Journal

of The New England Water Works Association

Our 131st Year

Volume 126 No. 1 March 2012

SACO RIVER
BIDDEFORD & SACO WATER COMPANY, MAINE

New England
Water Works Association
A Section of the
American Water Works Association

Journal of the New England Water Works Association

Contents

Volume 126, No. 1 March 2012

MAILING AND SUBSCRIPTION INFORMATION: (ISSN 0028-4939)(USPS 277-840) NEW ENGLAND WATER WORKS ASSOCIATION JOURNAL is published quarterly March, June, September and December by New England Water Works Association, 125 Hopping Brook Road, Holliston, MA 01746-1471 (www.newwa.org). Subscription rates: $26/year in the U.S. and U.S. possessions, $48/year elsewhere (including Canada). Must be paid in U.S. funds on a U.S. bank. Periodicals postage paid at Worcester, MA and other offices. Printed in USA. Postmaster: Send address changes to New England Water Works Association, 125 Hopping Brook Road, Holliston, MA 01746-1471.

Vulnerabilities of Wireless Water Meter Networks

By John K. McNabb*

Received October 3, 2011

Abstract

U.S. water utilities depend on their water meters for accurate determination of water usage to support their collection of the usage portion of their estimated $40 billion a year in water revenue. Only about 33% of water utilities in the U.S. have implemented or are considering implementing a smart meter program. The worldwide installed base of smart water meters is expected to increase from 5.2 million in 2009 to 31.8 million by 2016. Wireless water meters have many benefits, such as enabling better leak detection, providing more accurate usage information, supporting water conservation, and improving management of the distribution system infrastructure. However, wireless water meters may increase the vulnerability of a water utility to cyber attack, and raises other security and privacy issues which will be discussed in this paper.

I. Introduction

U.S. drinking water utilities collect $40 billion annually, and depend on the readings from water meters for this income. Wireless water meters, while providing quantifiable benefits to a local drinking water utility and their customers, may also result in security vulnerabilities. Water utilities have historically been a target for attacks by nation states, terrorists, and others, and need to do more to protect their critical assets from potential attack.

This paper discusses the specific facts and issues concerning wireless water meters, in their various forms as Automatic Meter Reading, Advanced Metering Infrastructure, and as part of an overall "Smart Grid" infrastructure which includes electric and gas utilities. Furthermore, the larger context of drinking water cyber security is also addressed to put this potential risk in context. Finally, the various security and privacy issues raised by wireless water meters are discussed.

II. Water Meters

A water meter is a device which collects and registers information on the volume of water used over a period of time at a particular location. The resultant information, which is the volume of water used in gallons or cubic feet since the installation of the meter, is used to calculate the amount charged by the local drinking water utility to the customer for water usage at that location for that billing period.

Water meters[1] are typically composed of metal, usually brass or copper, but sometimes plastic, and typically range in size from 5/8" to 2" diameter for residential and commercial customers. The most common type of meter used is a positive displacement meter, which uses a vane, piston, diaphragm, or disk to separate measured volumes of

*Water Commissioner, Town of Cohasset, Cohasset, MA, 1997-2010

[1] *Control and Mitigation of Drinking Water Losses in Distribution Systems*, EPA (Environmental Protection Agency), USA, November 2010, Chapter 2, "Metering," pp. 3-1 through 3-13.

water and count these measured volumes to indicate the accumulated volume on the meter register.

Overall, there are four major types of meters: positive displacement, velocity, compound, and electromagnetic meters. There are two types of positive displacement meters: nutating disc and piston. There are six types of velocity meters: turbine, multi-jet, propeller, ultrasonic, venture, and orificemeters. Compound meters include both positive displacement meter, for low-flow conditions, and velocity meter, for high-flow conditions.

The meter register is a mechanical or digital display which indicates the volume of water which has flowed through the meter since its installation. One of the oldest types is the dial read meter, which shows a series of dials showing the volume used in ones, tens, hundreds, thousands, etc. of gallons or cubic feet. One of the most common shows the water volume on an increasing counter similar to an automobile odometer. Many registers have a red leak detector hand or triangle which, if moving when all water usage is shut off, indicates that there is a leak.

Water meters are an important component[2] of a local drinking water utility for a number of reasons. They allow the utility to: (a) charge customers for the volume of water used, (b) monitor the total amount of water produced and sent to the distribution system, and (c) detect and fix leaks in the distribution system. They allow the customer to: (a) monitor the volume of water they are using, (b) have some control over their water bill, (c) detect and fix leaks at their location, and (d) take measures to conserve water.

Accurate metering[3] is also required for effective accounting and rate making, to identify and study peak and non-peak water use, verification of water and cost savings, the implementation of water efficiency and conservation measures, to allow the utility to make informed decisions on operations, maintenance, capital investment, and customer service, and to facilitate and improve management of the water utility.

Water meters are not perfect instruments, and do not always provide accurate measurements. Over time, as the meter ages, wear and tear on the components and the accumulation of sediment, lime scale, and impurities reduces the accuracy of the meter.

For example, a water audit conducted by the city of Tampa, Florida, found that inaccurate meters cost the city $2,473,535 in FY2005.[4] Dubuque, Iowa projected[5] in a 2009 water meter testing program that inaccurate meters would cost the city $676,000 in lost revenue, about 6.9% of the projected water and wastewater revenue for that fiscal year.

Proper management of the metering and billing system is also important to provide the needed level of revenues to the utility and to sustain public confidence in the system. The June, 2011 audit[6] of the Brockton, Mass. Water

---

[2] Satterfield, Zane and Vipin Bhardwaj, Tech *Water Meters*, National Environmental Services Center at West Virginia University, Tech Briefs, Summer, 2004.

[3] *Water meter calibration, repair, and replacement program*, Georgia Environmental Protection Division, August 2007.

[4] Pickard, Brad D., Jeff Vilagos, Glenn K. Nestel, Rudy Fernandez, Stephen Kuhr, and Daniel Lanning, *Reducing non-revenue water: a myriad of challenges*, Florida Water Resources Journal, May, 2008.

[5] *Dubuque Water Meter Review and Testing - Final Water Meter Review and Testing Phase Two*, HDR Engineering, Inc. March 2009.

[6] *Review of policies, practices, and procedures of the City of Brockton's Water and Sewer Department*, The Abrahams Group, Woodard & Curran, June, 2011.

& Sewer Department found that most of the city's meters were 15 years or older, that FY2006 through FY2010 approximately 25% of the water bills were not based on reading the meter but were estimated readings, and that the billing staff did not have sufficient training in using the system. The audit was called for by the City Council following the issuance of numerous retroactive bills to residents, resulting in one case of a water bill of $97,000 for one homeowner.

Tampering of water meters is a serious issue which costs money for water utilities. For example, water meter tampering has been reported to be on the rise in Temple, Texas; Georgetown, South Carolina; Taylor, Texas (which reported losing 2.5 million gallons in FY 2010); Lavergne, Tennessee; Pleasant Grove, Utah; and Mammoth Springs, Arkansas. The motive is to steal water and pay less in water bills. These jurisdictions and other have been passing laws to punish water meter tampering.

Historically, prior to the introduction of wireless and other automatic reading of water meters, the amount of information and the purposes for which it could be used were rather limited. Meters are usually located in the basement of a home or in a meter pit at the property boundary, and have historically been manually read only once every 3 months or, in some cases, monthly.

III. Wireless Water Meter Sensor Networks

The methodology and technology for reading water meters has evolved greatly since the 1980's, producing major improvements in the technology and concomitant increases in the quantity and quality of the information collected. Water meters have thus evolved from stand alone devices to networked devices working in a sometimes complex sensor network providing information services that the inventors of water meters decades ago never would have imagined was possible.

A. Evolution of meter reading methods

(1) Eyeball

This is the legacy method which requires a meter reader to physically enter the premises and read the meter, usually in the basement. The meter reader eyeballs the register and writes down the numbers on a sheet in a location corresponding to the customer's account number. This information is then manually inputed into the utility's billing system database for calculating the charge for water usage for that billing period.

Since this method is labor-intensive and expensive, such readings have been made only quarterly, but in some places monthly, providing very few data points for each location. This information is usually more than sufficient to use to calculate the portion of the customer's water bill for that location for water usage and to detect leaks.

(2) Walk-by

The meter is connected with wires to a device located on the outside of the building, so even though a physical visit by a meter reader is still required he does not have to enter the building, eliminating the problems caused by lack of access to the meter (in which case an 'estimated' reading would have to be used for the water usage part of the water bill).

The meter reader uses a handheld computer, which is either touched onto the touchpad of the external meter unit, or receives the information via infrared or radio frequency. The handheld computer records the water usage information for later download to the meter billing system.

While this method reduces human error in the transcription, twice, of the information from the register in the "eyeball" method, it does have the possibility of computer error if the protocols in the handheld computer and in the billing system software are not compatible.

This method does not increase the quantity or quality of the information collected, which is still just water usage for each quarter or month, which can be used for water billing purposes and leak detection.

(3) Drive-by

The meter is retrofitted with, or already comes with, a radio frequency transmitter, that is read by the meter reader in his vehicle as he drives past all the metered buildings on his route. The information is collected on a laptop in the vehicle, which has vendor-supplied software which matches the account information, location, and meter register information and prepares it for download to the billing system when the vehicle returns to base.

Drive-by does not by itself increase the amount of meter readings, because of the time and expense of driving the routes, but is usually employed on rural routes that are not cost effective to put into a fixed network, or in some cases as a mid-stage to developing a fixed network system which allows for much more frequent meter reading.

(4) Fixed Network

The fixed network is what we usually think of when we talk about automatic meter reading. This implementation takes the full use of the capabilities of the wireless water meter and enables it to become a sensor network for the water utility that can allow almost continuous water usage readings for a number of purposes which will be discussed.

In the fixed network the signals from the single meter are transmitted and then collected in a central receiving station, if close enough, or to repeaters and then to the central receiving station. In most cases a star topology is used, but in some implementations a mesh topology is used so each meter can act as a repeater for any others within range.

B. Smart Water Meter – AMR/AMI

The smart water meter market is expected to total $4.2 billion between 2010 and 2016.[7] The worldwide installed base of smart water meters is expected to increase from 5.2 million in 2009 to 31.8 million by 2016.[8]

A "smart" meter is defined as one that is a component of the "smart grid,"[9] has two-way communication between the meter and the water utility that allows the utility to obtain meter readings on demand (hourly or more frequently) and can issue commands to the meter.

- AMR refers to Advanced Meter Reading, and includes the walk-by and drive-by methods as well as a fixed network, but usually only includes one-way communication from the meter to the billing system.

- AMI refers to Advanced Metering[10] Infrastructure which is a fixed network system, with smart meters, and refers to the full measurement & collection system, including the meters, communications network, and the data management/billing system.

---

[7] *Global Investment in Smart Water Meters to Reach $4.2 Billion by 2016*, Pike Research., February 21, 2011. http://www.pikeresearch.com/newsroom/global-investment-in-smart-water-meters-to-reach-4-2-billion-by-2016.

[8] *Installed Base of Smart Water Meters to Surpass 31 Million by 2016*, Pike Research, July 13, 2010. http://www.pikeresearch.com/newsroom/installed-base-of-smart-water-meters-to-surpass-31-million-by-2016.

[9] There is no widely-accepted definition of what the "smart grid" is.

[10] "Advanced metering is a metering system that records customer consumption hourly or more frequently and that provides for daily or more frequent transmittal of measurements over a communications network to a central collection point." *Assessment of Demand Response & Advanced Metering*, Federal Energy Regulatory Commission, 2006. http://www.ferc.gov/legal/staff-reports/demand-response.pdf.

Only 7% of U.S. water utilities have adopted a smart meter program, so far. About 33% of water utilities in the U.S. have implemented or are considering implementing a smart meter program. The top five benefits[11] perceived by managers of water utilities for adopting smart water meters:

(1) Enabling early leak detection

(2) Supplying customers with information to reduce water use

(3) Providing more accurate water rates

(4) Curbing overall water demand

(5) Improving ability to conduct preventative maintenance

Other operational benefits[12] associated with smart meters include:

(1) Reduced meter reading costs

(2) Reduced costs for field visits and customer calls

(3) Improved billing accuracy and improved cash flow

(4) Improved outage information and response

(5) More efficient asset management & distribution engineering design

(6) Increased revenue by reducing leaks & unaccounted for water

(7) Help detect theft of service

(8) Help detect violations of water conservation restrictions

(9) Allow remove/virtual turnoff of water

(10) Help better determine timing of water use & demand

C. Components of a "smart" meter AMI fixed network[13]

(1) **Meter.** Many legacy meters can be retrofitted with transceivers, or be replaced with meters with attached transceivers.

(2) **Meter Transceiver Unit (MXU).** This unit contains the transceiver, battery, and antenna.

(3) **Smart meter.** This is the meter plus the MXU; it reports the interval data – the meter reading and information regarding continuous flow, high flow, and reverse flow, and when capable, can turn off water on command.

(4) **Smart endpoint.** Collects and stores the interval data, event alarms, and other usage data. Two way communication allows on-demand consumption data, interval data reads, and future functionality such as water shutoffs.

(5) **Data collection network.** Usual configuration is either a star topology with communication directly from MXU to the endpoint, or a mesh topology where all MXUs can act as repeaters for any other meter, or hybrid systems where MXUs transmit to repeaters using other mediums such as cell phones which then send the signal to other collectors and/or the endpoint.

---

[11] *Testing the Water: Smart Metering for Water Utilities*, Oracle Utilities, January 2010.

[12] *AMR/AMI for Water Utilities*, Lon W. House, Ph.D., presentation to California Water Association, November 11, 2008.

[13] *Advanced metering infrastructure: lifeblood for water utilities*, by Sherlynn Moore and David M. Hughes, Journal of the American Water Works Association, April 2008, pp. 64-68.

(6) **Application software**. Managed the flow of information over the network and between the MTUs and the endpoint. Collects data from the endpoints as well as performing system diagnostics.

(7) **Meter data management software**. Repository for the collected information, to use for billing but also for analysis of the data for leak detection and offers interfaces to other utility systems such as distribution monitoring, GIS systems, and preventative maintenance.

The data collected from the AMI system can also be used to present information to the customer about their water use, either in an in-house device or over the internet in a secured web site. This customer-faced information portal can provide a wealth of information such as historical water usage and pricing information. This information could help the consumer pinpoint when a leak may have occurred and take steps to conserve more water.

By collecting water usage in short intervals, the water utility could also adopt time sensitive rates, similar to what some electric utilities are doing, to charge higher rates in times of high consumption to reduce peak usage and conserve resources. The utility could also synchronize such time sensitive rates with their electrical costs to encourage consumers to lower water usage during peak electrical cost periods, lowering the utility's costs and leading perhaps to lower water rates.

D. Anatomy of a "Smart" Water Meter

The basic architecture of a "smart" water meter, which has automated meter reading and radio frequency transmission capabilities, includes the following components:

- **Transceiver** – for example the 700/800/900 MHz Atmel AT86RF212 with internal 128 byte RAM buffer, max 1 MB/s data rate, AES encryption
- **Processor** – usually 8 or16 bit microcontroller, and also 32 bit now
- **Memory** – typically EEPROM with 1 – 4 Kb nonvolatile storage
- **Power supply** – batteries with 5 to 20 year estimated life span

Review of product datasheets shows that most smart water meters in the U.S. operated in the 902-928 MHz ISM band, and most use Frequency Hopping Spread Spectrum with no encryption.

IV. The Cyber Threat Dimension: Water System SCADA Control System Vulnerabilities[14]

Historically, drinking water treatment facilities were isolated systems accessible only through physical access to the valves, chemical feed units, and control panel in the water treatment plant. In these legacy control systems, each valve, chemical feeder, and mechanism was connected by individual wires to one or more central control panels where the operator could view the many dials and meters showing the status of each component and could change the settings individually as needed.

Remote facilities like water storage tanks, reservoir gates, and pump stations, were also connected through radio, telephone, cable, or other means. However, in the past three decades many water utilities have retrofitted their facilities by installing computer-controlled SCADA or

[14] This section is also published in the chapter *Chemical and Biological Threats Against Public Water Systems*, by the author, in the book Weapons of Mass Destruction and Terrorism, James J.F. Russell and Russell Howard, eds. (McGraw-Hill, 2012).

other control system type hardware and software.[15] The dedicated communications channels for remote facilities were in most cases replaced by internet connections,[16] and also in many cases remote operation over the internet of the SCADA system was implemented. A computer screen replaced the large mechanical control panel with its dozens of dials, levers, and mechanical registers.

Supervisory Control and Data Acquisition (SCADA)[17] is the term usually used to describe the computerized central control system used in many drinking water utilities, as well as in many other industrial, manufacturing, and energy facilities. SCADA replaced the legacy control schemes which utilized electro-mechanical process control.

SCADA systems were designed to provide consistent and reliable access; security considerations were not in the forefront of design concerns. A public water system is expected to operate 24 hours a day, every day, setting the flow rate of water entering the plant, automatically setting the amounts of treatment chemicals to keep pace with the flow rate, and timing the flocculation, settling, and filtration phases to meet the required time periods to be effective.

As a result, the computer systems that control these actions are not designed to be regularly updated with security patches (which often require a system to pause services or even restart). Many water utility SCADA systems were designed in isolation, but most of this kind of software runs on Microsoft Windows XP or Server 2003[18] systems. Some do not have regular internet access, but many do. Both of these factors contribute to the vulnerability of drinking water facilities to intentional or unintentional intrusions.[19]

A March 2008 report by the Water Sector Coordinating Council's Cyber Security Working Group lists a variety of "water sector industrial control system risks today" including design limitations, more open environments, increased connectivity and complexity, system accessibility, supply chain limitations, and information availability.[20]

This report, *Roadmap to Secure Control Systems in the Water Sector*,[21] states that there are many ways in which a cyber event[22] can affect a water system, "some with potentially significant adverse effects in public health," such as:

---

[15] For a detailed description of the technological transition, see C4 Security, *The Dark Side of the Smart Grid – Smart Meters (in)Security*, (September 2009), online at: http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf.

[16] Many of them, however, still retain "always on" modem connections using phone lines, another potential route of attack by attackers who perform "wardialing" to find active modems and then exploit them.

[17] SCADA usually refers to highly distributed systems to control geographically dispersed facilities, and the term Distributed Control Systems (DCS) usually refers to the control systems in a localized facility such as a single treatment plant. However, we will use the term SCADA as a generic term to be inclusive of the larger systems as well as the localized systems, since for the purposes of this paper the same factors apply to a full-fledged SCADA as do to a DCS.

[18] *"Improving Security for SCADA Control Systems"* Mariana Hentea, Interdisciplinary Journal of Information, Knowledge, and Management, Volume 3, 2008, pp. 73-82.

[19] GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, March 2004.

[20] *Roadmap to Secure Control Systems in the Water Sector* (March 2008), p. 14. Available online at: http://www.awwa.org/files/GovtPublicAffairs/PDF/WaterSecurityRoadmap031908.pdf.

[21] Ibid

[22] The term "cyber event" is a broad term meant to encompass both unintentional and intentional compromise of a system from malware.

- Interfere with the operation of water treatment equipment, which can cause chemical over or under-dosing
- Make unauthorized changes to programmed instruction in local processors to take control of water distribution or wastewater collection systems, resulting in disabled service, reduced pressure flows of water into fire hydrants, or overflow of untreated sewage into public waterways
- Modify the control systems software, producing unpredictable results
- Block data or send false information to operators to prevent them from being aware of conditions or to initiate inappropriate actions
- Change alarm thresholds or disable them
- Prevent access to account information

Further, the report notes that although many facilities have manual backup procedures in place, the failure of multiple systems at once may overtax staff resources—even if each failure is manageable by itself.

Known Water System SCADA Cyber Attacks

There are only a handful of publicly disclosed SCADA cyber attacks involving drinking water and wastewater facilities, including:[23]

- **2000** – Maroochie Water System, Australia; former consultant took control of wireless pump system 46 times to spill 264,000 gallons of raw sewage onto waterways.
- **2006** – Harrisburg, Pennsylvania water treatment plant; foreign hacker planted malware in plant computers to use them to distribute spam and pirated software.
- **2007** – Tehema Colusa Canal Authority, California; former employee remotely installed unauthorized software on a SCADA computer that controlled the flow of water.

The Department of Homeland Security publishes a daily Open Source Infrastructure Report[24] which summarizes incidents that often involve public water systems. In 2010, these reports revealed a total of 914 "Water Sector" incidents, including 246 incidents at drinking water treatment facilities. Of these, 71 involved water contamination, 79 were water main breaks, 18 were chlorine leaks, 13 involved plant malfunctions, and 12 were incidents of vandalism. There was only one reported incident of a "terrorist threat," which turned out to be a hoax.[25] Four incidents are of particular interest to this discussion, in that they involved computer systems:

- **March 2010:** The public water system in Silver City, New Mexico lost 3 million gallons because of a water leak that investigators linked to a possible malfunction in their newly installed SCADA system.[26]

[23] Ibid

[24] DHS only makes the last 10 reports available on their web site. I was able to obtain past reports from the repository maintained by Bob Johnston, CISSP http://dhs-daily-report.blogspot.com/, who has been downloading and storing the reports since 2004.

[25] The incident reporting in these reports is not exhaustive, so one should not assume that these are all the incidents that actually occurred or that these numbers are representative of the actual incidence nationwide during 2010.

[26] Silver City Sun News, March 11, 2010. DHS Open Source Report, March 12, 2010, p. 13.

- **June 2010:** A computer failure caused the public water plant in Lake Chelan, Washington to stop operating.[27]

- **September 2010:** A computer malfunction apparently shut down the water plant in Glidden, Iowa and drained the town's water storage tank.[28]

- **December 2010:** The water plant in New Canaan, Connecticut was shut down because of a computer malfunction, but water was still pumped into and through the plant, causing flooding from the plant across the nearby roadway.[29]

Other incidents within the past year have served to heighten concerns over the cyber security of drinking water facilities. In June 2011, an IT security professional performed a penetration test for an unnamed Southern California water utility, and was able to gain control of the utility's chemical control systems in less than a day. The route of exploitation was workers who were able to remote into the SCADA system from home.[30]

In August 2011, another IT security professional giving a demonstration at the annual Black Hat IT security conference in Las Vegas showed how to use Google to access the Programmable Logic Controller (PLC) of a water treatment plant pump, but he did not try to remotely have it do anything.

The Powerful Stuxnet Worm

In June, 2010, the IT security world was rocked by the discovery by security firm VirusBlokAda of a powerful worm[31] which was showing up in control systems all over the world. While it was first thought that Stuxnet was designed to steal trade secrets and intellectual property, it was soon learned that even though Stuxnet was found in computers and control systems all over the world, it affected only certain Siemens control systems used for controlling centrifuges in the Iranian nuclear development program.

Stuxnet is considered a "game-changer" because it is the first known malware to effectively attack SCADA systems. It utilized four previously unknown vulnerabilities in the Windows

---

[27] Lake Chelan Mirror, June 23, 2010, http://lakechelanmirror.com/main.asp?SubSectionID=5&ArticleID=2670&SectionID=5.

[28] Associated Press, September 20, 2010. http://www.whotv.com/news/who-story-glidden-water-tower-092010,0,1010748.story.

[29] New Canaan Patch, December 4, 2010. http://newcanaan.patch.com/articles/computer-glitch-shuts-down-water-plant.

[30] Marc told the author that *"… it was a rather straight forward pen test just compromising a series of systems using your standard Adobe and Microsoft related vulnerabilities. They suffered from the same problem as most places in that the actual control systems are not really ever patched, because of all the usual red-tape, which makes them easy to hack and really the only hard part was trying to find the private network (attached to the county network) where the control systems were located. That was the scary part about it like most of these pen test is that there was nothing james bond or interesting to it really. Sure plenty of the specific control software used in these environments has security flaws also but that does not matter when its an unpatched Windows 2000 system etc."* Email from Marc Maiffret, April 18, 2011.

[31] A worm is a self-replicating program that, unlike a virus, does not have to infect a file to cause damage. Since many malicious programs these days utilize the features of worms and viruses, and also of trojans (which disguise themselves and non-malicious programs), the generic term "malware" is usually used.

operating system used to run the Siemens' control system software — a major accomplishment, since most successful malware tend to exploit just one undiscovered vulnerability. Stuxnet was also designed to successfully bridge the "air gap" supposedly protecting the Siemens systems: in other words, the machines were not connected to the internet, but the worm was still spread by using thumb drives as the delivery method.

In its Stuxnet Dossier, the IT security firm Symantec describes Stuxnet as "a threat targeting a specific industrial control system likely in Iran, such as a gas pipeline or power plant. The ultimate goal of Stuxnet is to sabotage that facility by reprogramming programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries."[32]

While the objective of Stuxnet was to damage the Iranian nuclear program, its methodology could be applied, or its code could be altered, to attack other industrial control systems such as those at a water treatment plant. Of course, it still would take an enormous amount of reconnaissance and research to design a Stuxnet-like malware to attack a water treatment plant, and a separate design may be needed for each individual plant attacked, because of their uniqueness, but it's possible. Perhaps only a nation-state would have the resources to accomplish this (as has been surmised about Stuxnet), but perhaps not. If that day comes, then the question becomes whether the water sector has the capability to defend against an attack from malware delivered through USB drives; right now, the answer to that question is an emphatic "No."

Summary of the Cyber Threat to Public Drinking Water Systems

By spring 2011, about one year after the discovery of Stuxnet, there had been a plethora of additional vulnerabilities discovered in SCADA systems used around the world and in water utilities. The antivirus company Symantec reports[33] that there had been 15 new SCADA vulnerabilities disclosed in 2010, one more than the 14 publicly disclosed vulnerabilities in 2009.

In March, 2011, Italian security researcher Luigi Auriemma released proof of concept code on 34 SCADA vulnerabilities to Bugtraq (an online repository of software vulnerabilities), which was followed by many advisories from ICS-CERT (Industrial Control Systems Cyber Emergency Response Team). These vulnerabilities, according to Auriemma,[34] would allow an attacker to execute a program remotely on a SCADA system with an internet connection, allow attackers to access stored data or to interfere with the process control hardware that is run by the SCADA system.

There has been speculation that the release of Stuxnet could be followed by some kind of modified "Son-of-Stuxnet," based on the capability shown by the original Stuxnet. Witnesses testifying in a hearing in November 2010 before the Senate Committee on Homeland Security and Government Affairs testified that variants of Stuxnet could be used to attack other critical infrastructure, such as the power grid, transportation systems, or water supplies.[35]

---

[32] *W.32 Stuxnet Dossier*, Version 1.4, February, 2011. Symantec Corporation.

[33] Vulnerability Trends – SCADA Vulnerabilities, Symantec. http://www.symantec.com/business/threatreport/topic.jsp?id=vulnerability_trends&aid=scada_vulnerabilities.

[34] *"34 SCADA vulnerabilities revealed,"* Help Net Security, March 22, 2011. http://www.net-security.org/secworld.php?id=10771.

[35] For example, see: Statement for the Record of Sean P. McGurk Acting Director, National Cybersecurity and Communications Integration Center Office of Cybersecurity and Communications National Protection and Programs Directorate Department of Homeland Security Before the United States Senate Homeland Security and Governmental Affairs Committee, Washington, DC, November 17, 2010.

Stuxnet could be leading the way[36] as the first "weaponized" malware, setting a precedent for newer variants targeting different applications because:

(1) Stuxnet provides a "step-by-step cookbook" for SCADA malware design;

(2) There are many vulnerabilities in SCADA that have been discovered since Stuxnet, and many more most likely remain to be discovered;

(3) Specific knowledge of the target process used by the PLC's controlled by the SCADA software isn't necessarily needed; and

(4) The Stuxnet-type code that is now available provides the basic structure to remotely control a SCADA process for whatever objective the attacker might want, the customizations can be added as needed.

Clearly, the U.S. does face potential cyber attacks, on our critical infrastructure and other assets, from nation states, terrorist networks, criminal groups, malicious hackers, and others, as pointed out by Director of National Intelligence Dennis Blair in his Annual Threat Assessment: "Malicious cyber activity is occurring on an unprecedented scale with extraordinary sophistication."[37]

Almost a decade earlier, the CIA indicated in a Senate hearing that they were alert to the possibility of al Qaeda and Sunni extremists planning cyberwarfare attacks against U.S. critical infrastructures:

> Cyberwarfare attacks against our critical infrastructure systems will become an increasingly viable option for terrorists as they become more familiar with these targets, and the technologies required to attack them. Various terrorist groups--including al-Qa'ida and Hizballah--are becoming more adept at using the Internet and computer technologies, and the FBI is monitoring an increasing number of cyber threats…. These groups have both the intentions and the desire to develop some of the cyberskills necessary to forge an effective cyber attack modus operandi.[38]

There is evidence that al Qaeda has been researching SCADA and control systems used in drinking water and wastewater. However, most observers conclude that al Qaeda does not have the skills, manpower, or technical sophistication to carry out a cyber attack on critical infrastructure, or any other cyber attack. One reason is that most of their key computer experts have been captured or killed.[39] Dorothy Denning, of the Center on Terrorism and Irregular Warfare at the Naval Postgraduate School, has been closely examining this issue for many years, and recently concluded that "Terrorists have not yet demonstrated that they have the knowledge and skills to conduct highly damaging attacks against critical infrastructures

---

[36] *"Son-of-Stuxnet" – Coming Soon to a SCADA or PLC System near you."* Eric Byres, May 31, 2011. http://www.tofinosecurity.com/blog/%E2%80%9Cson-stuxnet%E2%80%9D-coming-soon-scada-or-plc-system-near-you.

[37] Dennis C. Blair, Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intelligence," Statement for the Record, (February 2, 2010). Online at http://*ww.dni.gov/testimonies/20100202_testimony.pdf*.

[38] CIA -- Unclassified responses to the Questions for the Record from the Worldwide Threat Hearing on 6 February 2002, Senate Select Committee on Intelligence. http://www.fas.org/irp/congress/2002_hr/020602cia.html.

[39] *Cyberterrorism Hype v. Fact*, by Robert K. Knake, Council on Foreign Relations, February 16, 2010. http://www.cfr.org/terrorism-and-technology/cyberterrorism-hype-v-fact/p21434.

(e.g. causing power outages) although there are a few indicators showing at least some interest . . . At least in the near future, bombs remain a much larger threat than bytes."[40]

Securing the Water Sector

Responsibility for the security, maintenance, and operation of a local water utility is principally the sole responsibility of that utility, subject to applicable local laws and regulations, the state regulatory authorities, and the U.S. Environmental Protection Agency (EPA).

Homeland Security Presidential Directive 9 (HSPD9) directed the EPA to develop a surveillance and monitoring program to provide early warning detection of a terrorist attack using biological, chemical, or radiological (CBR) weapons. EPA awarded funding for CWS pilots in New York City, San Francisco, Philadelphia, and Dallas. These four additional pilots were selected through a national competition and will conclude in 2012.[41]

In addition, the Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188, 42 U.S.C. 300i) amended the Safe Drinking Water Act[42] to require community water systems serving more than 3,300 individuals to complete a vulnerability assessment, prepare an emergency response plan, and to submit them to the EPA. These vulnerability assessments[43] had only one question regarding general PC security (passwords, etc.) and did not address control system security.

Neither the Bioterrorism Act, nor any other federal law or regulation require any water utility to actually make security upgrades to address vulnerabilities; provide funds to help water utilities to make security improvements; or require water utilities to revise or update the vulnerability assessment or emergency response plan after they were completed in 2003-2004.

The progress of U.S. drinking water systems in improving their overall security was assessed in a talk[44] given at the September 21, 2010 American Water Works Association (AWWA) Water Security Congress. The metrics used to assess this progress were developed by the Critical Infrastructure Partnership Advisory Council (CIPAC) and were collected and aggregated by the Water Information Sharing and Analysis Center (WaterISAC). According to their study:

- 70%+ had incorporated security planning and design programs to all assets and facilities.

---

[40] *A view of cyberterrorism five years later*, Dorothy Denning, Center on Terrorism and Irregular Warfare, Naval Postgraduate School, Chapter 7 in Internet Security: Hacking, Counterhacking and Society (K. Himma ed.) Joes and Bartlett Publishers, 2007. In two emails to the author on June 30, 2010, Denning said that *"I also haven't seen anything to give me concern about the jihadists or change my overall assessment.. ..I would be very surprised if AQ has anything resembling a computer training center today. Maybe they did at one time, but it seems unlikely they would now. There are people who have associated themselves with AQ who have cyber skills, but I don't think any of them have the kind of skills needed to launch a serious cyber attack against a water system or any other critical infrastructure. Most of their skills relate to putting stuff on websites and protecting their cyber activities using tools like Tor and encryption. The jihadist cyber attacks are pretty rudimentary, e.g., web defacements and DoS attacks."*

[41] *Water Security Initiative Program Overview and Available Products,* EPA Fact Sheet.

[42] Tiemann, Mary, *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, September 30, 2010.

[43] *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, Association of State Drinking Water Administrators National Rural Water Association May 30, 2002.

[44] *Measuring Water Security Progress*, L. Vance Taylor, AWWA Water Security Congress, September 21, 2010, National Harbor, Maryland.

- 90%+ secure and monitor perimeters and have chemical safeguards in place.
- 80%+ control access to restricted areas by screening/inspecting people/vehicles who enter.
- 94%+ secure and monitor shipping, receipt, and storage of hazardous chemicals.
- 85%+ integrated security and preparedness into budgeting, training, and manpower responsibilities.
- 90%+ have developed emergency response plans.
- 50%+ are training, exercising, reviewing, and updating those plans.
- 75% are networking for collaborative responses in an incident.
- 86% have backup power for 24 hours; 50% for 96 hours (4 days) or more.
- 66% of water utilities can provide 91-100% of minimum daily demand for 24 hours.
- Almost 33% of water utilities can provide 91-100% of minimum daily demand for 72 hours.[45]

However, it is important to note that of the "22 Sector Specific Measures" which were used in this assessment, none of them addressed SCADA or Cyber security.

There has been some progress in developing new resources to assist local water utilities to protect against cyber and other attacks. For example:

- Water ISAC. The Water Information Sharing and Analysis Center is "a highly secure Internet portal that provides the best source for sensitive security information and alerts to help America's drinking water and wastewater community protect consumers and the environment."[46]
- Training, information, and workshops on security issues are provided through the U.S. EPA, American Water Works Association, Water ISAC, and other affiliated organizations.
- Cyber Security Evaluation Tool (CSET), which assesses the control system and information technology network security practices resulting in a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems."[47]
- Threat Ensemble Vulnerability Assessment (TEVA) – program developed by the EPA, Sandia National Laboratories, and others to provide tools, software, and guidance to assist water utilities to implement real time monitoring for contaminants in the distribution system.

The American Water Works Association in 2004 estimated[48] that at least $1.6 billion is needed for public water systems to implement just the recommended first steps (fences, locks, etc.) in improving security, based on the vulnerability assessments. However, the federal government has

[45] Ibid
[46] WaterISAC Fact Sheet. http://www.epa.gov/safewater/watersecurity/pubs/waterISACFactSheet.pdf.
[47] Control Systems Security Program, US-CERT, http://www.uscert.gov/control_systems/satool.html.
[48] *PROTECTING OUR WATER Drinking Water Security in America After 9/11*. American Water Works Association, 2004. http://fortressteam.com/resources/watersecurity.pdf.

not provided funding for this, and existing federal and state financial assistance to water utilities does not include funding for security improvements.

Securing the Control Systems

In March 2008, the Water Sector Coordinating Council Cyber Security Working Group published a *Roadmap to Secure Control Systems in the Water Sector* which "presents a vision and supporting framework of goals and milestones for reducing the risk of ICS [Industrial Control Systems] of the next ten years."[49] The *Roadmap* identifies the following as some of the "challenges" to reaching its goal to develop and deploy ICS security programs:

- Limited executive recognition of ICS security threats and liabilities.
- Lack of awareness about ICS security risks.
- Business case for ICS security has not been established throughout the water sector.
- Difficult or impossible to integrate new technologies into legacy systems.
- Implementation of security measures is often time consuming.

The "strategic framework" in the *Roadmap* seeks to achieve four main goals: 1) develop and deploy ICS security programs, 2) assess risk, 3) develop and implement risk mitigation measures, and 4) partnership and outreach. The *Roadmap* also describes 18 near-term (0-1 year) milestones, including "isolate ICS from public switch networks" and "Replace default security passcodes," but there are no "progress reports" available anywhere that detail how many of these milestones, if any, have been accomplished.

Serious Gaps Remain

While some progress has been made to better secure the U.S. drinking water infrastructure following 9/11, there are several serious gaps that need to be addressed. To begin with, the Bioterrorism Act does not provide clear lines of authority,[50] leading to some administrative overlap, duplication of effort, and confusion of roles between the EPA and Homeland Security. Neither the EPA nor Homeland Security has legal authority to order any water utility to take action to improve their security. Each water utility makes its own decision on whether to spend money if it has it to increase security.

Water utilities so far have only been required to complete a Vulnerability Assessment and an Emergency Plan – but have not been required to take any action to address the deficiencies revealed in their assessments. Further, these assessments do not adequately address terrorist threats but were designed to address more traditional and less costly threats such as vandalism and disgruntled employees. The EPA has not yet issued standards to the water utility community around which they can develop a baseline for water security.[51]

There is no requirement that these Vulnerability Assessments or Emergency Plans be updated or reviewed following their completion in 2003-2004. Most likely they are gathering dust on shelves all over the United States. Since the Vulnerability Assessments were exempted from state Freedom of Information Acts, no one outside

[49] *Roadmap to Secure Control Systems in the Water Sector.*

[50] *Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, Updated December 15, 2004, by Mary Tiemann, Congressional Research Service, RL31294. http://www.hsdl.org/?view&did=459643.

[51] *EPA needs a better strategy to measure changes in the security of the nation's infrastructure*, EPA Inspector General report, September 11, 2003. http://www.epa.gov/oig/reports/2003/HomelandSecurityReport2003M00016.pdf.

the report writers and utility managers know what the vulnerabilities were or the status of any actions to address them. The information from Vulnerability Assessments has not been used to identify water security research needs or to allocate funds to water utilities to make needed security improvements.

These efforts also require funding, but not enough money has been made available to complete the Vulnerability Reports. While the maximum grant to a utility for completing an assessment was capped at $115,000, the estimated cost for a very large utility to complete one was in the millions.[52] No federal funds have been made available to actually implement the recommendations of these assessments, and there has been no overall assessment of how much this exercise may have made water utilities safer.

There has been insufficient research on the effects of chemical and biological weapons in drinking water, and how to best respond to such an attack on the water supply. Current practices for routine monitoring of water supplies for contaminants are inadequate for detecting chemical or biological contamination.[53] There has not been a strategic analysis on the national level of what it would actually take to achieve security – and what the metrics for that should be – for the national drinking water infrastructure.[54] These and other challenges must be mitigated in the years ahead if we are to avoid a major catastrophe involving the exploitations of the public water sector vulnerabilities identified in this discussion.

V. Security Issues of Wireless Water Meter Sensor Networks

The implementation of wireless water meters in an Advanced Metering Infrastructure or Smart Grid, will provide a wealth of useful information to the water utility to help it with rate setting, leak detection, and infrastructure management. However, the flip side is that it may introduce additional vulnerabilities into an already vulnerable drinking water infrastructure.

Characteristic Vulnerabilities of Wireless Sensor Networks

A wireless water meter network is a kind of Wireless Sensor Network, which is defined[55] as "a large network of resource-constrained sensor nodes with multiple preset function, such as sensing and processing … the major elements of a WSN are the sensor nodes and the base station." Each individual water meter is a "sensor node."

There is a body of literature on vulnerabilities and security of WSN's which is applicable to wireless water meter networks. There are many possible attacks[56] based on the protocol stack, on the physical layer, data link layer, network layer, transport layer and application layer.

---

[52] *"Estimated costs for conducting a large system vulnerability assessment range from approximately $100,000 to several million dollars, depending on the complexity of the system. Additional resources are required to develop or revise the utility's emergency response plan. AWWA has estimated the total national cost to develop vulnerability assessments as required by the Bioterrorism Act to be approximately $500 million."* PROTECTING OUR WATER Drinking Water Security in America After 9/11, American Water Works Association [no date]. http://fortressteam.com/resources/watersecurity.pdf.

[53] *The biological threat to U.S. water supplies: toward a national water security policy*, by Jennifer B. Nuzzo, Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science, Volume 4, Number 2, pp. 147-159, 2006. Page 152.

[54] Nuzzo, p. 157.

[55] *Security vulnerabilities in wireless sensor networks: a survey*, by Kavitaha, T. and D. Sridharan, Journal of Information Assurance and Security, 5 (2010) 031-044.

[56] Ibid, pp. 037-039.

WSN's present many security[57] challenges: the wireless medium itself, unattended operation, random topology, and hard to protect against insider attacks. A packet sniffer allows the attacker to overhear network traffic, conduct traffic analysis, and extract information about a network's nodes and usage. The sniffer allows the attacker to compromise confidentiality; to identify the hardware platform used, the kind of application, frequency of monitored events, and routing information.

At Black Hat Spain, 2010, Giannetsos and Dimitriou demonstrated Sensys, an attack tool against sensor networks *"to reveal the vulnerabilities of such networks, to study the effects of severe attacks on the network itself and to motivate a better design of security protocols that can make them more resilient to adversaries."*[58] This may be the first tool purposely written to penetrate the confidentiality and functionality of a sensor network.

Privacy Issues

Privacy of the data collected by the "smart grid" is a major concern. A poll of more than 9,000 consumers in 17 countries by the Accenture consulting firm found that about 33% would be discouraged from using smart metering if it gave the utility more data about their energy use.[59] There are many scenarios where such information could be used as an invasion of privacy, as summarized in this table:

WHO WANTS WATER METER DATA?	HOW COULD THE DATA BE USED?[60]
Utilities	To monitor water usage and load; to determine bills
Water usage advisory companies	To promote water conservation and awareness
Insurance companies	To determine health care premiums based on unusual behaviors that might indicate illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about famous people
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify the best times for a burglary or to identify high-priced appliances to steal

[57] *Weaponizing wireless networks: An attack tool for launching attacks against sensor networks*, Thanassis Giannetsos and Tassos Dimitriou, Athens Information Technology Algorithms and Security, Black Hat Spain 2010 [slides].

[58] *Weaponizing wireless networks: An attack tool for launching attacks against sensor networks*, Giannetsos, Thanassis, Tassos Dimitriou, and Neeli R. Prasad, Black Hat, Spain, 2010, http://www.ait.gr/export/sites/default/ait_web_site/faculty/tdim/various/attackTool-BlackHat10.pdf [white paper].

[59] *Privacy on the smart grid: Are smart meters spies? They don't have to be*, by Ariel Blecher, IEE Spectrum, October 2010. http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid.

[60] Ibid. This table was adapted by Blecher from Table 5-3, pp. 30-32 of *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid*, NSTIR 7628, National Institute of Standards and Technology, August 2010.

In Cary, North Carolina, such concerns were raised about a proposal to install smart water meters:

> Cary's citizens are right to be **concerned** about the information about our private **lives** that our town staff will be able to collect if the Aquastar/AMI water meter system is implemented as planned. According to **Daniel Burrus**, a technology futurist and keynote speaker at the Autovation conference last September, "As a utility, I could know exactly when you take a shower, exactly when you water the plants or wash the dishes. I could figure out how much water or electricity you are using at any point in time, and probably figure out what you are using it for."[61] [emphasis in original.] … This equipment gives the water cops the ability to **collect evidence around the clock** and to **issue tickets** to violators of conservation rules. Town ordinances **allow the town to assess civil and/or criminal penalties** including fines, debt, and termination of service for any period of time for violators.

The Cyber Security Working Group of the Smart Grid Interoperability Panel, in NISTIR 7628 concluded that, yes, there are privacy concerns with the smart grid (for electricity; there is no NISTIR for the water smart grid), and made the following recommendations to mitigate those concerns:

(1) A utility should conduct a Personal Information Assessment (PIA) that is collected, processed, stored, and otherwise handled, and determine other appropriate risk mitigation activities.

(2) Develop and formally document privacy policies and practices drawn from the Organization for Economic Cooperation and Development (OECD).

(3) Develop a comprehensive set of privacy use cases that will help utilities and third-party Smart Grid providers to rigorously track data flows and the privacy implications of collecting and using data flows and their privacy implications.

(4) Educate the public about the privacy risks in the Smart Grid and what they as consumers can do to mitigate those risks.

(5) Share information about solutions to common privacy-related problems with other Smart Grid participants.

(6) Manufacturers and vendors of smart meters should collect only the energy and personal data necessary for the purposes of smart meter operations.

VI. Demonstrated Methods to "Sniff" Smart Water Meters

Security researchers have demonstrated two "proof of concept" methods to intercept, or "sniff," the transmissions from wireless devices similar to wireless water meters, which broadcast in the 902-928 MHz ISM band, and which attempt to secure the transmission from eavesdroppers by using Frequency Hopping Spread Spectrum (FHSS).

FHSS is still pretty widely used, was originally designed in World War II as a security protocol; but actually provides little to no security at all. Typically, FHSS uses one of 78 different hop sequences defined in the ANSI/IEEE 802.11 standard to hop to a new 1MHz channel about every 400 milliseconds. It was very resistant to narrow band interference and narrow band jamming. However, FHSS uses the same type of management frames used in 802.11 b/a/n/g – Beacon, Associate, Probe, and Probe Response.

[61] *Utility Expert describes privacy invasion through AMI*, The Cary Watchman, January 28, 2010. http://carywatch.net/watermeter.html.

Method #1: Using GNU Software Radio to Crack FHSS

At Black Hat[62] Europe 2009, in *Yes it is Too WiFi, and No It's Not Inherently Secure*, Rob Havelt discussed how he was able to crack Frequency Hopping Spread Spectrum (FHSS) in 802.11 using GNU software defined radio, which uses a Universal Software Radio Peripheral device which is "tuned" using the software. It was possible to just use a USRP locked to a specific channel band, then feed the raw data into the software."[63] To join a FHSS network, he explained, you only need to use Software Radio to listen for a management frame to "hop" by to provide the hopping sequence, which then could be used to unlock the signal.

Method #2: Using

In their Shmoocon[64] 2011 presentation *Hop Hacking Hedy*, researchers atlas, cutaway and Q showed how FHSS was not inherently secure and how to crack it in 900 Mhz wireless devices using the Texas Instruments CC1111EMK 868-915 Evaluation Module Kit programmed with python code they wrote. They explained that a listener, to "tune in" to an FHSS signal, needs to know the number of frequencies, the hopping sequence, and the dwell time, and they showed a "proof of concept method" that succeeded in unlocking the signal.

VII. Conclusion

Water utilities have a number of well-known and documented cyber security vulnerabilities, both in their control systems and in their newer wireless water meter sensor networks. It is vital for the health of the nation's 150,000 water utilities and the 250 million people whom they serve that these vulnerabilities be addressed forthrightly and are resolved. Hopefully this paper has served to advanced that purpose, to make such vulnerabilities known so they can be resolved by the appropriate parties.

Note: This paper was presented at Black Hat USA, Las Vegas, NV on August 3, 2011.

[62] Black Hat is a series IT security technical conferences held in Las Vegas (July-August), Washington DC (January), Europe (April), and/or the Middle East (December) every year.

[63] Email from Rob Havelt, February 3, 2011.

[64] Shmoocon is an annual IT security technical conference held January-February every year in Washington, DC.