Wired PLC smart meters are a privacy and security risk

PLC is the most commonly used form of wired communication for electrical meters. Many PLC systems lack basic security precautions, so the meters can be snooped on and hacked into. This means private information can be revealed and terrorists can create long-lasting blackouts.

Keywords: power line carrier, power line communication, wired smart meters, cyber attack, terror attack, privacy, security, PLC, PLT

What is PLC?

PLC stands for power line carrier or power line communication, which is a method where signals travel on the existing electrical wires. These signals create a disturbance in the electricity on the line, which travels into houses and through the power lines along the streets. This disturbance is picked up by a receiver somewhere else on the power line, often several miles away.

PLC is used to communicate with electrical meters in various ways. One way is for the utility to read the electrical consumption remotely, instead of having to send out meter readers.

In some versions, the utility can also instruct the meter to disconnect power to the house, if the bill is not paid or the house is vacated.

Some meters can even have their internal software upgraded by a download through PLC.

Another way an electrical meter can communicate using PLC is to "talk" to appliances inside the house. Some pre-pay meters have a display screen inside the house that shows how much money is left and the present power consumption. Some meters can also use PLC to turn off the water heater, air conditioner, clothes dryer and other appliances if the utility needs to reduce the power consumption.

PLC can be tapped into

There are three basic ways to snoop on PLC signals:

- from a wall socket

- from a coupler on a wire
- wirelessly

The easiest way is to tap an electrical wall socket. The PLC signals create disturbances of the line voltage, which can be displayed using an oscilloscope or decoded using a computer.

The voltage disturbances travel widely, and can go from house to house[1], so a person can pick up the signals from the neighbor's PLC meter via an ordinary electrical outlet.

A second method is to use a current transformer, or a coupler, which is clamped around the wire carrying the PLC signals. This is less convenient in most cases.

The third method is to pick up the signals wirelessly. PLC systems are not considered wireless systems, but the wires will always radiate the signals. Utilities like to say that this isn't true, and the Federal Communications Commission (FCC) apparently believed them, until they actually looked into it[2]. The PLC "antenna effect" is now a well-documented fact[3].

PLC signals may not be encrypted

The PLC vendors and utilities are tight-lipped about their security, as they should be. However, there is various evidence that commonly used PLC meters in the United States are not protected by encryption.

A search of vendor literature for the most common PLC meters in the United States[4,5] did not find any claims of encryption being available. If encryption was available, it would most likely be proudly displayed as a positive feature.

Pacific Gas and Electric (PG&E) in California admitted publicly that they had disabled features in their PLC meters due to security concerns.[6] It was not disclosed whether this was due to a lack of encryption or some other major security flaw, but PG&E did not take the same step for their wireless electrical meters, which do have encryption.

Yet another indicator of a lack of encryption is when the Arizona Corporation Commission issued their draft guidelines for smart meters. The first draft required encryption for all smart meters[7]. The Arizona utilities responded back, requesting that only wireless smart meters should use encryption[8]. If their PLC systems used encryption, why would they make this request? If they were generally opposed to

encryption, then why accept the requirement for wireless smart meters? A few Arizona utilities use the Turtle TS1 and TS2 systems.

A utility in Colorado describes their PLC security as a "natural encryption of information", consisting of "ones and zeros riding the electricity current"[9]. This does not sound like real encryption, using encryption keys, etc. This is more like considering two Swedes talking their own language in a room full of Americans. Yes, the other people in the room would not understand the Swedes, but it is not hard to decode their conversation, if one made the effort.

Decoding the PLC signals

With the PLC signals available, a would-be hacker or terrorist will need a computer, a line filter and a simple interface to start looking at the signals. This is no more than a bright engineering student can figure out.

It will take some effort to decode the signals and figure out how to read them, but there are people who enjoy such a challenge[10]. The movie industry thought their DVDs were copy protected, but it didn't take long before someone figured out how to defeat it. The result is that software to copy DVDs is now widely available.

Important details on how to decode one commonly used PLC smart meter system are already available on the web[11].

Another help in decoding PLC signals is that the PLC signals have to use a meter ID number of some sort. That ID number is typically posted in plain view on the front or sides of each meter.

Decoding these signals is not rocket science. Considering unencrypted PLC signals as "secure" is simply not responsible.

Privacy problems

Once someone has figured out how to decode a PLC system, they will boast about it. There are websites dedicated to this sort of information. Detailed information will be posted, and then others can simply follow the directions.

What can be learned from snooping on a PLC meter varies with how often the meter transmits a reading. Some PLC meters can send as often as every 15 minutes[12].

The Congressional Research Service cites two studies showing that a smart meter reading every 15 minutes is sufficient detail to find out what goes on inside a private home.[13] This includes:

- when people go to bed and wake up
- when food is cooked
- when showering
- when not at home

This kind of information can be used in various ways, including by would-be burglars and abductors, tabloid magazines, government agencies and the insurance industry.

PLC smart meters vulnerable to terror attacks

With the PLC signals available for snooping, and not protected by encryption, the next step for a hacker or terrorist is to also transmit PLC signals. Basic information about PLC signals and their generation is available on the web[11], though experience with electronics and experimentation will be needed.

By monitoring and decoding PLC messages, it is possible to figure out how to transmit instructions to PLC smart meters. With no encryption, this does not require large resources.

A terrorist could then use the PLC system to tamper with the PLC smart meters, creating blackouts or other mayhem.

One method of attack is to instruct each PLC smart meter to turn off the power to the business or household. Pacific Gas & Electric (PG&E) has already realized this vulnerability in their PLC meters, and disabled that feature[6].

Another way to cause mayhem is for the attacker to download bogus software to the smart meters, through the PLC system. This could be used to crash the meter's computer, turning appliances off in the building or other mayhem.

A PLC system is also vulnerable to more primitive forms of attacks, that require less technical expertise. Simple "noise makers" that transmit on the same frequencies as the PLC system can be plugged into inconspicuous outlets in various public places, such as restrooms, stores and libraries. The noise makers would jam the PLC signals so the utility cannot communicate with their electrical

meters. This form of attack is probably not destructive and wouldn't cause power outages, but be a great nuisance for the utility, which would have great trouble locating the noise makers. This form of attack is more likely to be used by demonstrators/protesters.

Attacks on the grid have already happened

The CIA have reported that extortionists have already taken down the power grid in multiple regions outside the United States[14]. The methods and locations were not disclosed. This author is not aware of any actual attacks using PLC.

If it is possible for a well-funded organization to launch a cyber attack on a secure nuclear facility and make vital equipment self-destruct[15], cyber attacks on the nation's vital grid must be taken seriously. Fortunately, the vulnerability of the electrical grid is finally receiving some attention by the federal government[16].

Meanwhile, it does not make sense to keep installing equipment with serious security vulnerabilities.

More information

Additional articles about PLC systems ans smart meters are available on www.eiwellspring.org/smartmeter.html.

2013

References

(1) National Institute of Standards and Technology Smart Grid Collaboration PAP-15 group collaborate.nist.gov/twiki-sggid/bin/view/SmartGrid/PAP15PLCForLowBitRates. (scroll down to Why Is Coexistence Important)

See also www.eiwellspring.org/plc/PLC_travels_into_homes.htm for commentary.

(2) Federal Communications Commission, ET Docket 04-39, April 29, 2009 www.eiwellspring.org/plc/FCClaboratoryBPLreport.pdf

See also links to FCC web site, interpretation and commentary on www.eiwellspring.org/plc/FCC_investigates_PLC.htm

(3) Power Line Communication turns electrical wires into antennas, www.eiwellspring.org/plc/PLC_antenna_effect.htm

(4) TWACS, www.aclara.com

(5) Turtle TS1 and TS2, www.landisgyr.com

(6) Security Pros Question Deployment of Smart Meters, Kim Zetter, Wired Magazine, March, 2010

(7) Arizona Corporation Commission, Steven Olea, Docket E-00000C-11-0328, February 24, 2012 (Guideline #3)

(8) Arizona Corporation Commission filing, Thomas Mumaw/APS, Bradley Carroll/TEP & UNS, John Wallace/Coops, Docket E-00000C-11-0328, August 23, 2012 (Guideline #3)

(9) TWACS – How Our AMI System Works, San Miguel Power Association, www.smpa.com

(10) Hacking for Privacy: 2 days for amateur hacker to hack smart meter, M. Smith, *Network World*, April 2012. www.networkworld.com

(11) For the most commonly used PLC system in the USA, see United States Patent 5,933,072 and *A TWACS System Alarm Function for Distribution Automation,* by Sioe T. Mak, IEEE Transactions on Power Delivery, April 1994.

It appears that the outbound signals (i.e. to the smart meter) are voltage pulses, while the inbound (i.e. to the substation) are current pulses. The pulses are sent at the AC zero voltage crossing, with four pulses comprising one bit.

(12) Spec sheet for TWACS UMT-R, www.aclaratech.com

(13) Smart Meter Data: Privacy and Cybersecurity, Brandon J. Murrill et al., Congressional Research Service, 2012, page 3-6. www.crs.gov.

(14) Fed's Smart Grid Race Leaves Cybersecurity in the Dust, Kim Zetter, Wired Magazine, October 2009, www.wired.com

(15) Time Magazine, March 11, 2013, page 24.

(16) Digital Danger, Charles Choi, *Scientific American,* December 2012.