Interoperability and Security for Converged Smart Grid Networks

Andrew K. Wright
N-Dimension Solutions, Inc.
9906 Brightling Lane
Austin, TX 78750
andrew.wright@n-dimension.com

Paul Kalv
City of Leesburg Electric Utility
2010 Griffin Road
Leesburg, FL 34748
Paul.Kalv@leesburgflorida.gov

Rodrick Sibery
Spectrum Engineering
5524 N. County Line Rd
Auburn, IN 46706
rlsibery@spectrumeng.com

Keywords: converged networks, cyber security, interoperability, WiMax, Fiber-To-The-Premise, FTTP

Abstract

This paper investigates interoperability and cyber security issues that arise with the use of *Converged Smart Grid Networks* in distribution utilities. Due to the interoperability proffered by IP, several progressive utilities are considering placing control communications such as Advanced Metering Infrastructure (AMI) and Distribution Automation (DA) on the same network that is also used to offer other services, such as utility Intranet and residential customer broadband. Two case studies of planned AMI and DA deployments, one using Fiber-To-The-Premise and the other using WiMax with a fiber backbone, are analyzed to determine cyber security risks and requirements that arise from AMI and DA communications being carried over the same infrastructure that is used to deliver residential broadband, voice, video, and public Internet services. Directly applying typical best practices for secure control system design such as NIST SP800-83 is not possible, because these best practices call for the control system network to be physically separated from the corporate network. Instead, strong logical separation of network traffic must be achieved using appropriate networking protocols, security tools, and defense-in-depth architecture. This paper examines the challenges that arise in implementing strong logical traffic separation for converged smart grid networks and explores potential solutions.

1. INTRODUCTION

Throughout North America, many utilities are currently deploying new Smart Grid technologies that require two-way communications with devices in the field. Examples are Advanced Metering Infrastructure (AMI) for reading Smart Meters, Demand Response (DR) systems for controlling customer loads, Distribution Automation (DA) technologies that include controllable capacitor banks, voltage regulators, and motor operated switches, and upgrades and extensions of existing Supervisory Control And Data Acquisition (SCADA) systems. Some of the most progressive distribution utilities are planning to select implementations of these technologies that are based on Internet Protocol (IP), and to deploy these technologies in concert with upgrading their communications infrastructures to high-speed *Converged Smart Grid Networks* that will provide AMI, DR, DA, and SCADA communications over the same infrastructure that also provides data, voice, and video. The interoperability proffered by IP has enabled converged networks that provide both data and voice to become common in businesses, and a variety of "triple play" providers currently offer residential data, voice, and video on converged networks. However, converged smart grid networks that include utility communications for AMI, DR, DA, and SCADA are – so far – rare. Interoperability is a fundamental principle of converged smart grid networks, but it must be achieved together with strong cyber security.

Cyber security for *control systems*, of which AMI, DR, DA, and SCADA are examples, is a significant and current concern [2]. Best practices for secure control system design [1][3][4][5] generally call for a control system network to "be logically separated from the corporate network on physically separate network devices" [1]. However, the essence of converged smart grid networks is that control traffic is carried by the same networking infrastructure that carries other traffic, so direct application of traditional best practices for control system security is not possible. Instead, strong logical separation between control traffic and other traffic must be achieved using appropriate networking protocols and security tools.

In the remainder of this introduction, we discuss the implementation plans to deploy converged smart grid networks of two municipal distribution utilities that were awarded Smart Grid Investment Grants in 2010 under the American Reinvestment and Recovery Act. Section Two describes the traditional approach to building a secure control system network, and outlines the structure of a converged smart grid network. Section Three discusses

interoperability for converged smart grid networks, and Section Four discusses various approaches to achieving logical separation between different types of traffic at different networking layers in a converged smart grid network.

1.1. WiMax with Fiber Backhaul

The City of Leesburg, FL Electric Utility is a municipal distribution utility located in central Florida approximately 40 miles north-west of Orlando. Leesburg serves approximately 23,000 electric locations of which 16,300 are active residential and 3,200 are commercial customers. The system includes a control center and five distribution substations, and covers a service territory of fifty square miles. The City also owns an extensive communications network consisting of 185 miles of 96-strand fiber that link city hall, the police department, library, several fire department locations, the electric operations center, five substations, all public school schools in the County, and various commercial enterprises. The City also provides natural gas, water and wastewater utility services to customers in and around Leesburg.

During 2007, Leesburg identified rapidly rising wholesale power supply costs, particularly the demand component of the monthly power bill, as a priority problem to be corrected. Leesburg deployed a 120 meter Advanced Metering Infrastructure pilot during January 2008 and commissioned a Business Case Study to identify the benefits and costs associated with full deployment of the new meter technology. Leesburg's residential rate was the fourth most expensive in the state of Florida during 2008 and the utility had a less than stellar outlook reported by the three major bond rating agencies. Today, Leesburg's residential rate is below the average of 34 municipal utilities in Florida, reserves are significantly improved, and the rating agencies have recognized the improvement and are reporting the equivalent of A+ for Leesburg's bonds.

With the early 2009 announcement of ARRA funding for Smart Grid technologies, Leesburg expanded the AMI initiative to include elements of Distribution Automation, Integrated Distributed Generation, and Demand Response strategies designed to engage consumer participation to reduce peak demands and share the savings with participating customers.

Leesburg received one of the 100 ARRA Smart Grid Investment Grants awarded during the fall of 2009, and will receive $9.7M in matching funds to deploy new Smart Grid technologies. Much of the proposed $20 million budget will be used as early as next year to replace about 23,000 existing meters with AMI Smart Meters that will wirelessly report energy usage every 15 minutes. All single-phase meters will also include a remote connect/disconnect service switch, enabling prepay as a billing option. Programmable communicating thermostats and electric water heater controllers will be made available to customers who switch to a Time Differentiated rate schedule or choose to participate in a DR program. Leesburg's SGIG application was identified by Kurt Yeager (former head of EPRI and now leading the Galvin Electricity Initiative) as one of the fewer than 20 "best" DOE funded SGIG projects.

Initial DA capabilities will include remotely controlled capacitor banks and voltage regulators placed along distribution feeders to optimize voltage control and power quality along the length of the feeders. Motor operated switches will enable rerouting of power flows in the distribution network, enabling load balancing, isolation of damaged line sections, and automated service restoration. Communicating faulted circuit indicators placed along lines will enable more rapid location of faults and improve outage restoration activities.

To provide communications to all the new AMI meters, demand response devices, and distribution automation equipment, Leesburg is considering deploying WiMax [12] base stations throughout its service territory, with backhaul provided over its extensive fiber network. Base stations would be sited at the five substations, as well as additional locations as needed to ensure universal coverage by at least two base stations. The fiber network would be reconfigured as a Gigabit Ethernet redundant ring or partial mesh reaching all WiMax base stations and City facilities. The existing SCADA network that communicates with substation IEDs using a serial protocol over point-to-point fiber will be upgraded to use the new high-speed Ethernet fiber backbone.

Many other uses are envisioned for the high-speed fiber/WiMax network. Leesburg already uses its existing Intranet to control several backup generators to reduce expensive power purchases during peak periods. The availability of high-speed fiber at the substations will enable deployment of IP-based security cameras and electronic access control. Via WiMax, mobile workforce connectivity for electric service personnel would enable workers in the field to access corporate Intranet resources as well as see the status of the entire distribution system in real time. Mobile workforce connectivity would also be made available to other city departments, such as police, fire, and ambulance. Further in the future, WiFi hotspots and residential broadband could be offered over WiMax and/or fiber to residents, thanks to a grandfather clause held by Leesburg in Florida state law that would otherwise prevent this.[1]

[1] Eighteen states have enacted barriers to make it difficult for municipalities to build publicly-owned networks; see http://www.muninetworks.org/content/community-broadband-preemption-map for details.

1.2. Fiber-To-The-Premise

The City of Auburn, IN Electric Utility is a municipally owned utility serving approximately 6,110 residential customers and 773 commercial and industrial customers. The system includes two interconnections at 138 kV, a 69 kV sub-transmission loop, and six substations, and covers a service territory of fifteen square miles. Through Auburn Essential Services, a department of the Auburn Electric Department, the City also owns an extensive Fiber-To-The-Premise (FTTP) network consisting of 185 miles of 96-strand fiber that link city hall, the police department, library, several fire department locations, the electric department, the six substations, schools, and various commercial enterprises. In addition to these critical infrastructure locations the network also provides Internet, data network, voice and data center co-location services to business and residential customers in the Auburn Service Territory.

Earlier this year, Auburn was awarded one of 100 ARRA Smart Grid Investment Grants, and will receive $2.1M in matching funds to deploy new Smart Grid technologies. Much of the proposed $4.2 million budget will be used as early as next year to provide 6,883 customers with AMI Smart Meters that will utilize the FTTP network to report energy usage every 5 minutes. The City plans to enhance the existing Government site to allow customers to view their energy usage on a real time basis. Enhancements will also include the ability of the customer to set limits/targets for energy consumption and receive alerts based on those settings. Tools will also be available for the customer to understand how energy is used in the home or business to help them use energy in a more efficient manner. The meters will have the capability for communication with programmable thermostats and electric water heater controllers, and this demand response program will be offered on an opt-in basis.

Electric infrastructure upgrades will also include new Distribution Automation capabilities. Remotely controlled capacitor banks and new microprocessor based feeder relays will enable Auburn Electric to optimize voltage control and power quality along the length of each distribution feeder. Motor operated smart switches and reclosers will enable rerouting of power flows in the distribution network, enabling load balancing and automated service restoration. Integration of the UMS SCADA system, ESRI GIS and AMI meter data will assist with coordinating response and restoration to outages throughout the system.

To provide communications to all the new AMI meters, demand response devices, and distribution automation equipment, the city intends to utilize the existing fiber-to-the-premise network to connect all the way to the meter. The meters will also utilize a mesh network to provide redundant coverage for all meters throughout the network.

2. SECURE CONTROL SYSTEM DESIGN

Cyber security for utility control systems, such as SCADA, AMI, DR, and DA, is a current and significant concern [2]. A comprehensive approach to cyber security requires both perimeter and interior network security, endpoint security, monitoring, policies, procedures, training, physical security, and other elements. In this paper, we will focus primarily on network security, and begin our discussion with perimeter network security.

Best practices for secure control system design [1][3][4][5] generally call for a control system network to be logically separated from the corporate Intranet on physically separate network devices and separately secured. Logical separation of traffic is best achieved using firewalls, cryptographic Virtual Private Networks (VPNs) such as IPsec and SSL, application proxies, and other cyber security technologies to provide a single point of connection to the corporate Intranet through a DeMilitarized Zone (DMZ). Similar to the Internet DMZ that insulates the Intranet from the Internet and offers web services, a Control DMZ provides highly controlled connectivity between control system servers and Intranet systems. Figure 1 sketches a typical utility control system network that follows this design and provides SCADA communications to substations and AMI communications to Smart Meters.

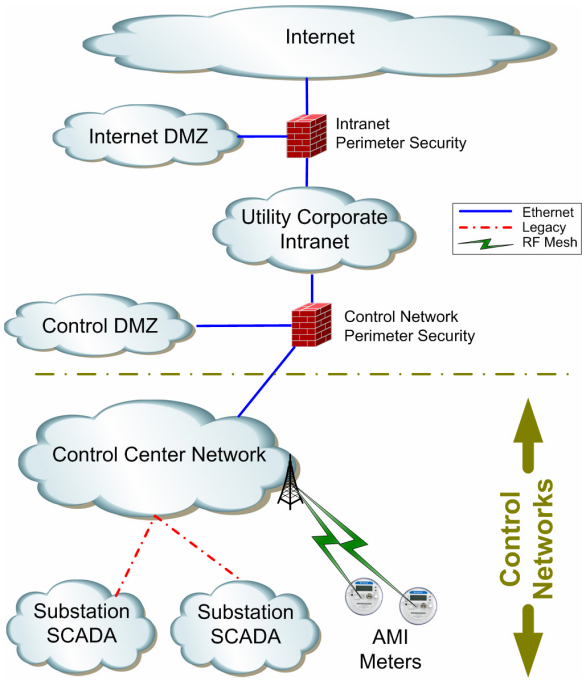

Figure 1: Secure Utility Network

In Figure 1, the Control Center includes SCADA master servers, operating stations, AMI head end systems, and

communications equipment. Communications from SCADA master servers travels over dedicated modems, radios, wires, and/or fiber to reach field equipment such as IEDs, RTUs, and relays in substations. Communications with AMI Smart Meters travels over special purpose wireless networks that typically use RF mesh technologies. As indicated by the broken line in the figure, all control networks are separated from the higher-risk utility Intranet, and consequently control traffic is kept entirely separate from Intranet and Internet traffic.

Placing control system communications on a converged IP-based network offers many advantages over using a collection of legacy and new but proprietary technologies. Taking advantage of state-of-the-art communications and networking technologies, such as Gigabit Ethernet and WiMax, will enable much higher levels of network performance. This will enable more applications to use the network, including new applications as yet unknown. Furthermore, as IP-based networking technologies evolve, the utility will be able to upgrade this network to higher levels of performance. Greater reliability will be possible by deploying redundant paths with automatic rerouting, which can be achieved by any of several widely used switching and routing protocols. Backup paths can be as fast as primary paths, ensuring no degradation in network performance and services when primary paths are out. In short, converged IP-based networks can achieve better speed, performance, and upgradeability, and will over the long term result in lower costs.

Figure 2 illustrates a converged smart grid network, representative of what Leesburg and Auburn are planning. This network will provide a common communications infrastructure for existing SCADA traffic as well as new AMI, DA, DR, physical security, mobile workforce, public WiFi, and even residential broadband, Voice over IP (VoIP), and IPTV.

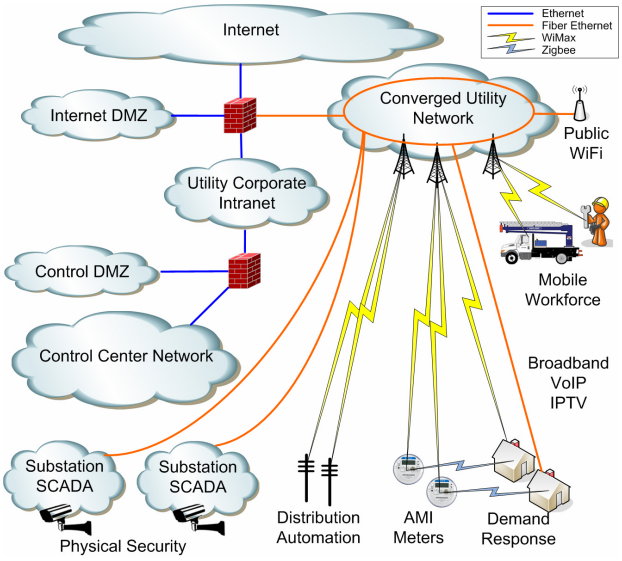

Figure 2: Converged Smart Grid Network

This converged smart grid network will be some combination of fiber Ethernet and wireless, including possibly WiMax, WiFi, ZigBee, 3G cellular, etc., all utilizing IP. For Smart Meters, DA equipment, and mobile workforce systems that use WiMax, the same WiMax base stations will provide connectivity for all of these devices to the fiber backbone. For Smart Meters connected via Fiber-To-The-Premise, the same fiber that provides residential broadband, VoIP, and IPTV will also carry AMI traffic. As a comparison between Figure 1 and Figure 2 clearly indicates, there is no longer a separation between critical control traffic and other uses of the network. Strong logical security will be essential to ensure that highly critical SCADA, DA, AMI, and DR systems and traffic are separated from and not affected by less critical systems and traffic also on the converged smart grid network.

3. INTEROPERABILITY IN CONVERGED SMART GRID NETWORKS

It is hard to imagine how to build a converged smart grid network that unifies SCADA, AMI, DA, and DR traffic on common infrastructure without using IP. The full benefits of using IP become clear when considering all the other services that the network can offer and organizations that the network can serve. Public WiFi hotspots, 4G mobile data services via WiMax and LTE, commercial and residential broadband, voice and video, security services, and many others are all possible due to the interoperability provided by IP. These services are of interest to a municipality not only for its own convenience, but to entice new development and new businesses into the community. By building a converged smart grid network that can support these and as yet unimagined applications, a

municipality will likely find that the cost and effort of building and securing a converged smart grid network will be well repaid.

Using an IP network for utility control traffic requires using SCADA, AMI, DA, and DR protocols that can be carried over IP. DNP3, Modbus, and ICCP, the most commonly used SCADA and DA protocols in North America, all have had IP variants for many years [DNP/TCP, Modbus/TCP, ICCP/TCP]. ANSI C12.22 [42] is a relatively new protocol for AMI communications, and work is currently ongoing in the IETF towards standardization of transport of C12.22 over IP [6]. ZigBee is a relatively new wireless protocol widely expected to be used for Demand Response in Home Area Networks, and support for IP is included in the ZigBee Smart Energy Profile 2.0 currently in development [7]. Thanks to these and other control system protocols that operate over IP, interoperability at the internet layer – meaning getting all these disparate types of traffic onto one converged smart grid network – is reasonably straightforward, and possible with technology available today or in the very near future. Securing the network, however, is not quite so easy.

4. SECURITY IN CONVERGED SMART GRID NETWORKS

We consider techniques of achieving logical separation between different types of traffic across five networking layers: the *physical* layer, the *link* layer, the *internet* layer, the *transport* layer, and the *application* layer. The link, internet, transport, and application layers are the four layers of the Internet Protocol Suite [23]. While usually not part of the Internet Protocol Suite, we also include a *physical* layer to capture important issues arising from the geographically distributed nature of the components comprising a converged smart grid network.

At times we find it helpful to consider impact on the following security properties: *availability*, *integrity*, *confidentiality*, *authentication*, and *access control*. The first three – availability, integrity, and confidentiality – are the classical properties for data security. *Confidentiality* refers to the concealment of information or resources; *integrity* refers to the trustworthiness of data or resources, and *availability* refers to the ability to use the information or resource desired [9]. The relative importance of confidentiality, integrity, and availability is reversed in control systems from that of typical enterprise applications. *Authentication* refers to whom or what is accessing the data or service, and *access control* refers to who is permitted to do what with the data or service. We include authentication and access control separately because of their particular importance in control applications.

For the most part, we limit our attention to WiMax and Gigabit Ethernet over fiber, but our analysis should extend easily to other technologies. Our focus is on technologies that are available or very nearly available today, and that are affordable and available in appropriate form factors for deployment by a distribution utility in small data centers, substations, and outdoor enclosures.

This analysis must be considered preliminary. We hope to develop more detailed analyses and best practices for solutions as we gain experience with converged smart grid networks.

4.1. Layer 1 - Physical Layer

At the physical layer, a typical municipal fiber network consists of cables containing a large number (e.g. 96) of fiber strands run through buried conduit, passive interconnection points such as patch panels, active interconnection points where optical signals are converted to and from electronic signals, core routing and switching equipment, and management systems. A WiMax network consists of base stations that include radio and interface hardware, towers and antennas for base stations, access points that may be standalone radios or embedded into devices such as meters, and various management systems.

Regardless of the communications technologies used, any network covering an area the size of a distribution utility will consist of many interconnection points. For fiber and WiMax networks, these include:

- the Smart Meter to Optical Network Terminal (ONT) connection which is protected only by a plastic box on the outside of the residence;
- the ONT to fiber connection which is protected by the same plastic box;
- for external WiMax radios not located “under glass”, the connection between the Smart Meter and the radio is likely located in a similar box;
- connections between equipment inside pole-top enclosures;
- connections between equipment within WiMax base stations;
- outdoor fiber patch points, which may be located in curb-side pedestals or junction boxes, or underground;
- indoor fiber patch points, which may be located in utility closets in various city facilities, schools, and other buildings;
- Optical Line Terminal (OLT) to fiber connection points, which may be located in data centers;
- indoor fiber switching and routing points, which may be located in utility closets in various city

facilities, schools, and other buildings or in data centers.

Physical security measures such as padlocks, electronic badge systems, cabinet locks, and video security can deter but not completely prevent cyber security breaches at these interconnection points. It is generally impractical to strongly secure all but the most key interconnection points.

Using different fibers within a fiber bundle for different kinds of traffic prevents an attacker with access to only one fiber from affecting the traffic on other fibers. However, there are often many interconnection points such as patch panels where all fibers of a bundle are terminated at the same location. For these locations, physical security is particularly important to deter malicious attacks. Change management procedures and policies for personnel with access to these locations are also important to prevent accidental interruption of critical control traffic. Electronic badge access or cabinet "door open" sensors can help ensure that these procedures and policies are followed.

Eavesdropping on traffic carried in optical fiber is reasonably straightforward and can be carried out without splicing by bending the fiber and intercepting a small fraction of light that escapes at the bend [8]. This can be performed with equipment that is available for less than $1,000 USD.

Eavesdropping on and forging false wireless signals is straightforward. Frequency hopping and spread spectrum techniques offer zero security because making the network available for many different uses means the channel hopping scheme must be made public.

WiMax can be deployed on both licensed and unlicensed spectrum. Using licensed spectrum can help assure availability, but in this era of global commerce, it is not difficult for an attacker to obtain a radio or development kit that can operate on a licensed band.

The above considerations dictate that physical layer properties alone should not be relied on to provide sufficient security for critical control traffic in a converged smart grid network. Nevertheless, physical defenses such as mentioned above should be employed to protect the network infrastructure from attacks that may indirectly compromise logical traffic separation implemented by higher layers.

4.2. Layer 2 – Link Layer

WiMax 802.16e-2005 can use AES encryption with CBC mode to encrypt all traffic transmitted between the mobile subscriber and the base station, and CBC-MAC [13] to ensure integrity. These methods are approved by NIST for use in Federal systems, and NIST offers guidance on appropriate use of cryptography in WiMax [14]. Properly configured, integrity and confidentiality protection for WiMax traffic at the link layer is quite strong.

On an Ethernet [31] network, fiber or otherwise, packets are transmitted "in the clear" at the link layer. Ethernet packets carry a Cyclic Redundancy Check (CRC) that is intended only for detecting transmission errors. This mechanism affords no security against an adversary modifying or forging a packet. Consequently, Ethernet offers no protection of confidentiality or integrity against a malicious adversary.

The original Ethernet specification was a broadcast channel, and any station could receive traffic transmitted by any other. Ethernet hubs provide essentially the same behavior for point-to-point links, broadcasting a packet to all other links. Consequently, converged smart grid networks should avoid use of hubs. However, CAM table attacks [21] can cause a switch to broadcast all packets to all links, just like a hub. Consequently, switched infrastructure should not be relied on for secure separation of traffic.

VLANs [11] allow separation of packets into different logical channels within the same physical Ethernet link. A host on one VLAN cannot direct packets to a host on another VLAN, and thus cannot send forged or modified packets to that host, unless the VLANs are routed together. VLANs are useful for controlling broadcasts, for quality of service differentiation, and as a layer of separation between different groups of hosts. However, a number of "Layer 2" attacks [21] can subvert VLANs and allow an attacker to compromise the separation of VLANs. Preventing these attacks requires configuring several different defenses carefully and precisely across all switches in the entire infrastructure [15][22]. Even with these defenses in place, VLANs are usually routed together, either by core routers, or by "layer 3 switches" that automatically route all connected links together. Consequently, either this routing must be disabled, or Access Control Lists (ACLs) must be deployed uniformly across every switch to separate different networks. The complexities and pitfalls of VLANs for logical traffic separation make relying on VLANs alone for logical separation risky, but they are a valuable tool as one layer of defense.

Network Access Control (NAC) refers to controlling authentication and admission to the network, and can optionally be implemented on Ethernet by using IEEE 802.1X [17]. Today, 802.1X is widely used on 802.11 WiFi networks. IEEE 802.1X can also associate traffic from authenticated users and devices with specific VLANs. Thus a device authenticated as a Smart Meter could be placed into a Meter VLAN, a user authenticated as a utility employee could be placed into the Utility Intranet VLAN, and all devices not otherwise authenticated could be placed into a Public Access VLAN. There are serious vulnerabilities with

the 2004 version of 802.1X that have been corrected in the recently approved 802.1X-2010 specification. Support for 802.1X is limited in control system equipment, and using such equipment directly on a network running 802.1X may require using whitelists of MAC addresses, which is relatively weak. Alternatively, control system equipment located at substations that does not speak 802.1X can be placed on a local substation network connected through a security gateway. Management of 802.1X can be complex and challenging, but nevertheless controlling access to the converged smart grid network is a valuable defense, particularly for FTTP networks where network access points are highly exposed.

The Trusted Computing Group [25] is developing an architecture called Trusted Network Connect that extends 802.1X Network Access Control with endpoint posture assessment. Proprietary solutions to endpoint posture assessment have existed for some time. It is likely to take some time for the market to adopt interoperable solutions to endpoint posture assessment, and still longer until Smart Meter, FTTH, and DA products support these capabilities.

Physical switch ports can be associated with specific VLANs, so that devices connected to them are placed into those VLANs. Various switch configuration options can lock a port if more than one MAC address is seen on that port, or if the MAC address changes [33]. MAC addresses are easily spoofed, but switch port security can provide a weak measure of network access control if 802.1X is not implemented.

Similar to 802.1X, WiMax uses PKMv2 with EAP [18][19] to authenticate users and devices to the network. Devices such as Smart Meters and DA equipment that do not have users will use device authentication only, and EAP-TLS is well-suited and provides strong security for this purpose. Network authentication is mandatory in WiMax.

Both 802.1X and PKMv2 can use Authentication, Authorization, and Accounting (AAA) backend servers running the RADIUS [28] or DIAMETER [29] protocols, ensuring interoperability for management of network authentication.

With multiple types of traffic carried on a converged smart grid network, Quality of Service (QoS) is important to ensure that critical control traffic is not delayed by less critical traffic. WiMax supports five levels of QoS to allow different packets to be given different service. Ethernet VLANs, as defined in IEEE 802.1Q [11], support eight different Class of Service (CoS) markings [10] in the 802.1Q header to carry QoS information. Delay sensitive control traffic should use these mechanisms where appropriate.

Any link layer methods of achieving logical traffic separation are forfeit if an attacker can gain administrative access to a switch. The distributed nature of a converged smart grid network makes out-of-band management impractical, and consequently secure in-band management is essential. Switch security varies by manufacturer and model, but most switches require a number of configuration options be set appropriately to properly secure the switch [33][34].

4.3. Layer 3 – Internet Layer

Firewalls are frequently used to protect networks and network segments. Firewalls range from stateless packet filter firewalls, to application layer firewalls that are aware of certain protocols, to stateful firewalls that keep track of connections, to deep packet inspection firewalls. Today, most standalone firewall products are stateful firewalls. Firewalls can be used to block or route traffic based on source IP address, destination IP address, port number, and other IP header fields, and thus can serve as a means of logically separating traffic. However, source IP addresses are easily spoofed. IP source verification features in switches and routers can defend against source IP spoofing for packets originating from directly attached devices, but ensuring that all switches and routers in the network are properly configured for this can be challenging. Firewalls are therefore a valuable tool for ensuring separation of traffic, but should be considered only as one layer of defense.

Many network switches implement Access Control Lists (ACLs) that can implement some of the functionality of firewalls and can thus be used to separate traffic. However, ACLs must be deployed uniformly and pervasively across all switches in the infrastructure to ensure separation, and the complexity of managing the many configurations is high. Like firewalls, ACLs are therefore a valuable tool for ensuring separation of traffic, but should be considered only as one layer of defense.

Multiprotocol Label Switching (MPLS) [30] is a protocol used by large carriers to deploy Virtual Private Networks (VPNs) between branch offices of customers while keeping those customers networks logically separate. It relies on Virtual Routing and Forwarding (VRF) technology, in which a router contains multiple independent routing tables, and can thereby separate and route different traffic flows independently. Traffic in an MPLS VPN is not cryptographically protected, but is logically separated by the labels in the MPLS headers of packets. Consequently, MPLS security crucially relies on physical security of all routers and intermediate connection points in the MPLS network. In this sense, the security of MPLS is similar to that of VLANs in terms of providing logical traffic separation. There do appear to be fewer attacks currently

known against MPLS [32] than against VLANs that can break logical traffic separation. MPLS support tends to be limited to high end routers intended for data center deployment. Provided that appropriate equipment for field deployment can be found, MPLS could be a valuable tool as one layer of defense, but it requires support for VRFs, MPLS, and usually iBGP in the network routers, as well as significant networking expertise to deploy and manage.

VRF-lite refers to using VRF technology without MPLS. With this approach, separate logical routed networks can be built up over a network of routers. VRF configuration must be performed on every router, so this approach does not scale well to large carrier environments. However, for a typical distribution utility, the number of routers in the network is generally small enough to make VRF-lite feasible without the management complexity of MPLS. As with MPLS, security crucially relies on physical security of all routers and intermediate connection points in the network, as well as correct configuration of all routers. More routing products are available that support VRFs alone than support both VRFs and MPLS, but support still tends to be limited to high end equipment. Provided appropriate equipment for field deployment can be found, VRF-lite could be a valuable tool as one layer of defense to separate networks.

IPsec [27] is an open suite of Internet Layer protocols that can establish secure tunnels across multiple switching and routing hops to assure the security of traffic carried in those tunnels regardless of intermediate connection points. IPsec can carry most types of IP traffic. IPsec includes a variety of cipher suites and modes for encrypting traffic, verifying the integrity of traffic, and authenticating users and devices. Specific modes are negotiated by the Internet Key Exchange (IKE) protocol. IKE version 1 has a number of flaws and vulnerabilities that are addressed by IKE version 2 [26]. With proper selection of cipher suites and modes, IPsec can provide strong logical traffic separation.

DiffServ [20] is a mechanism for classifying traffic and providing quality of service guarantees. DiffServ uses the Differentiated Services Code Point (DSCP) field in the header of an IP packet to assign up to 64 different classes of service. DiffServ can carry comparable information to the CoS field of an 802.1Q VLAN header or the QoS profile of a WiMax packet, but by carrying this in the IP header of the packet, the DiffServ QoS information can be carried across routed networks. Translation to and from DSCP markings should be performed if routing is used in the converged smart grid network to ensure that quality of service is preserved end to end.

DiffServ is also useful when traffic with QoS markings is placed in IPsec and other types of tunnels. When a packet is placed into an encrypted tunnel, the header of the encapsulated packet may be encrypted, and thus QoS markings on the encapsulated packet cannot be respected by the routing and switching infrastructure. With appropriate configuration at the tunnel entrance, DSCP markings on the encapsulated packet can be copied to DSCP markings on the encrypted packet. Cisco calls this “QoS pre-classification”; other vendors have different ways of achieving the same result. Preserving QoS markings on encrypted traffic should be used wherever control traffic is encrypted, to ensure it retains appropriate priority and quality of service.

Any internet layer methods of achieving logical traffic separation are forfeit if an attacker can gain administrative access to a router. The distributed nature of a converged smart grid network makes out-of-band management impractical, and consequently secure in-band management is essential. Router security varies by manufacturer and model, but most routers require a number of configuration options be set appropriately to properly secure the router [36].

4.4. Layer 4 – Transport Layer

The transport layer of the Internet Protocol Suite provides several transport protocols offering differing delivery guarantees. The primary transport protocols in common use are TCP, UDP, DCCP, and SCTP. While all of these protocols provide multiplexing of different traffic flows between two hosts, the logical separation provided by the transport layer is not intended to guard against malicious attacks by a determined adversary. TCP provides a modicum of data integrity protection provided the provisions of RFC 1948 [35] are in place on all hosts, but there are several other attacks against TCP that can lead to data integrity compromise. None of the transport protocols provides confidentiality protection. For these reasons, the transport layer protocols offer little help in achieving strong logical traffic separation.

4.5. Application Layer

Applications can implement various cryptographic techniques independent of the network to protect their traffic streams. From the standpoint of the application, end-to-end encryption and authentication offers the strongest guarantees of confidentiality and integrity between components of an application, since this ensures security of application traffic regardless of intermediate connection points. For example, end-to-end encryption and authentication between an AMI system head end and the meters in the field protects the confidentiality and integrity of billing data and remote disconnect commands regardless of attacks against mesh collectors or backhaul networks. Below, we discuss several application layer protocols that can be used to protect critical control system traffic. Throughout this discussion, it is important to bear in mind that these protocols offer no help in ensuring that

communications remain *available*. Availability – the most important characteristic required of a control system – can only be assured by techniques implemented at lower layers in the network, such as discussed in previous sections, that logically separate control system components, and deny attackers the opportunity to launch Denial Of Service attacks, exploit vulnerabilities in applications and operating systems, guess passwords, etc. Put another way, cryptographic protocols implemented in applications protect against compromises of the network; while cryptographic protocols implemented in the network protect against compromises of applications.

TLS [37], which evolved from SSL, provides confidentiality and integrity protection for TCP streams, together with user and device authentication. DTLS [38] provides similar protection for UDP traffic, and can also be applied to DCCP traffic [39]. As with IPsec, TLS and DTLS support multiple cipher suites and modes. TLS authentication is usually based on certificates. As used in HTTPS, TLS authenticates only the server, but the protocol also provides for client – and thus mutual – authentication. Both TLS and DTLS can be built into applications, such as browsers that encapsulate HTTP traffic in TLS to implement HTTPS connections. Implemented in applications or operating system services, and with proper selection of cipher suites and modes, these protocols can provide strong end-to-end protection of application traffic.

Due to the flexible layering structure of the Internet Protocol stack, TLS and DTLS can also be used in a recursive way to implement secure tunnels at a lower layer between networking appliances. Used in this way, TLS and DTLS tunnels provide logical separation of traffic similar to that of IPsec.

Several control systems protocols in use in the electric sector incorporate security mechanisms useful for strong logical traffic separation. IEC 62351 [41] specifies use of TLS with mutual authentication for IEC 61850 [40] traffic. Secure DNP3 [43] provides authentication and data integrity but not confidentiality for DNP3 traffic. It can be used for both serial and TCP/IP DNP3 traffic. IEEE P1711 [44] provides integrity and confidentiality for many serial SCADA protocols, but is primarily applicable to serial traffic. A similar protocol known as the Secure SCADA Communications Protocol (SSCP) was developed by the Hallmark Project [45] and provides data integrity and user authentication for serial SCADA traffic. ANSI C12.22 [42] provides confidentiality, data integrity, and device authentication for smart meter communications. Secure DNP3, IEEE P1711, SSCP, and C12.22 are all relatively new cryptographic protocols. While they all use established cryptographic ciphers and building blocks, construction of correct and secure protocols from sound building blocks is well known to be a challenging problem fraught with potential error. Consequently these protocols should be used as only one layer of protection in a defense-in-depth architecture.

5. CONCLUSION

While modern computing and technologies are now widely used throughout control centers and utility enterprise environments, field communications equipment largely uses outdated technologies. By deploying a converged smart grid network, utilities like Auburn and Leesburg can modernize their communications infrastructure, deploy new applications such as AMI and Distribution Automation, and adopt an architecture that is based on standards and supports interoperability based on Internet Protocol. Interoperability will allow them to replace individual subsystems that become out of date as technology evolves, without requiring forklift upgrades. Converged smart grid networks will require strong logical separation of traffic to ensure security of smart grid applications, and this will be best provided by a defense-in-depth architecture that considers security across all layers of the IP stack .

References

[1] Stouffer, Falco, Scarfone, *Guide to Industrial Control Systems (ICS) Security*, Draft, National Institute of Science and Technology SP800-82, Sept. 2008.

[2] The Smart Grid Interoperability Panel, Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, Volumes 1, 2, 3, National Institute of Science and Technology NISTIR 7628, Sept. 2010.

[3] Idaho National Laboratory, *Control Systems Cyber Security: Defense in Depth Strategies*, Homeland Security External Report #INL/EXT-06-11478, May 2006.

[4] *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, National Infrastructure Security Coordination Center, London, 2005.

[5] *TR99.00.01: Security Technologies for Industrial Automation and Control Systems*, ISA, 2007.

[6] Moise and Brodkin, *ANSI C12.22, IEEE 1703 and MC12.22 Transport Over IP*, Internet Draft, August 2010.

[7] ZigBee Alliance, *ZigBee Smart Energy 2.0 DRAFT 0.7 Public Application Profile*, June 2010.

[8] Olzak, *Protect your network against fiber hacks*, TechRepublic 2007. http://blogs.techrepublic.com.com/security/?p=222&tag=nl.e036

[9] Bishop, *Computer Security: Art and Science*, Addison-Wesley, 2002.

[10] *LAN Layer 2 QoS/CoS Protocol For Traffic Prioritization*, IEEE Standard 802.1P, 2004.

[11] *Virtual Bridged Local Area Networks*, IEEE Standard 802.1Q, 2003.

[12] *Air Interface for Broadband Wireless Access Systems*, IEEE Standard 802.16e-2009.

[13] Whiting, Housley, Ferguson, *Counter with CBC-MAC (CCM)*, IETF RFC 3610, Sept. 2003.

[14] *DRAFT Guide to Security for Worldwide Interoperability for Microwave Access (WiMAX) Technologies*, NIST SP800-127.

[15] Cisco, *Virtual LAN Security Best Practices*, Application Note, 2002.

[16] Dworkin, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*, National Institute of Science and Technology SP800-38B, May 2005.

[17] *Port Based Network Access Control*, IEEE Standard 802.1X-2010.

[18] Aboba, Blunk, Vollbrecht, Carlson, Levkowetz, *Extensible Authentication Protocol (EAP)*, IETF RFC 3748, June 2004.

[19] Aboba, Simon, Eronen, *Extensible Authentication Protocol (EAP) Key Management Framework*, IETF RFC 5247, Aug. 2008.

[20] Nichols, Blake, Baker, Black, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*, IETF RFC 2474, Dec. 1998.

[21] FX, *Routing and Tunneling Protocol Attacks*, Blackhat Briefings, November 21 2001, Amsterdam.

[22] Convery, *Understanding and Preventing Layer 2 Attacks*, Cisco Networkers 2003.

[23] Braden, *Requirements for Internet Hosts – Communication Layers*, IETF RFC 1122, Oct. 1989.

[24] *Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations*, IEEE Standard 1613, 2003.

[25] Trusted Computing Group, http://trustedcomputinggroup.org

[26] Kaufman, *Internet Key Exchange (IKEv2) Protocol, IETF RFC 4306*, Dec. 2005.

[27] Kent, Seo, *Security Architecture for the Internet Protocol*, IETF RFC 4301, Dec. 2005.

[28] Rigney, Willens, Rubens, Simpson, *Remote Authentication Dial In User Service (RADIUS)*, IETF RFC 2865, June 2000.

[29] Calhoun, Loughney, Guttman, Zorn, Arkko, *Diameter Base Protocol*, IETF RFC 3588, Sept. 2003.

[30] Rosen, Viswanathan, Callon, *Multiprotocol Label Switching Architecture*, IETF RFC 3031, Jan. 2001.

[31] *Carrier Sense Multiple Access with Collision Detection (CMSA/CD) Access Method and Physical Layer Specifications*, IEEE Standard 802.3-2008.

[32] Ray, *MPLS Security*, Layer One, Sept. 2006.

[33] Borza et. al., *Cisco IOS Switch Security Configuration Guide*, National Security Agency, June 2004.

[34] Cisco Systems, Securing Cisco LAN Switches, SECL 1.0, 2006. http://www.cisco.com/E-Learning/bulk/public/celc/SECL_10/index.html

[35] Bellovin, *Defending Against Sequence Number Attacks*, IETF RFC 1948, May 1996.

[36] Antoine et. al., *Router Security Configuration Guide*, National Security Agency, December 2005.

[37] Dierks, Rescorla, *The Transport Layer Security (TLS) Protocol, Version 1.1*, IETF RFC 4346, April 2006.

[38] Rescorla, Modadugu, *Datagram Transport Layer Security*, IETF RFC 4347, April 2006.

[39] Phelan, *Datagram Transport Layer Security (DTLS) over the Datagram Congestion Control Protocol (DCCP)*, IETF RFC 5238, May 2008.

[40] *Communication Networks and Systems in Substations*, IEC Standard 61850, 2005.

[41] *Power System Control and Associated Communications - Data and Communication Security*, IEC Standard 62351, 2007.

[42] *Protocol Specification For Interfacing to Data Communication Networks*, ANSI Standard C12.22-2008.

[43] *DNP3 Secure Authentication Version 2.0*, DNP Users Group, Aug. 2008.

[44] *Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links*, IEEE Standard P1711, Aug. 2010.

[45] Hallmark Project, 2010. www.oe.energy.gov/DocumentsandMedia/4-Hallmark.pdf

Biographies

Andrew Wright is Chief Technology Officer at N-Dimension Solutions, where he guides the company's technical strategy for development of cyber security products for the electric power sector. He has 20 years of experience in research and development, including 12 years in the area of cyber security. Wright has a PhD in Computer Science from Rice University.

Paul Kalv is Chief Smart Grid Systems Architect at the City of Leesburg, Florida and holds overall responsibility for the implementation of Leesburg's Smart Grid Investment Grant.

Rod Sibery is Project/Operations Manager at Spectrum Engineering and holds overall responsibility for the implementation of Auburn's Smart Grid Investment Grant.