

[Smart Grid Security: Ground Zero for Cyber Security](#)

June 2, 2010 at 12:51 PM by [Larry Karisny](#)

It was pretty amazing to see the amount of people involved in [Conductivity Week in Santa Clara California last week](#). They were all there positioning their expertise on how to build and secure the smart grid. With NIST, WiFi Alliance, Zigbee Alliance, and the IEEE and hundreds vendors and speakers attending, it was like a wireless IP Mecca of intellectuals all contributing to this global energy network requirement. Even the Godfather of the Internet Vint Cerf opened the meeting and ended his keynote speech with a daunting announcement, “One of things incumbent on all of us is to introduce strong authentication into the fabric of the smart grid,” Cerf said. “We did not do that with the Internet.”



“My excuse is public key cryptography not even publically written about until 1977 which is just about when TCP/IP was getting standardized,” Cerf said.”But today we don’t want devices to respond to control from something that’s not authenticated,” he added.

What is the smart grid?

Wikipedia defines it rather well: “A smart grid delivers electricity from suppliers to consumers using two-way [digital](#) technology to control appliances at consumers’ homes to save energy, reduce cost and increase reliability and transparency. It overlays the [electricity distribution grid](#) with an information and [net metering](#) system.” With this definition, why is the smart grid such a security issue?

We need to first look at how our power grid operates today. With a [daunting list of power companies throughout the nation](#), there is no one answer but we can make some generalizations. Power distribution and monitoring today is in its initial stages of becoming a smart grid with some substation network intelligence often connected by microwave, power line and/or fiber optic point to points. Although these core network infrastructures are very basic, they may prove useful in operating the needed private IP backbone of the smart grid. These network backbones were not meant to securely connect two-way digital connections from every home, every building every factory and every energy using appliance throughout the power companies service area. In fact, adding millions of these connections to the power grid distribution system is no easy task in network or network security.



Power companies are in the precarious position of having to do something now while preparing for the future. In my [earlier article, grid security firms and even a past cyber security Czars](#) clearly explained today's power grid vulnerabilities. With [\\$3.375 billion kicked in by the Federal Government](#) and even more funds added by Power and Utility Companies, they need to produce now but only if a smart grid security plan can be demonstrated. This leaves the power companies in a tough position of needing to do something today while being prepared to migrate smart grid security platforms to newer standards. The bottom line is there is no hurry up and wait when it comes to deploying and securing smart grid networks. There is only hurry up and be prepared to hurry up again.

Security problems and how they can be solved

The Smart Grid Network, Smart Grid Operating Center and Back Office are pretty much secure. The problem is when you start connecting smart grid devices to homes, commercial buildings and factories. You have opened up the potential of accessing the smart grid distribution network through millions of smart grid end user access points. This network edge connection is called layer 2 which in the past had limited concern for security. It now has to lock out smart grid end users while also having the capability of running independently and interoperably with throughout the smart grid.



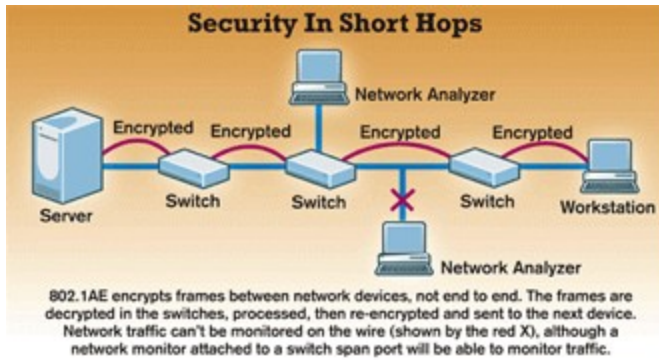
WWII Veteran Ludwig Karisny

In trying to explain the layer 2 security and its importance, this Memorial Day I remembered some old WW II war stories from my father. His Army job was to make field communications work in sometimes impossible situations. These WWII networks were very basic, running wires from fox hole to fox hole (layer 3) then connecting to the wireless fielded radios (layer 2). Even if the wireline connections were cut or if the radio battery died, the battle still went on. If the wires were cut (layer 3) the pre-intelligence was already given from the commanders in the fox hole (layer 2) with the special code commands being conveyed man to man (today's machine to machine, M2M). When I asked my dad what the most important network connection was surprisingly the answer was the radios in the fox holes and the man to man communications. They were able to continue the battle operating in layer 2 and M2M without command layer 3 connectivity. This is how we need to build and secure smart grid networks today.

In a response in my earlier article, [“The Smart Grid needs to get smart about security”](#), Niall McShane, a smart grid consultant commented: “We need to start the process of re-architecting the grid into smaller, localized micro-grids that are loosely coupled in a federation to help balance supply and demand across wider geographic areas which can also island from the macro-grid to prevent the propagation of faults. In this way we move from a single large target that can be attacked and that will then propagate the fault throughout the network to a large number of much smaller targets.”

While micro-grids offer physical network security, a new awareness of the importance of layer 2 security is being becoming recognized. Strong security encryption must reside at the layer 2 network level when you are collecting two-way digital information from the smart grid network edge. Whether you are protecting personal information from the home or stopping potential grid network access from the network home gateway, layer 2 is where this security must reside. There are also additional advantages of security mobility and scalability that can only be offered at the layer 2 level.

These important layer 2 features have also been documented in [a recent white paper Portland: A Scalable Fault-Tolerant Layer 2](#). Just like the WWII soldiers were sometimes connected and sometimes not connected to the communication command center, smart grid edge applications will need to securely and independently migrate applications, computation and storage into local data centers spread across the smart grid edge. With all this intelligence being gathered, encryption latency also becomes an issue. [In a recent white paper from the Rochester Institute of Technology](#) addressing latency testing, layer 2 encryption well out performed the layer 3 latency adding more advantages to targeting security a the layer 2 level.



The 802.1AE standard was designed to protect data in transit on a hop-by-hop basis (see [Information Week article, "New Protocols Secure Layer 2"](#)), ensuring that the frames are not altered between Layer 2 devices such as switches, routers, and hosts. 802.1AE isn't a replacement for Layer 3 security but does ensure that frames are protected from eavesdropping and manipulation at Layer 2 between peers. All traffic passing between two switches is protected using the same security parameters.

There are companies recognizing the importance of layer 2 security with impressive orders starting to come in. Marvell has shipped more than one million ports of 1GE and 10GE link processors powered by first generation Marvell(R) LinkCrypt(TM) technology. Designed to merge Media Access Control (MAC) layer security functions into the Ethernet physical layer, LinkCrypt plays a key role in the integration of standards-compliant security solutions to expand the security perimeter in enterprise, data center, metropolitan networks and 3G/4G cellular infrastructures.

Cities, counties and even atomic plants are working with companies like [TLC-Chamonix](#) adding end-to-end security to their networks. Their premier FIPS 140-2 validated software-based solution is being used to protect wireless networks at the Layer 2 level while also offering the only Mesh certified software solution. With DOD installations in place, TLC-Chamonix is finding that DOE and Government FIPS 140-2 mandates are requiring higher security levels over many enterprise, local, county and critical network infrastructures. Rather than embedded chip sets, TLC-Chamonix offers a vendor agnostic software solution across a variety of network equipment and platforms.

From today's smart grid breaches to tomorrow's smart grid needs, security requirements seem to all be pointing to layer 2 and micro-grids network topologies. Maybe today's smart grid security problems can open the door to a complete new set of cyber security platforms. With billions released to build the smart grid, we should immediately focus the funds and expertise to securing the critical infrastructure of our nation's power grid. Let's make Smart Grid security the ground zero of cyber security.

* * * * *

About the author

Larry Karisny is the Director of Project Safety.org and a consultant supporting local wireless broadband, smart grid, transportation and security platforms. ProjectSafety Business and Technology Cluster researches and deploys leading edge standards based technologies

supporting secure migration paths to current and future wireless networks and network applications.