (GAO), Department of Energy (DOE), National Institute of Standards and Technology (NIST) and Department of Homeland Security (DHS), are engaged in cross-agency collaboration, and are working with utilities and technology suppliers too, in an effort to ensure security and privacy are part of all smart meter implementations.

In Canada, under the divisions of legislative responsibility of the Canadian constitution, electricity matters, such as AMI security and privacy, falling within the boundaries of a single province are under provincial jurisdiction. With the AMI initiatives in Canada, authorities such as Natural Resources Canada (NRCan) and the Standards Council of Canada (SCC), work with the International Electrotechnical Commission (CNC/IEC), and

SCC GUIDING PRINCIPLES

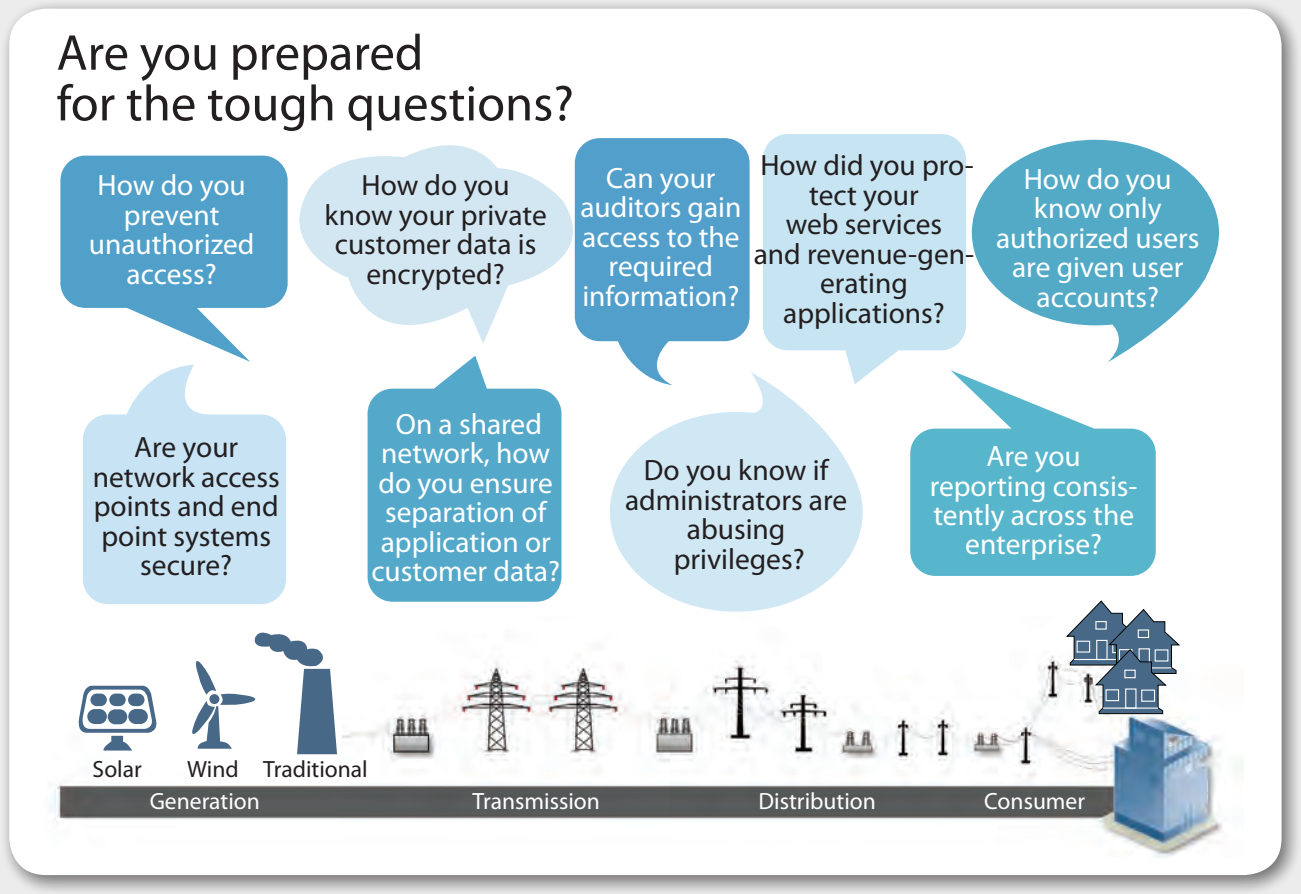
The Standards Council of Canada (SCC) provided three guiding principles for the operations of the International Electrotechnical Commission's Task Force on Smart Grid Technology and Standards.

1. Ensure that Canada's needs are reflected in products developed under the IEC's Smart Grid initiatives
2. Leverage—to the maximum extent possible—national and North American efforts to ensure Canadian Smart Grid priorities are identified and incorporated into the IEC's work plan
3. Coordinate standards development in such a way as to avoid national and regional differences

KEY SECURITY QUESTIONS

Educating utilities on pertinent information

- How do we ensure that the pricing signals being sent to the customer are being properly received?
- How do we know the AMI system has not turned all appliances on/off inappropriately? What feedback and protection loops do we have to have in place?
- How do we prevent unauthorized penetration of the network to the home? How do we ensure that unauthorized changes to customer consumption data is not occurring?
- What controls do we need to have so that sensitive customer data is not being externally transmitted? What is our liability if someone inappropriately leverages this data?
- How do we protect against unauthorized access to Internet-based controls and monitoring portals by third parties or customers?
- What controls do we need to put in place so the system, once interfaced to the WMS/OMS (workflow management system/outage management system), does not call out inappropriate information?
- How do we provide redundancy to ensure that events are properly recorded as they occur, and that faulty information is caught before it creates a costly diversion?
- How do we ensure that we are correctly capturing all the meter reads, and that we can qualify the data is correctly tied to a specific premise or customer account?
- If we link our AMI to distribution system control/management, how do we ensure that we do not inadvertently switch circuits through intentional or unintentional AMI faults?
- How do we prevent outsider/insiders from inappropriately seizing remote control of our assets?


Are you prepared for the tough questions?
How do you prevent unauthorized access?
How do you know your private customer data is encrypted?
Can your auditors gain access to the required information?
How did you protect your web services and revenue-generating applications?
How do you know only authorized users are given user accounts?
Are your network access points and end point systems secure?
On a shared network, how do you ensure separation of application or customer data?
Do you know if administrators are abusing privileges?
Are you reporting consistently across the enterprise?
Solar
Wind
Traditional
Generation
Transmission
Distribution
Consumer

U.S. counterparts to develop a national body, defining and coordinating Canada's Smart Grid standardization initiatives.

The CNC/IEC provides policy advice to SCC on matters pertaining to IEC and has oversight responsibility for many Canadian activities. To meet that need, the CNC/IEC created the Task Force on Smart Grid Technology and Standards (*see "SCC Guiding Principles"* sidebar).

For smart meter security, Measurement Canada's Software Security Joint Working Group has reviewed the International Organization of Legal Metrology (OIML) standard OIML-D31: "*General Requirements for Software-Controlled Measuring Instruments*". Measurement Canada, a department of the Canadian federal government, was represented within the TC5/SC2: *"General Requirements for Software-Controlled Measuring Devices"* standard's OIML Working Group. Consequently, Measurement Canada developed, in collaboration with industry stakeholders the S-EG-05: "*Specifications for the Approval of Software Controlled Electricity and Gas Metering Devices*", and the S-EG-06: *"Specifications Relating to Event Loggers for Electricity and Gas Metering Devices*".

These specifications are being used in Canada for meter-type approval, including encryption, authenticity check (public keys and signatures), and integrity check and design requirements. These specifications allow for software upgrades under certain conditions.

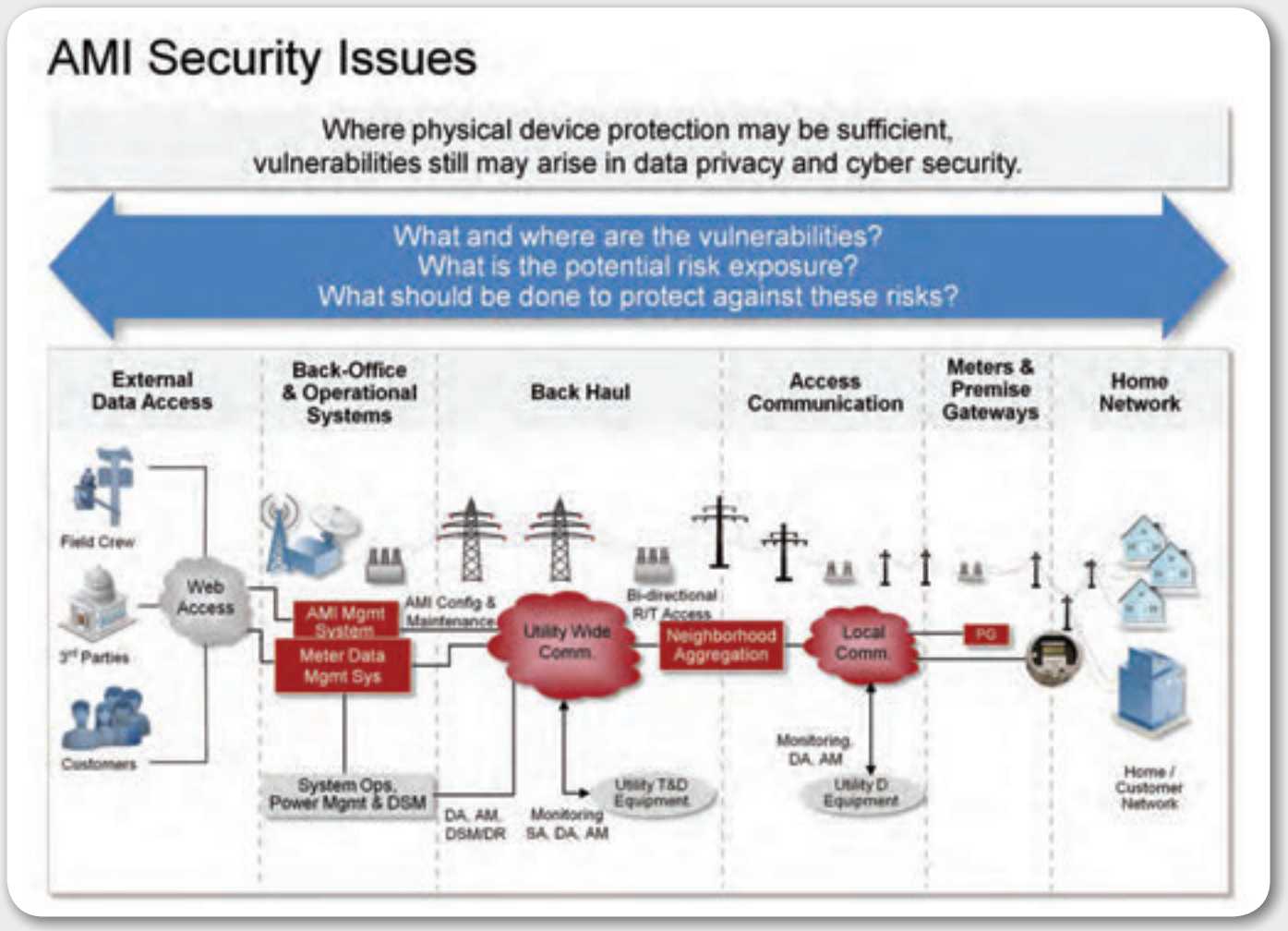
The NERC Technical Committees (Operating, Planning, and Critical Infrastructure) for the North American transmission systems have begun to address the implications of reliability through five task forces. In addition to being staffed by industry experts, these task forces are supported by globally-renowned U.S. and Canadian governmental agencies, scientists and subject matter experts.

North American electric utilities are investing in the communications technologies that are necessary in order to make security a reality by reliably transporting smart meter data in a way that maintains consumer privacy and ensures AMI security. In this issue's Technical Knowledge column, we'll answer the key security questions (see "Key Security Questions" sidebar on Page 20) that utilities should be asking, review some potential security vulnerabilities and examine the strategies proving most successful for countering them.

HAN SECURITY RISKS

Following are key security concerns for customers and utilities who support home area networks (HAN)

Privacy of HAN data	• Local customer usage data • Utility messages to local customer • Other neighboring customer data
Integrity of HAN data	• Prevent data modification
Unauthorized use of network services	• Local service disruption • Widespread service disruption • Data modifications that affects customer • Privacy of other customer data
Neighborhood area networks (NAN) intrusion	• Local service disruption • Widespread service disruption • Data modification that affects billing • Privacy of other customer data



IDENTIFYING THE WEAK POINTS

AMI is rightly applauded for its ability to help utilities and consumers better understand energy usage. But AMI, particularly when paired with home area networks (HANs), means consumers are no longer quarantined or protected from outside hackers. Data collected by smart meters can be highly detailed. For example, individual appliances used by the consumer, along with the days and times those appliances are used, may be identified through AMI data. The transmission of this personal information over communications networks makes it subject to potential interception or theft as it travels network segments.

Internet Protocol (IP)-oriented control protocols such as the Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF), as well as Layer 2.5 protocols such as Multiprotocol Label Switching (MPLS), dynamically exchange information for topology updates and routing. These protocols listen for updates and are inherently vulnerable to malicious attacks such as spoofing and denial of service (DoS). Since these protocols are IP-based, they also have the potential to be exposed to the Internet at large. IP is the favored access method by organized crime, profiteers and foreign powers intent on network intrusion, theft and attack. Even a novice hacker could create a lot of havoc in the AMI if given access to the routing information and the list of all user and devices in the IP network.

ELIMINATING WEAK POINTS

Successfully overcoming the challenges to smart meter and AMI vulnerabilities starts with selecting the right communications networking solution provider. After all, this company will provide the technology and the professional services on which the rest of the AMI depends. In reality, there is several existing security solutions that can assist utilities in creating a secure AMI network (see *"Existing Security Solutions"* sidebar on page 24). To protect the AMI application layer, the information in the *"Protecting the AMI Layer"* sidebar on page 25, is a starting point to protect networks from potential threats.

It's advantageous for utilities to select a communications networking solutions partner that understands the lower layers of the open systems interconnection (OSI) reference model and how it can be utilized to eliminate security threats. Unfortunately, too many AMI program implementations in the past were undertaken by vendors whose only focus was on their specific domain. This shortcoming left the responsibility for security risk mitigation to other participants in the project that provided quality work after the fact to ensure no security vulnerabilities were present.

The OSI model (see "OSI Model" table) divides the functions of a protocol into a series of layers to achieve a high reusability and standardization of software. Each layer exchanges information with the layer below, or to the layer above, or vice-versa. A communication device/system, with an implemented protocol consisting of a series of these OSI layers, is known as a 'protocol stack' or

OSI Model

	Data unit	Layer	Function
Host layers	Data	Application Presentation Session	Network process to application Data representation and encryption Interhost communication
	Segments	Transport	End-to-end connections and reliability
Media layers	Packets	Network	Path determination and logical addressing (IP)
	Frames	Data link	Physical addressing (MAC and LLC)
	Bits	Physical	Media, signal and binary transmission

Source: *International Telecommunication Union (ITU)*

OSI STACKS

The following diagram shows how the different layers are mapped into the OSI stack:

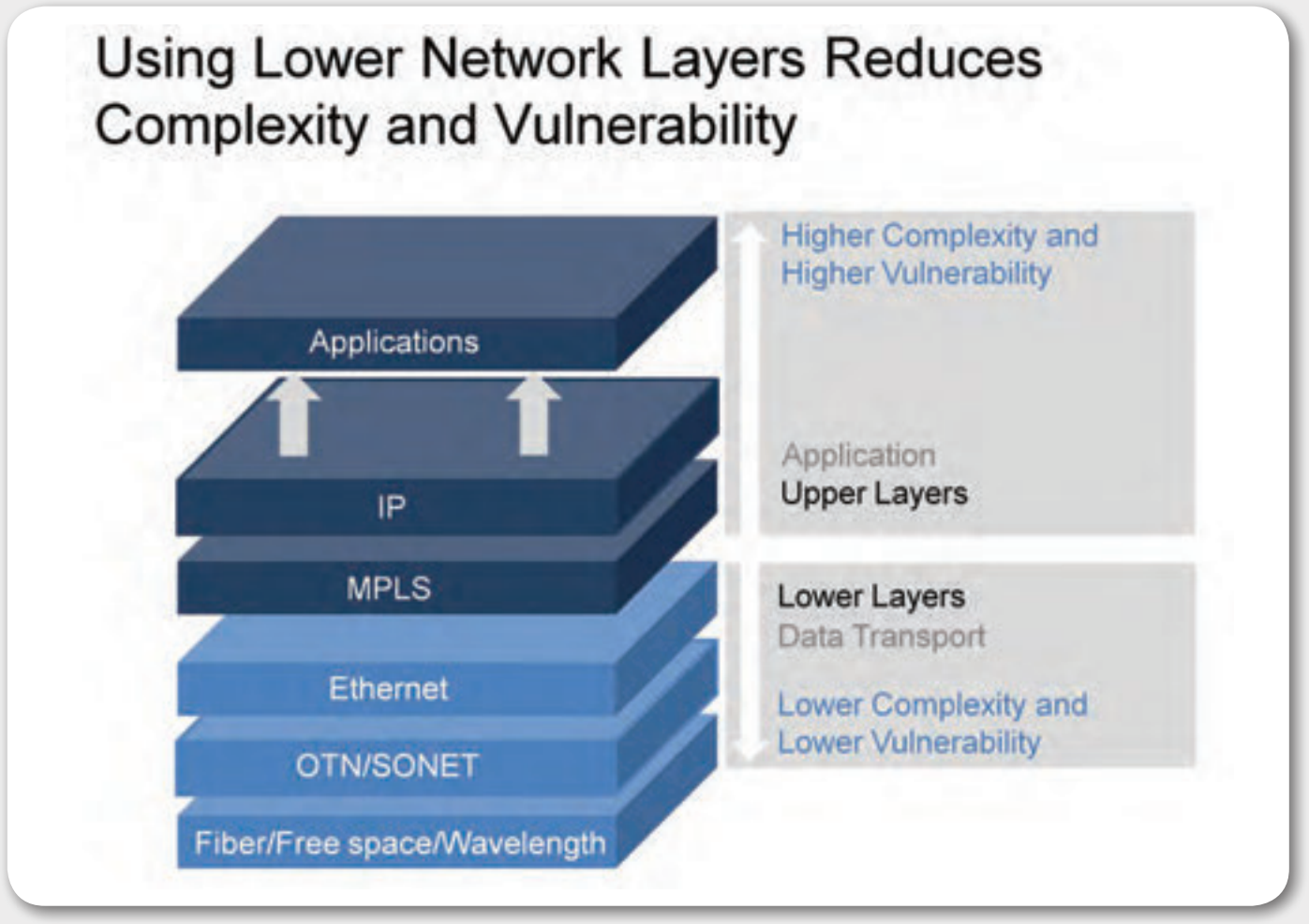
OSI Layer 4 to 7	< -- >	Applications
OSI Layer 3	< -- >	IP
OSI Layer 2.5	< -- >	MPLS
OSI Layer 2	< -- >	Carrier Ethernet
OSI Layer 1	< -- >	OTN/SONET Fiber/Free space/Wavelength

'communication stack'. Protocol stacks can be implemented either in hardware (for example, in embedded software) or software, or a mixture of both. Usually, the implementation of a protocol is mostly described in the OSI layers.

Utilities should utilize network communications technologies that operate at the lower levels as they are more secure than the upper layers, particularly in the access area that may not be as physically secure as a substation or data center. For example, Carrier Ethernet/Connection-Oriented Ethernet is a standards-based, Layer 2 technology that provides a primary path and a pre-defined backup data path across a packet network. It does not utilize any protocols that require an exchange of information between networking devices. For example, OSPF and IS-IS are link-state routing protocols, used by MPLS, which regularly exchange link-state information to update topology and routing information between routers. This makes every routing act vulnerable to intrusion and the theft of information residing in related databases.

Assuming AMI data is encrypted, which is an operation performed by smart meters, then transmitting the encrypted information across a network

EXISTING SECURITY SOLUTIONS	
PRINCIPLES	**EXISTING CONGRUENT, DEPLOYED SOLUTIONS**
Authentication, authorization	Public Key Infrastructure (PKI) for digital certificate management [vs. proprietary IDs, system-wide static keys]
Data/channel privacy	NSA Suite B encryption standards, Advanced encryption standards (AES) 128/192/256, Transport Layer Security (TLS), Internet Protocol Security (IPsec) [vs. proprietary encryption/scrambling]
Data integrity	Hashing via SHA1, SHA256, HMAC-SHA256-80 algorithms [vs. simple cyclic redundancy checks (CRCs)]
Viral attack resistance	Least-privilege design, admission control [vs. assumption of device integrity]
Insider threat protection	Layered authorization [vs. assumption of trust]
Alerting	SNMP (Simple Network Management Protocol)traps, email, SMS messaging, smart phone applications
Auditing	Time-stamped activity logs, change logs



PROTECTING THE AMI LAYER	
Threats	**Mitigation Plan**
Radio subversion	Use of digital signatures and authentication of the source of firmware
Network barge-in	Use of least-privilege design, admission control and hashing algorithms
Denial of service	Use of frequency hopping, digital signatures, and device authentication
Credential compromise	Use of cryptographic authentication with key rotation
Back office compromise	Use of physical security, authentication, role-based privileges and network access control (firewalls)
Cloning	Use of digital signatures and strong authentication
Migration	Use of authentication and unique media access control (MAC) addressing
Meter/Comm module interface intrusion	Use of digital signatures, device authentication and tamper detection

HAN SECURITY CHECK LIST

From the HAN perspective, the following key activities can assist in securing the network and customer privacy.

- ✓ HAN devices do not have direct access to AMI network
- ✓ All service commands in the NAN require a valid AMI security certificate for authentication and a valid role in the certificate for authorization
- ✓ ZigBee (specification for high-end communication protocols) code is part of the AMI meter firmware of the communications module and has all the security protections including image signature, verification, and secure upgrade commands.
- ✓ HAN-related sensitive information (for example, ZigBee private keys) can be stored encrypted in the meter flesh
- ✓ Additional logging capabilities exist beyond the recommendations specified by ZigBee Smart Energy Profile (SEP) standard 1.0

is only breakable with the encryption key. Even if a hacker were to put a listening device onto the network, the encryption would prevent him/her from understanding the data. At the lower layers (layer 1 and layer 2), with a Carrier Ethernet implementation, there is no exchange of information. All of the connections are pre-determined and provisioned from a secure network manager. As such, a hacker cannot spoof the system without a media access control (MAC) address, routing table or other necessary applications. Even a very sophisticated user might try to insert a number of control messages as a DoS attack. However, robust Carrier Ethernet equipment guards against this possibility and limits the number of control messages to the central processing unit (CPU), thus preventing any impact from such an attack.

Conversely, if an IP/MPLS element is put into the access network, it might be vulnerable to spoofing attacks as it does exchange information

MYTHS vs. REALITY	
The Smart Grid creates new security vulnerabilities	The Smart Grid improves security
No one is paying attention to security	Years of work on standards-based security (NERC CIP, AMI-SEC), design to a "40-year threat model"
They're putting the power grid on the internet. It'll be hacked like my cousin's Yahoo account	IP-based private networks are not "the Internet"; rather, they leverage years of proven technology and operational best practices and controls
Anyone can add a rogue device to the power grid	Devices are individually authenticated with strict admission control, behaviour dictated by policy management, and actions authorized using strong encryption signatures
Someone hacked a meter	Legacy devices are indeed insecure; modern devices erect barriers using HW/FW (half wave/full wave) best practices such as secure key storage
Someone created a worm/ virus	Legacy networks may be insecure; modern networks erect barriers using end-to-end authorization to prevent viral command propagation and signed FW-secure booting to prevent rogue FW from entering the system
The Smart Grid is built on new, unproven technologies	The Smart Grid actually improves security by leveraging well-established industry standards and by significantly utilizing remote monitoring and control capabilities.

with nearby routers. A general purpose Ethernet switch (not a Carrier Ethernet device) is also vulnerable to MAC table spoofing or broadcast storms that could overload the equipment and cause an outage. Utilizing the lower layers of the OSI stack in conjunction with Carrier Ethernet equipment provides a much more secure and robust network that is needed for these mission-critical services.

In fact, the Ethernet-centric communication networking approach has proven so secure that it falls within the NERC Critical Infrastructure Protection (CIP) exemption for non-routable protocols. The North American Electric Reliability Corporation (NERC) defines and enforces reliability standards for North America's bulk power system. NERC's CIP standards are meant to safeguard the power grid from cyber attacks.

> **"Today, there are communications solutions available that allow utilities to build the optimum infrastructure"**

THE CONSUMER'S ROLE

Up to this point, we've focused on securing the smart meter and AMI as data is retrieved and transported over the communications network. But we should also think about the consumer's role in establishing a secure smart meter environment. Customers should have access to historical usage data and billing data for a reasonable period of time via a utility-provided web portal. Not only does such a portal provide valuable real-time usage information, it also helps consumers spot abnormalities in data, which can then be brought to the attention of the utility. And customer authorization should be required before any third-party can gain access to meter data. Third-party use of meter data should be limited to the specific purposes disclosed by the third party to the customer.

FACING THE CONSEQUENCES

In February 2012, the U.S. Congressional Research Service published a report entitled, *"Smart Meter Data: Privacy and Cyber Security"*. As if the business reasons for securing smart meter data weren't sufficient enough, this report made clear that U.S. federal privacy and cyber security laws may apply to consumer data collected by residential smart meters. This data may be protected from unauthorized disclosure or access under the Stored Communications Act (SCA), the Computer Fraud and Abuse Act (CFAA) and the Electronic Communications Privacy Act (ECPA).

Authors of the smart meter privacy and security report also state that consumer data may be subject to Section 5 of the Federal Trade Commission (FTC) Act. The FTC has recently focused its consumer protection enforcement on entities that violate their privacy policies or fail to protect data from unauthorized access. This authority could apply to electric utilities in possession of smart meter data.

In Canada, the provincial privacy commissioners are tasked with responding to consumer complaints regarding possible infringements to the applicable privacy law. At the heart of current Smart Grid privacy discussions is a set of core principles, which states that the consumer should have the ultimate authority over access and usage of their own energy-related data.

The Ontario Information and Privacy Commissioner has set out a series of "Privacy by Design" principles for the Smart Grid. The Ontario Smart Grid Forum, an advocacy body for the development of Smart Grid technologies, has formally recognized these principles as crucial to the development of Canada's Smart Grid system. These principles broadly apply to Smart Grid development across Canada. Legislators and regulators need to consider the precise instruments and mechanisms by which such principles should be applied and enforced.

LAST LOOK

Securing the AMI and protecting customer data is critical to the continued adoption of smart meters. Today, there are communications solutions available that allow utilities to build the optimum infrastructure, one that offers the connectivity, reliability and security that is required. I encourage you to look closely at those solutions.

Finally, I want to clarify, contrary to the rumors, AMI/Smart Grid implementation is indeed elevating the conversations and concerns over security and, as a result, has mobilized an industry-wide effort to secure North America's power grid. The *"Myth vs. Reality"* sidebar provides a contrast between common security misconceptions with their actual truths. ET

John Chowdhury is the utility practice director at Fujitsu Network Communications,Inc., where he develops unique network integration solutions and modernization programs tailored to support utilities as they adapt their communications networks to meet new demands for scalability, reliability, standards and security.

COMMENTS: john.chowdhury@us.fujitsu.com