Melnykovych, Andrew (PSC)

From: Melnykovych, Andrew (PSC)
Sent: Friday, February 21, 2014 2:04 PM
To: 'song bird'
Subject: Your comments in Case 2012-00428 - smart grid administrative case

Ms. Holloway:

The documents you submitted will be entered as public comments in the record of the above-referenced case.

Andrew Melnykovych
Director of Communications
Kentucky Public Service Commission
211 Sower Boulevard
Frankfort, KY 40601
502-782-2564 cell:502-330-5981

From: song bird [redacted]
Sent: Friday, February 21, 2014 8:53 AM
Subject: Smart Water Meters Vulnerable to Attack

Dear Mr. Melnykovych,

I would like to ask that you and your peers at PSC read this document throughly and then add it to Case File 2012-00428 These Smart Meters and the Smart Grid System are **Dangerous** to all of us and the **Survival** of **All Life!** As you can see from this document...they are easily "Hacked" and not only violate our rights to health, but our right to privacy and freedom!

Sincerely,

Ruby Holloway

Vulnerabilities of Wireless Water Meter Networks

Black Hat USA Las Vegas August 3, 2011
by John McNabb
johnmcnabb@comcast.net

Abstract.

Why research wireless water meters? Because they are a potential security hole in a critical infrastructure, which can lead to a potential leakage of private information, and create the potential to steal water by lowering water bills? It's a technology that's all around us but seems to too mundane to think about.

Because a hacker can't resist exploring technology to see how it works and how to break it… because they are there? In this talk the speaker, who managed a small water system for 13 years, will first present an overview of drinking water security, review reported water system security incidents and the state of drinking water security over the past year, and will then take a deep dive into the hardware, software, topology, and vulnerabilities of wireless water meter networks and how to sniff wireless water meter signals.

ORGANIZATION OF THIS PAPER:

I. INTRODUCTION

US 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 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.

How meters work

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 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.

Importance of metering

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

---

[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

[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

informed decisions on operations, maintenance, capital investment, and customer service, and to facilitate and improve management of the water utility

Accuracy of metering & billing

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 & Sewer Department found that most of the City's meters were 15 years or older, that FY2006 though 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.

Meter tampering

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.

Information from meters

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.

---

[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, Woodward & Curran, June, 2011.

This evolution of automatic reading methods for water meters has resulted in an expansion of the information that can be gleaned from water meters and the purposes which this information can be used.

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 customers account number. This information is then manually input 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 customers 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 to 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

Only 7% of US water utilities have adopted a smart meter program, so far. About 33% of water utilities in the US 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.

---

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

[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.

(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.
(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 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 Patents[14]

Review of a patent for a smart water meter can tell us a lot. *Utility Meter with External Signal Powered Transceiver*, October 24, 2006, Patent # 7,126,493 provides the basic structure and technical detail for its design and engineering. The assignee is Landis+Gyr, Inc. of Lafayette, IN, a manufacturer of water meters. Here are some highlights from the patent:

[14] Note that patents are in the public record so this is all open source material.

- "The present invention …[provides] a meter that includes a transceiver that is operable to receive external signals, derive bias power from the external signals, and perform a data transfer operation in a nonvolatile manner in the meter using the bias power."
- "The RF/memory is a combination RF transceiver and dual port memory device, sometimes known in the art as an RFID device. A suitable exemplary device is the model AT24RF08C available from Atmel Corporation of San Jose, California."

Patent # 5,438,329, *Duplex Bi-Directional Multi-Mode remote Instrument Reading and Telemetry System*, August 1, 1995, the patent for the Sensus MXU Model 550 Meter Transceiver Unit (MXU) is very informative:

- "The instrument link 2 includes a microcontroller, such as an Intel 8051 family integrated circuit, to evaluate signals from the remote station and to control all the instrument link functions except those associated with the one second timer, the auto transmit counter, and the functions associated with those components."
- "The Electronically Erasable Programmable Read-Only Memory (EEPROM) interfaces with the microcontroller through a serial interface and provides one (1) kilobit (Kbit) of non-volatile storage. The EEPROM provides a means for storing configuration parameters and data that must be saved when the microcontroller is powered down (i.e. the instrument link sleep mode). For example, the EEPROM stores diagnostic data relating to the performance of the instrument link and a remote station. The EEPROM may be a Thompson 93C46 or equivalent."
- "An interrogation signal preamble is followed by a interrogation message that is preferably a Manchester encoded message at a data rate of 1 kbit per second. The interrogation message contains a variety of parameters including the interrogation mode (blind or geographic), instrument link ID with possible wild cards, reply window length, reply RF channel to be used, the pseudorandom code to be used for spread spectrum modulation, the reading cycle number, and the data to be transmitted (i.e. register reading or diagnostic information). Such a message is typically protected against transmission bit errors by a 16 bit CRC field."

These patents tell us a few things – that the smart water meters use standard micro-electronic embedded components, and that they have very small on-board memory and processing capability, as well as providing useful information to the attacker as well as to the security researcher to use to find and hopefully rectify vulnerabilities.

Review of some datasheets

Overview (incomplete) of frequencies used by other major wireless water meter manufacturers for the US market and whether they use FHSS, DHSS, or encryption.

Manufacturer	**Frequency**	**FHSS/DHSS**	**Security**
Aclara (Hexagram)	450 – 470 MHz		
Badger (Itron)	902 – 928		
Landis+Gyr (Cellnet)	902 – 928		

Datamatic	902 – 928	FHSS	
Elster AMCO (Severn)	902 – 928	FHSS	
Inovics	902 – 928	FHSS	
Itron	910 – 920		
Master Meter	902 – 928	DSSS	Encryption
Mueller (Hersey)	902 – 928	FHSS	
Neptune	900 – 950	FHSS	None
Performance	902 – 928	FHSS	
RAMAR	902 – 928		
Sensus	900 – 950	DSSS	Encryption

Most smart water meters in the US operated in the 902-928 MHz ISM band, and most use Frequency Hopping Spread Spectrum with no encryption.

IV. THE YEAR IN DRINKING WATER SECURITY[15]

There were some new developments in 2010 and the first 6 months of 2011 which should heighted our concern over the security of drinking water facilities:

- Stuxnet, the game changer, which came to light in June, 2010, is the first malware specifically designed to attack SCADA systems. Stuxnet potentially shows the way for a cyber attack on a water treatment plants as well as other infrastructure SCADA systems.
- Operation "Night Dragon," identified by McAfee[16], was a "coordinated covert and targeted cyberattacks.. conducted against global oil, energy and petrochemical companies." The objective appeared to be theft of intellectual property and trade secrets.
- Marc Maiffret[17], while performing a penetration test[18] in June, 2011 for an unnamed Southern California water utility, was able to gain control of the utility's chemical control

[15] This section is an update and expansion of the subjects covered in my DEF CON 18 presentation, *Cyberterrorism and the Security of the National Drinking Water Infrastructure*, http://www.defcon.org/images/defcon-18/dc-18-presentations/McNabb/DEFCON-18-McNabb-Cyberterrorism-Drinking-Water.pdf

[16] *Global Energy Cyberattacks: "Night Dragon"* white paper by McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011.

[17] Marc told me 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.

[18] *Virtual war a real threat*, Ken Dilanian, Los Angeles Times, March 28, 2011. http://articles.latimes.com/2011/mar/28/nation/la-na-cyber-war-20110328

systems in less than a day. The route of exploitation was workers who were able to remote into the SCADA system from home.

Importance of Drinking Water

Water, simply put, is essential for life. While nearly 70 percent of the world is covered by water, only 2.5 percent of it is fresh water. The rest is in the ocean. Of the rest, only 1 percent is accessible – the rest is trapped in glaciers and snow cover. Only 0.007 percent of the planet's water is available to its nearly 7 billion people.

A survey[19] conducted in 2010 by the engineering firm ITT found that 95% of American voters value water over any other service they receive, including heat and electricity, nearly one in four American voters is "very concerned" about the state of the nation's water infrastructure 29% percent of voters agree that water pipes and systems in America are crumbling and approaching a state of crisis, 80% of voters say water infrastructure needs reform; and about 40% say major reform is needed.

Water is a scarce commodity. 1.1 billion people in the developing world do not have access to clean drinking water, and 2.4 billion lack access to proper sanitation. Water use has been growing at twice the rate of population increase for the last 100 years. Lack of clean drinking water reduces food production, stifles economic growth, and leads to disease and death on a wide scale. Population growth, development, deforestation, and global warming further reduce available fresh water resources.

Water scarcity and availability has been a source of conflict and war[20] throughout human history. For example, water has been cited as a contributing factor in the recent conflicts in Darfur, Sudan (drought), between Pakistan and India (Indus River), between Israel, Jordan & Syria, Egypt and Ethiopia (the Nile River), and between Singapore and Malaysia (which threatened to cut off Singapore's water supply). As Mark Twain said "Whisky's for drinking, water's for fighting."

Water is a $400 billion global industry. Water has been called "the new oil." Private companies all over the world are increasingly acquiring drinking water resources and infrastructure which previously was publicly owned. This increased privatization, according to critics, leads to higher water prices, increased stress on water resources, and loss of democratic control over water resources.

Water is a critical infrastructure[21]. Drinking water and wastewater is essential to support the 17 other national critical infrastructures. In particular, the following critical infrastructures would be severely adversely affected by a failure of the water sector -- emergency services, healthcare facilities, schools, transportation, energy production, postal and shipping services, telecommunications, and food & beverage production and preparation

---

[19] ITT *Value of Water Survey*, October, 2010.
http://www.itt.com/valueofwater/media/ITT%20Value%20of%20Water%20Survey.pdf

[20] See "*Water conflict chronology*" by Dr. Peter H. Gleick, The Pacific Institute, http://worldwater.org/conflict.html

[21] Critical infrastructure is defined in the Patriot Act (P.L. 107-56) as "*systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters*" (Sec. 1016(e)).

Terrorist threats to drinking water

Al Qaeda has repeatedly threatened to "poison" United States drinking water supplies. Abu Mohammed al-Ablaj, a spokesman for al-Qaeda, stated on May 25, 2003, that "Al-Qaeda [does not rule out] using sarin gas and poisoning drinking water in U.S. and Western cities…" In 2008 an Al Qaeda website called on members to poison US drinking water supplies.

In 2002, the FBI arrested 2 individuals in the US with Al Qaeda ties with documents in their possession about poisoning US drinking water supplies. The FBI then issued a bulletin to computer security experts saying that "US Law enforcement and intelligence agencies have received indications that Al-Quida members have sought information on supervisory control and data acquisition (SCADA) systems available on multiple SCADA-related websites… They specifically sought information on water supply and wastewater management practices in the US and abroad."

Documents seized at the Tarnak Farms Al Qaeda training camp near Kandahar, Afghanistan, after it was attacked by US forces in 2002, show plans to poison US drinking water and food supplies with pathogens.

In September 2003, the FBI warned that terrorists might use two naturally occurring toxins, nicotine and solanine, to poison U.S. food or water supplies.

Historically[22], homegrown terrorists have targeted and attacked US drinking water supplies numerous times. For example:

- 1972 – two members of "Order of the Rising Sun" arrested in Chicago with botulism, meningitis, anthrax and 30 – 40 kg of typhoid cultures to poison water supplies in Chicago, St. Louis, and other cities.
- 1977 – a North Carolina reservoir was contaminated successfully with an unknown poison chemical, shutting down the reservoir
- 1980 – Pittsburg water mains were contaminated with a weedkiller
- 1984 – members of Rajnessshee religious cult contaminate Dallas, Oregon city water storage tank with Salmonella, causing an outbreak of 750 cases of Salmonella poisoning.
- 1985 – federal officials learn of a plot by the survivalist group The Covenant, Sword and the Arm of the Lord to contaminate New York City's water supply with a 30 gallon drum of potassium cyanide.

National drinking water infrastructure

An attack on the entire national drinking water infrastructure is unlikely, if not impossible, because of the fragmented[23] nature of the infrastructure. There are over 150,000 separate drinking water utilities in the United States. While some can be connected to provide backup water in case of emergency, and some share water supplies, at attack one does not threaten any of the others. Unlike the inherently interconnected electrical infrastructure, where a

[22] See "*Water and terrorism*" by Peter Gleick, http://www.pacinst.org/reports/water_terrorism.pdf

[23] *Challenges In The Water Industry: Fragmented Water Systems*, American Water, http://www.amwater.com/files/FragmentedWaterSystems012609.pdf

fault or attack on two nodes could bring down an entire grid[24], water utilities are separate entities that would have to be attacked one by one.

Also, each water utility is designed differently, in effect each one is a "one off" design based on specific local requirements based on water quality, location of water resources, growth of the served community over time, and other factors.

There has been some consolidation in the US water infrastructure, in the form a few water companies that span multiple states. American Water, the largest, serves 16 million people in 1,600 communities and 35 states. Their water facilities, however, are not connected in any way, but all their facilities are served by the same computer network for administrative purposes. The other water conglomerates include Aquarion Water and US Water.

However, since about 90% of US water utilities use chlorine for disinfection, that chlorine could serve as a potential Achilles heel[25]. About 43% of chlorine is produced in Louisiana and is transported by rail from there across the United States. An adversary could disrupt a significant portion of US drinking water production by attacking those chlorine plants or the rail lines they use. A less likely, but not impossible, scenario is that if an adversary could contaminate the chlorine with a radioactive substance then a very large proportion of the US population could be poisoned all at once through this attack vector.

Another important factor to consider is that the physical infrastructure of the national drinking water system[26] is crumbling. Decades of deferred maintenance have left the country with thousands of miles of decaying 100 year old water mains, clogged distribution systems prone to frequent water main breaks, substandard and failing treatment plants, broken and unusable fire hydrants, and insufficient storage capacity to provide fire protection. The American Society of Civil Engineers gives the nation's drinking water infrastructure a D- grade and estimates that an investment of $255 billion[27] is needed to bring the system to needed standards.

Water system components & potential vulnerabilities

A drinking water utility is composed of four primary physical components: supply, treatment, storage, and distribution. Although nothing should be ruled out entirely, the potential vulnerabilities of each component are examined below:

Component	Characteristics	Vulnerability
Supply	• Well fields & reservoirs • Large volume of water that	• Cost to monitor reservoir is very high and not 100%

[24]Wang, Jian-Weng and Li-Li Rong, *Cascade-based attack vulnerability on the US power grid,* Safety Science, Volume 47, Issue 10, December 2009, pp. 1332-1336

[25] See *Chlorine: the Achilles Heel?* Presentation at the 2009 American Water Works Security Congress, by John McNabb.

[26] See *Analysis of the Massachusetts Drinking Water Infrastructure* by John McNabb, presented at the September 18, 2008 New England Water Works Conference, http://www.newwa.org/PDF/AnnConf08-SessC1040.pdf, and published in the December, 2010 Journal of the New England Water Works Association, http://www.southshorepcservices.com/Analysis_Mass_Water_Infrastructure-NEWWA-Dec2010.pdf

[27] http://www.infrastructurereportcard.org/fact-sheet/drinking-water

	would require large amount of contaminant to overcome dilution. • Reservoirs are difficult to monitor and impossible to fully protect	• Since water goes to treatment, this reduces vulnerability. • Because large amount of contaminant needed, • **Low risk**
Treatment	• Treatment plants usually in enclosed buildings with fencing, video surveillance, alarm systems, relatively easy to adequately protect. • Each treatment plant is unique.	• Since each plant is unique, would require substantial research & local knowledge to change process to poison water • **Low risk.**
Storage	• Finished storage tanks collect water not used in distribution for use when treatment plant not running. • Also provide pressure to the system equal to that provided by the plant's high lift pumps.	• Water here is after treatment and not tested for more than coliform, so contaminants unlikely to be detected. • There are very few storage tanks in any system so they are easy to adequately guard. • **Low to Medium risk.**
Distribution	• Even a small utility will have dozens of miles of water mains and hundreds of fire hydrants. • Large utilities will have hundreds of miles of water mains and thousands of fire hydrants.	• Water mains and hydrants are usually not fully maintained because of costs. • Impossible to fully protect all water mains & hydrants from attack, too many of them. • **Medium to High risk.**

Most likely physical attack scenario

The most likely attack vector is through the distribution system, which is the most vulnerable[28] component. Studies show that effective attacks through the distribution system can be easily mounted with chemical biological or radioactive (CBR) agents for $0.50 to $5.00 per death. The method is referred to as a "backflow attack" and can be implemented by a single person with easy to obtain chemicals and pumping equipment.

In the backflow attack, pumps such as used by lawn chemical companies are used to inject chemicals, which could be weed killer or any one of a number of CBR agents, into the distribution system. The injection point could be any existing connection to the distribution system, such as a fire hydrant or a connection in the basement of a building where the activity couldn't be detected. The pump needs to exceed the pressure gradient of the water in the systems

[28] GAO-04-29, *DRINKING WATER: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*, October, 2003.

water mains, usually around 80 lbs/cubic inch. It is estimated that using this method, a few gallons of a toxic agent could contaminate the system of around 150,000 in just a few hours[29].

This same method could also be used to target a specific building or facility. With knowledge of the hydraulic conditions in the distribution system, and some calculations, an adversary could inject a relatively small amount of toxin in a fire hydrant near the facility which would result in a lethal dose being received in the water at that location.

The only effective defense for such attacks is continuous real-time monitoring of the quality of the water in the distribution system. There are many such monitoring systems on the market today but so far very few systems have installed them because of the cost and, so far, little perceived need for them.

Supervisory Control and Data Acquisition (SCADA)

Supervisory Control and Data Acquisition (SCADA)[30] 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.

The Israeli IT security firm C4 described[31] this transition very well:

> Control systems were initially built from relatively simple electric and mechanical devices. A typical control room would have hundreds of buttons, dials, levers and gauges in every form, shape and color. The control system as a whole was dedicated solely for the control purposes and therefore was stand-alone in nature. In the past 20 years three changes impacted the security of control systems, technological and business-induced:
>
> 1. As the computing power and "off the shelf" capabilities of general purpose PCs and servers increased dramatically over the years, standard computers and commercial operating systems gradually replaced their electrical and mechanical predecessors.
> 2. Another technological shift that soon followed was a change from proprietary, serial communications to IP based networking. It is nowadays rare to find a control center that is not using IP as its primary communication

[29] Kroll, Dan., "*Water distribution monitoring: opportunities and challenges for enhancing water quality and security*." Hach Homeland Security Technologies White Paper July 2010, http://www.hachhst.com/wp-content/uploads/2010/07/White-Paper_-Enhancing-Security-in-Water-Distribution-System.pdf

[30] 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..

[31] *The Dark Side of the Smart Grid – Smart Meters (in)Security*, C4 security, September, 2009. http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf

protocol, and recently more and more field devices have a standard Ethernet/IP port alongside or instead of the more traditional RS232 port.

3. The corporate environment is constantly getting more competitive, and business executives became more computer-literate. These two factors lead for a demand by the corporate executives to obtain real-time data from the control network in order to improve their business performance. This need led to interconnection between the control and corporate networks.

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.

When these legacy systems were transitioned to SCADA, the components were fitted with Programmable Logic Controllers (PLC's), the individual wires were replaced by Ethernet cables and the control panel was replaced by SCADA HMI (Human Machine Interface) software operating on a personal computer running a Windows, Linux or Sun operating system. Most of them run on Windows. The dedicated communications channels for remote facilities were in most cases replaced by internet connections, 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 & mechanical registers.

SCADA systems were not designed with security in mind. Since they have in most cases have to run 24/7, they also are not designed to be easily patched. Most large water systems run all the time, 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.

They were also designed as isolated systems, so having them exposed on the internet increases the attack surface much more than the designers ever imagined. The Windows computers on which many SCADA/HMI systems are on are not routinely updated because they do not have regular internet access, making them more vulnerable from an attack from malware on a thumb drive or from the internet when access is possible into the computer.

SCADA Vulnerabilities

Historically, drinking water treatment facilities were isolated systems accessible only through physical access to the valves, chemical feed unites, and control panel in the water treatment plant. However, in the past three decades many water utilities have retrofitted their facilities by installing computer-controlled SCADA or other control system type hardware and software, which in most cases are accessible from the internet.

These utilities have in almost all cases installed their SCADA software on Microsoft Windows XP or Server 2003 systems, and in almost every case have placed the systems on the internet as well. These developments have greatly expanded the attack surface[32] of drinking water facilities, making them vulnerable to intentional or unintentional intrusions.

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

The 2004 report by the Government Accountability Office (GAO) reported that industrial control systems, previously isolated, were now more vulnerable because of:

(2) Adoption of standardized technologies with known vulnerabilities,
(3) Connectivity of control systems with other networks,
(4) Insecure remote connections, and
(5) Widespread availability of technical information about control systems.

A more recent report, *Common Cybersecurity Vulnerabilities in Industrial Control Systems*, May 2011, by the Control Systems Security Program, National Cyber Security division, at the Department of Homeland Security, concluded that the most commonly found vulnerabilities in industrial control systems were:

(1) Credentials management
(2) Weak firewall rules
(3) Network design weaknesses.

The *Roadmap to Secure Control Systems in the Water Sector*[33] lists the following "water sector industrial control system risks today" as the following:

(1) Design limitations
(2) More Open Environments
(3) Increased Connectivity
(4) Increased Complexity
(5) System Accessibility
(6) Supply Chain Limitations
(7) Information Availability

New SCADA vulnerabilities continue to be discovered

Over the past 18 months, in addition to Stuxnet, there have been a plethora of vulnerabilities revealed in SCADA software used around the world and in water utilities.

Symantec reports[34] that there have been 15 SCADA vulnerabilities disclosed in 2010, an increase of one over the 14 publicly disclosed in 2009.

In March, 2011, security researcher Luigi Auriemma released proof of concept code on 34 SCADA vulnerabilities to Bugtraq, which was followed by 4 advisories on them and one related additional advisory from ICS-CERT.

One or more additional SCADA vulnerabilities are expected to be disclosed in other talks here at Black Hat USA this year.

[33] *Roadmap,* page 14.
[34] Vulnerability Trends – SCADA Vulnerabilities, Symantec. http://www.symantec.com/business/threatreport/topic.jsp?id=vulnerability_trends&aid=scada_vulnerabilities

Control System Incidents

The January 21,2010 *Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats* report, by GreyLogic, found that:

- state and/or non-state actors from China, Russia, and Turkey are "almost certainly" targeting and penetrating the networks of energy providers and other critical infrastructure in the US and other countries, and that network attacks on the power grid will escalate over the next 12 months;
- "100 smart grid projects distributed across 49 states have been funded by federal grants and industry contributions equaling about $8 billion… the rush to implement this technology before serious vulnerabilities are addressed and patched serves to make the Grid more vulnerable to cyber attacks."

The January 28, 2010 *In the Crossfire Report* by McAfee surveyed 600 IT and security executives from critical infrastructures in 14 countries all over the world – who reported that their networks and control systems are under repeated cyberattacks, and that the reported cost of downtime from major attacks is more than US$6 million a day. Some other interesting findings are that:

- 75% of control systems overall are connected to the internet or other IP network, in the water/wastewater sector only 55% are so connected;
- 33% overall have policies that restrict or ban the use of USB sticks or other removable memory;
- 77% in the water/wastewater sector said that government regulation has either diverted resources from improving security or had no effect;
- "New service delivery platforms like the interoperable 'smart grid' of electricity or banking on mobile devices create new vulnerabilities, but also offer new opportunities."

The 2011 edition, released March 4, 2011, of the Repository of Industrial Security Incident's (RISI) *RISI Water/Wastewater Sector Analysis Report*[35] reported that the repository contained 25 confirmed water sector incidents which occurred between 1998 and 2010, and that 13 of them were the result of unintentional control/SCADA failure.

The April 18, 2011 report by McAfee and CSIS, In *the Dark - Crucial Industries Confront Cyberattack*, reported on a survey of 200 IT security executives at critical infrastructure facilities – including water supply facilities – in 14 countries. The results are that 40% believed that their vulnerability had increased since last year. McAfee concludes that "they are not ready" for a cyberattack.

> Despite these vulnerabilities, many power companies are doubling down on the danger; they are implementing "smart grid" technologies that give their IT systems more control over the delivery of power to individual customers — or even to individual appliances in customers' homes. Without better security, this increased control can fall into the hands of criminals or "hacktivists," giving them the ability to modify billing information and perhaps even control which customers or appliances

[35] *SCADA Report: Incidents Continue to Grow*, http://www.isssource.com/scada-report-incidents-continue-to-grow/

> get electricity. But security is not a priority for smart grid designers; according to [former Director of Central Intelligence Jim] Woolsey] ….."Ninety to ninety-five percent of the people working on the smart grid are not concerned about security and only see it as a last box they have to check."[36]

Other findings include:

- 30% said that their company was not prepared for a cyberattack.
- 80% said they had been hit with a large-scale Denial of Service (DDos) attack (an increase over the 50% reported last year)
- 25% reported getting daily or weekly DDos attacks.
- 70% said they frequently found dangerous malware on their systems.
- 85% reported at least one network intrusion.
- 25% said they had been a victim of cyber extortion
- 40% reported they had found Stuxnet on their systems
- 46% of the water & wastewater sector adopted additional security measures, up from their 38% adoption rate last year

Known Water System SCADA Cyber Attacks

There is a short list of known or disclosed SCADA cyber attacks involving drinking water and wastewater facilities, which includes the following: –

- **1994** – Salt River Project Water Dept., Arizona; 27 year old hacker reportedly broke into computers but was never in control of dams [this story is in dispute]
- **2000** – Maroochy Water System, Australia; former consultant took control of wireless pump system to spill 264,000 gallons of raw sewage onto waterways.
- **2006** – Harrisburg, PA 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
- **2010** – Cyber criminals hacked into the North Garland County Regional Water District, Arkansas and stole $130,000
- **2011** – Water utility (unnamed) reported cyber incident when remote users were unable to log on, according to an ICS-CERT report.

Measuring Water Security Progress

The progress of US drinking water systems to improving their overall security was assessed in a talk[37] given at the September 21, 2010 American Waterworks Association (AWWA) Water Security Congress.

[36] *In the Dark*, page 1.
[37] *Measuring Water Security Progress*, L. Vance Taylor, AWWA Water Security Congress, September 21, 2010, National Harbor, Maryland.

The metrics used were developed by the Critical Infrastructure Partnership Advisory Council (CIPAC) and were collected & aggregated by the Water Information Sharing and Analysis Center (WaterISAC).

The Water Sector's Security vision is: "*a secure and resilient drinking water and wastewater infrastructure that provides clean and safe water as an integral part of daily life. This Vision assures the economic vitality of and public confidence in the nation's drinking water and wastewater through a layered defense of effective preparedness and security practices in the sector*."

The Summary of Results includes:

- 70%+ had incorporated security planning & design programs to all assets and facilities
- 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 & monitor shipping, receipt & storage of hazardous chemicals
- 85%+ integrated security & preparedness into budgeting, training & manpower responsibilities
- 90%+ have developed emergency response plans
- 50%+ are training, exercising, reviewing & 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

NOTE: *Of the "22 Sector Specific Measures" which were the basis for the metrics, <u>none of them addressed SCADA or Cyber security</u>.*

***Roadmap* to Nowhere?**

In March 2008, the Water Sector Coordinating Council Cyber Security Working Group developed the *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."

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 the following four goals:

- Develop and Deploy ICS Security Programs

- Assess Risk
- Develop and Implement Risk Mitigation Measures
- Partnership and Outreach

The *Roadmap* has 18 Near-Term (0-1) years milestones, including "isolate ICS from public switch networks" and "Replace default security passcodes," but I cannot find any "progress reports" anywhere that detail how many of these milestones, if any, have been accomplished.

Regulatory Environment

The Bioterrorism Preparedness and Response Act of 2002 (P.L. 107-188, 42 U.S.C. 300i) amended the Safe Drinking Water Act[38] 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[39] had only one question regarding general PC security (passwords, etc.) and did not address control system security. Furthermore, neither the Bioterrorism Act, nor any other federal law or regulation, did NOT:

- require any water utility to actually make security upgrades to address vulnerabilities; or
- 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.

There has been progress in developing the following resources to assist local water utilities to protect against cyber attacks:

- Training, information, and workshops on security issues are provided through the US EPA, American Water Works Association, Water ISAC, and other affiliated organizations.
- Cyber Security Evaluation Tool (CSET), which is "a desktop software tool that guides users through a step-by-step process to assess their control system and information technology network security practices against recognized industry standards. The output from CSET is a prioritized list of recommendations for improving the cybersecurity posture of the organization's enterprise and industrial control cyber systems."[40]
- 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.

[38] Tiemann, Mary*, Safeguarding the Nation's Drinking Water: EPA and Congressional Actions*, September 30, 2010.
[39] *Security Vulnerability Self-Assessment Guide for Small Drinking Water Systems*, Association of State Drinking Water Administrators National Rural Water Association May 30, 2002
[40] Control Systems Security Program, US-CERT, http://www.us-cert.gov/control_systems/satool.html

Stuxnet

Stuxnet is a game-changer because it is the first known malware to effectively attack SCADA systems. Symantec, in its Stuxnet Dossier[41], described how Stuxnet worked; which was summarized by Symantec as follows:

> Stuxnet is 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.
>
> Stuxnet was discovered in July, but is confirmed to have existed at least one year prior and likely even before. The majority of infections were found in Iran. Stuxnet contains many features such as:

- Self-replicates through removable drives exploiting a vulnerability allowing auto-execution.
- Spreads in a LAN through a vulnerability in the Windows Print Spooler.
- Spreads through SMB by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability
- Copies and executes itself on remote computers through network shares.
- Copies and executes itself on remote computers running a WinCC database server.
- Copies itself into Step 7 projects in such a way that it automatically executes when the Step 7 project is loaded.
- Updates itself through a peer-to-peer mechanism within a LAN.
- Exploits a total of four unpatched Microsoft vulnerabilities, two of which are previously mentioned vulnerabilities for self-replication and the other two are escalation of privilege vulnerabilities that have yet to be disclosed.
- Contacts a command and control server that allows the hacker to download and execute code, including updated versions.
- Contains a Windows rootkit that hide its binaries.
- Attempts to bypass security products.
- Fingerprints a specific industrial control system and modifies code on the Siemens PLCs to potentially sabotage the system.
- Hides modified code on PLCs, essentially a rootkit for PLC's.

While the objective of Stuxnet does appear to be to damage the Iranian nuclear program, its methodology could be applied 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.

If that day comes, then the question is -- does the water sector have the capability to defend against a zero day attack through USB drives? Right now the answer to that question is "NO."

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

DHS Open Source Infrastructure Reports

The US Department of Homeland Security (DHS) issues every business day an Open Source Infrastructure Report[42] which summarizes news from the previous day that affects each of the critical infrastructures.

In 2010 there were a total of 239 reports which listed a total of 914 "Water Sector" incidents, which included stormwater, wastewater, regulatory actions, news stories, and other reports, including 246 incidents at water treatment facilities, which is what we are concerned about here.

These 246 incidents at water treatment facilities break down as follows:

Contamination	71
Water main breaks	79
Chlorine leaks	18
Plant malfunction	13
Vandalism	12
Trespassing	8
Other	41
Computer problem	4

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. There was one incident of a " terrorist threat," which turned out to be a hoax.

However, the four computer-related incidents bear some examination, they are as follows:

- March 11, Silver City, New Mexico *Silver City Loses 3 million gallons in water leak*[43]. The city recently installed a new SCADA system, which caused a water hammer that broke a pipe to water tanks which quickly drained. (Possibly a SCADA malfunction.)
- June 23, Lake Chelan, Washington. *Computer failure interrupts flow from city water plant*[44]. On June 13 the plant's computer failed the plant stopped operating. (No other details available.)
- September 20, Glidden, Iowa. *Iowa town asked to conserve water after computer problem drains water tower*[45]. On the Sept. 19 there was a computer malfunction which

[42] 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.
[43] Silver City Sun News, March 11, 2010. DHS Open Source Report, March 12, 2010, p. 13.
[44] Lake Chelan Mirror, June 23, 2010 http://lakechelanmirror.com/main.asp?SubSectionID=5&ArticleID=2670&SectionID=5
[45] Associated Press, September 20. http://www.whotv.com/news/who-story-glidden-water-tower-092010,0,1010748.story

apparently shut down the plant, draining the town's water storage tank. (No further details available.)

- December 4, First taxing District Water Dept., New Canaan, Connecticut. *Computer glitch shuts down water plant*[46]. The computer shut down the plant, except water was still pumped into the plant, causing flooding from the plant across the nearby roadway. (Again, no further details available).

Looks like there are some small water utilities who need redundant computer systems, at the very least.

Conclusions

Are US drinking water utilities less vulnerable or more vulnerable to cyber attack than they were on January 1, 2010? One would have to conclude, based on the reporting herein, that they are **MORE VULNERABLE**.

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[47] 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. Here is a taxonomy of possible attacks[48] based on the protocol stack:

(1) Physical layer
  (a) Jamming
  (b) Radio interference
  (c) Tampering or destruction

(2) Data link layer
  (a) Continuous channel access (exhaustion)

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

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

[48] Ibid, pp. 037-039

(b) Collision
(c) Unfairness – a partial DOS attack
(d) Interrogation – exhausts resources
(e) Sybil attack – single node presents numerous identities

(3) Network layer
(a) Sinkhole – route all traffic to one node
(b) Hello Flood
(c) Node capture – capture of one node can allow takeover of entire network
(d) Selective forwarding/ Black Hole Attack (Neglect and Greed)
(e) Sybil attack
(f) Wormhole attack
(g) Spoofed, altered, or replayed routing information
(h) Acknowledgement spoofing
(i) Misdirection
(j) Internet smurf attack
(k) Homing

(4) Transport layer
(a) Flooding
(b) De-synchronization attacks

(5) Application layer
(a) Overwhelm attack
(b) Path based DOS attack
(c) Deluge (reprogram) attack

WSN's present many security[49] 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 or 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*."[50] This may be the first tool purposely written to penetrate the confidentiality and functionality of a sensor network.

[49] *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]
[50] *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]

Vulnerabilities of the "Smart Grid"

The electric Smart Grid has been under a lot more scrutiny than the drinking water component. While some of the characteristics of the electric grid, such as the complete interdependence of the electric grid, are not mirrored in the drinking water infrastructure, which is highly fragmented, the characteristics of the hardware & firmware used in smart electric meters, and their vulnerabilities, may be applicable to smart water meters.

Jonathan Pollet of Red Tiger Security, in his Black Hat USA presentation[51] last year, listed existing vulnerabilities of the electric grid's AMR and Smart Meters:

- Perimeter Issues. These systems are interconnected with business applications and often also interconnected to operational SCADA and energy Management systems.
- Back End Server/Application issues. The applications have similar vulnerabilities as do business applications, have less secure implementation of protocols, and have old versions of application frameworks.
- Too much trust in the Protocol. Most AMI/AMR vendors trust that the 802.15.4 protocol security implementation will work and haven't considered what to do when it doesn't.
- End devices have limited resources. The meters themselves typically do not have the resources (memory, computational power, etc.) to handle security features.

What could an attacker do to these electric Smart Grid systems, considering those vulnerabilities? Pollet listed the following capabilities exist for an attacker, which his firm has duplicated in their own research:

- Data enumeration - read real time grid data.
- Host enumeration - scanning from meter back to the head-end
- Service enumeration – determine what services are exposed
- Change data (such as change usage & billing data)
- Steal accounts and passwords (man in the middle attacks + Wireshark)
- Damage core system components (i.e. bricking meters)
- Denial of Services (PING FLOOD, malformed packets, etc.)

What could a hacker do to the smart grid?

Smart Grid vulnerabilities have been documented[52] by the Israeli IT security firm C4 following security audits on a water pipeline and two electric grids; they also listed potential attacks based on those vulnerabilities:

(1) DDos attacks are possible where the smart grid uses public IP addresses;
(2) Each meter is a node in the smart grid network; so an attacker who uses the communication module of the smart meter can cause network-wide changes;

[51] *Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters*, Jonathan Pollet, Black Hat USA, 2010

[52] *The Dark Side of the Smart Grid – Smart Meters (in)Security*, C4 security, September, 2009. http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf

(3) Many meters did not have any authentication or encryption support, allowing an attacker to impersonate the control center and send unauthorized commands to meters or read metering data;
(4) The protocol between the master meter and slave meter is usually considered of lesser importance because its impact is restricted to a single customer household; however this may allow the insertion of a "man in the middle" device to lower the usage reading, which could be of considerable impact to the utility if such devices are mass produced like pirate cable boxes;
(5) Some slave meters that support disconnection of the customer use wireless protocols, making it possible for an attacker to disconnect multiple customers;
(6) Many meters were unable to improperly handle malformed requests, making them vulnerable to a Buffer Overrun/Overflow Vulnerability; allowing the attacker to execute arbitrary code;
(7) The capability to remotely execute firmware upgrades can allow an attacker to disconnect the meter or take any other action; and
(8) Lack of input validation could allow an attacker to submit a malformed packet which could lead to arbitrary code execution.

What could a hacker do to the water utility control systems?

The Roadmap to Secure Control Systems in the Water Sector listed[53] the following potential impacts from an attacker:

- Interfere with the operation of chemical feed systems, to cause over or under dosing;[54]
- Make unauthorized programming changes, resulting in disabled services, reduced pressure or flows of water into fire hydrants;
- Modify control system software to produce unpredictable results;
- Block data or send false information to operators to prevent them from being aware of alarm conditions;
- Change or disable alarm thresholds;
- Prevent access to account information;
- Cause multiple failures that may be too much for the facility to manage;
- Be used as ransomware

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 form found that about 33% would

[53] *Roadmap*, page 15.
[54] Just as Marc Maiffret was able to do in his pen test of an unnamed California water system. "We did not change anything or go beyond showing access to the control system where an operator could then make changes at the point of access we had. In this specific case the filtration levels of different chemicals could be manipulated. Specifically one of the plant engineers and I came up with the maybe not so funny joke "SCADA Sport Fishing." And I believe that had to do with a modification of chlorine levels…" Email from March Maiffret, April 18, 2011.

be discouraged from using smart metering if it gave the utility more data about their energy use.[55] There are many scenarios where such information could be used as an invasion of privacy, as summarized in this table:

WHO WANTS SMART METER DATA?	HOW COULD THE DATA BE USED?[56]
Utilities	To monitor electricity usage and load; to determine bills
Electricity usage advisory companies	To promote energy 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

Similar concerns may be raised, one would think, with smart water meters, which could show information based solely on the total water usage if reported in short intervals of 5-15 minutes, about whether a house was occupied, and when, when people were awake, how many people were in the house, how many times they took a shower, used the toilet, etc. Especially in addition to smart grid electric load information, one could get a good picture of human activity in a house that would be an invasion of privacy.

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

[55] *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.

[56] 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

using at any point in time, and probably figure out what you are using it for." [57] [emphasis in original.]

A few weeks ago, in early November 2009, the Town of Cary Council approved the purchase and installation of smart wireless water meters at a cost of $17. 9 million. This installation makes Cary the first municipality in North Carolina, the USA and perhaps the world that will have a metering system that will be used by "Water Conservation Technicians" (aka **Water Cops**) to monitor (i.e. **spy**) on our consumption of water on a minute by minute basis, 24 hours per day and 7 days a week for the purpose of enforcing water conservation measures. 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. Many citizens are appalled that the Town of Cary has found it necessary to resort to **such extreme measures** to get citizens to conserve water. A civilized society depends upon its citizens to **voluntarily** follow the rules and in most communities this is enough. Do our leaders think of us as **unsophisticated wild animals** that need constant policing to assure compliance? In fact there has been discussion and consideration of **adding water cops** commensurate with population growth. Will we soon have "Block Captains" to report on a resident's behavior and compliance with the rules? Immigrants from eastern Europe tell us that the right to privacy is precious. If you give up this right it won't be long before the government starts to erode all rights. Do we want that in Cary? [58][emphasis in original.]

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) before deciding to participate in the Smart Grid to identify risks to the personal information 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) Privacy Principles and other sector's privacy policies, regulations, and laws that may be applicable.
(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.

[57] *Utility Expert describes privacy invasion through AMI*, The Cary Watchman, January 28, 2010. http://carywatch.net/watermeter.html
[58] *Cary leads the nation, in Water Cops*, The Cary Watchmen, January 4, 2010.

(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 the smart meter operations.

Beyond the Smart Grid: Hydrosense

But… it gets better!

The amount and quality of information that can gathered about human activity in a household, which is limited when relying just on the water usage information from the water meter, can be supplemented to provide a complete picture of water use by a new device called HydroSense.

HydroSense[59] is a simple, single point, sensor of pressure of water in a building, which can give accurate information about when each water fixture is turned on and for how long. Each water fixture can be accurately identified by sensing the pressure at a single point in the buildings infrastructure. The information is then sent via wireless – perhaps "backhauled" over the same wireless channel used by the water meter – to the water utility to accumulate the information. Hydrosense works based on the following theory of operation:

- The home plumbing system forms a closed loop pressure system
- The instant a valve is opened or closed a pressure change occurs and a pressure wave, also called a surge or water hammer, is generated;
- The unique transient water hammer signature sensed for a particular fixture depends on the valve type and its location in the plumbing network of the home;
- One can discriminate between fixtures of the same type that are in different locations because their pressure wave impulses traverse different paths through the pips;
- This allows one to use Hydrosense to estimate flow rate, which is related to pressure change via Poiseuille's Law, which is that the volumetric rate of fluid in a pipe Q is dependent on the radius of the pipe r, the length of the pipe l, the viscosity of the fluid μ and the pressure drop ΔP.
- Hydrosense measures the change in pressure ΔP

Hydrosense is a simple, screw-on device that doesn't require the services of a plumber. It operates on battery power, or uses WATTR[60], a self-powered version that uses the flow of water to power the device. Then there is NAWMS[61]: the Nonintrusive Autonomous

[59] *Hydrosense: Infrastructure-Mediated Single-Point Sensing of Whole-Home Water Activity*, Froelich, Jon, Eric Larson, Tim Campbell, Conor Haggerty, James Fogarty, and Shwetak N. Patel, *Ubicomp 2009*, Orlando, Florida.
[60] *WATTR: A method for self-powered wireless sensing of water activity in the home*, Campbell, Tim, Eric Larson, Gabe Cohen, Jon Froelich, Ramses Alcaide, and Shwetak N. Patel, *UbiComp, 2010*.
[61] *NAWMS: Nonintrusive Autonomous Water Monitoring System*, Kim, Younghun, Thomas Schmid, Zainul M. Charbiwaia, Jonathan Friedman, and Mani B. Srivastava, *SenSys 2008*.

Water Monitoring System, which uses the flow information from the existing water meter in addition to one or more vibration sensors on water pipes.
These devices are part of a larger effort called *infrastructure-mediated sensing*, which is being applied to detect the use of gas (GasSense) and electronic devices (ElectriSense) as well as for electric devices and for water fixtures.

While these devices would be useful to assist homeowners and utility companies to track and control resource use, with obvious benefits to society, they offer substantial possibilities to the ultimate invasion of privacy, since they could allow one or more utility companies, or the government, an eavesdropper, or an attacker, to know just about anything that is done within the home.

VI. HACKS OF OTHER "SMART METERS" AND WIRELESS DEVICES

Other smart meters and wireless devices have been successfully sniffed & hacked, which lends confidence to the assumption that wireless water meters can also be hacked. Reviewing these case histories can be instructive to understand common elements that would also apply to wireless water meters and the process for attacking them.

Smart Parking Meters – Joe Grand, Jacob Applebaum, & Chris Tarnovsky

This, of course, is a different type of "meter" and the attack didn't involve any wireless component, although it could have. In their presentation *"Smart" Parking Meter Implementations, Globalism, and You*, at Blackhat USA 2009, Grand et al. followed a methodical process to postulate potential attacks, gather information, analyze the hardware, reverse engineer firmware, and analyze the smartcards used.

By looking at oscilloscope capture of San Francisco MTA smart card transactions, they were able to determine how to replay transactions with modified data to "obtain unlimited parking." They used a "shim" between the smart card and the meter to monitor the I/O transaction with a digital oscilloscope, and were able to decode the transmissions by hand. They then developed modified code to show that the card had the maximum possible value, and ported the code to a Silver Card to test on a meter.

They recommended some fixes to make these smart parking meters more secure: daily audit log/serial number correlation/blocklisting, reduce the number of access methods, incorporate antitamper mechanisms into the meter circuitry, abandon the offline system, and have meters communicate with a "mothership" using digital signatures for all transactions.

Smart Subway Fare Meters – Russell Ryan, Zack Anderson, Alessandro Chiesa

In their presentation "*Anatomy of a Subway Hack*" that a court order prevented them from giving at DEF CON 16 in 2008, these three MIT students demonstrated a thorough analysis of the vulnerabilities in the Boston MBTA subway electronic fare system. They attacked the RFID using a MiFare RFID reader/writer, and OpenPCD open design 13.56MHz RFID reader and emulator, and a USRP and GNU radio and a plugin they wrote.

They used GNU radio and a Universal Software Radio Peripheral (USRP) to sniff the RFID toolchain of the Charlie card smartcards communication with the card reader at 13.56 and

12.71 Mhz. They sniffed the handshake and used a KwickBreak FPGA Brute-Forcer to crack the key, allowing them to clone the cards.

They used a MSR206 Stripe card reader/writer that worked with their GPL'd software to read the Charlie Card, then reversed engineered the code to enable them to forge a card with a large stored value. They wrote Python libraries for analyzing magcards and integrated it with the MSR206 card reader/writer to allow them to forge cards.

Smart Electric Meters – IOActive

David Baker, Director of Services at IOActive, writes in the October 2009 Journal of Energy Security that

> "Most alarming is that "worm-able" code execution on standard smart meters has been achieved. The smart meter's chipset used for radio communication is publicly available in a developer kit format, and the radio interface's lack of authentication can be leveraged to produce a worm. If an attacker installed a malicious program on one meter, the internal firmware could issue commands to flash adjacent meters until all devices within an area were infected with the malicious firmware. Once the worm has spread to the meters, the attacker gains several abilities including:
>
> • Connecting and disconnecting customers at predetermined times.
> • Changing metering data and calibration constants.
> • Changing the meter's communication frequency.
> • Rendering the meter non-functional." [62]

In his Black Hat USA 2009 presentation, *Smart Grid Device Security*, Mike Davis described some of the inherent hardware & software problems of an electrical smart meter, an pointed out that the TI MSP430 chip has small stack space, no memory protection, can flash itself, and that malware can hook interrupt vectors allowing 'normal' meter function – that malware can patch and re-patch the firmware! He found that the meters also did not have effective encryption and couldn't tell the difference between another meter and one that was authorized to patch its firmware. He wrote a worm, self-replicating code, and ran it in a simulation of 22,000 nodes, and found that in less than 24 hours the work had taken over 15,000 of the meters.

Smart Electric Meters/Zigbee – Joshua Wright, Inguardians

In Killerbee*: Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic world"*, which he has presented Toorcon 11, Quahogcon, and a number of other conferences, Joshua Wright described ZigBee and the exploitation framework for it which he has developed. ZigBee used 2.4 GHz IEEE 802.15.4, DSSS modulation, and 128-bit AES-CCMP encryption, and is used for a multitude of applications such as smart thermostats, spill gates at dams, lighting, HVAC, and natural gas control, as well as electric meters.

[62] *Making a Secure Smart Grid a Reality*, David Baker, Journal of Energy Security, October, 2009

Zigbee keys are sent in plaintext, and has meager replay protection. Killerbee is a low-cost system, using the $40 AVR RZ Raven USB stick and software written by Wright, which can sniff, decrypt, and take over Zigbee controlled devices. NOTE: Inguardians also has prepared *Advanced Metering Infrastructure Attack Methodology*, which is very useful.

"How to sniff strange radio" – Travis Goodspeed

At the April 22, 2010 Source Boston, Travis Goodspeed presented "*Not quite ZigBee; or How to sniff a strange radio*," Travis showed how he reverse engineered a variety of "weird radios," such as radio remote controls, Apple/Nike+Show Pod, Garmin ANT+ Watch, and the Microsoft keyboard. After examining the die badges to identify the internal part number he was able to focus on Chipcon ISM Band, Nordic nRF24E1G, Amicom A7125, and other chips.

His methodology is to dissect a device, get part numbers, chip die photographs, & firmware, determine radio encoding, rate, and frequency, and then build a transceiver (such as the modified IM-ME "pink pager)." He cautioned that one needs to get the part numbers, because vulnerabilities are indexed by part numbers, not the product name; and that it is important to read the whole datasheet, and also read the errata sheets, you are sure to find bugs.

802.11 Frequency Hopping Spread Spectrum (FHSS) Hacks – Rob Havelt

At Black Hat 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 radio and a USRP 2.0 and how it is not inherently secure. "For legacy 802.11, it was possible to just use a USRP locked to a specific channel band, then feed the raw data into the BBN Adroit code - for kicks, you could set a file as the sniffer interface for Kismet or a tool like that to do analysis at each layer."[63]

Havelt explained that 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. FHSS uses the same type of management frames used in 802.11 b/a/n/g – Beacon, Associate, Probe, and Probe Response.

To join a FHSS network, he explained, you need either the SSID, MAC address of an authorized client, or a40 bit WEP key, but usually just the SSID will do. The SSID can be found in the Frame Body. The modulation, hop patterns and other parameters are similar to those in Bluetooth; so one can apply the Bluetooth ideas and methods[64] developed by Dominic Spill and Andrea Bittau, and of Spill and Michael Ossman. But, he finished, its easier than Bluetooth because with 802.11 FHSS you only need to use Software radio to listen for a management frame to hop by.

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

[64] See the Bluesniff project at http://gr-bluetooth.sf.net, and *Bluesniff: Eve Meets Alice and Bluetooth* by Spill and Bittau; http://darkircop.org/w00t.pdf, and *Building an All Channel Bluetooth Monito*r by Ossman & Spill; http://www.ossmann.com/shmoo-09/ossmann-spill-shmoo-2009.pdf.

FHSS 900 Mhz Wireless Sniffing – atlas, cutaway & Q

In their Shmoocon 2011 presentation *Hop Hacking Hedy*, atlas, cutaway and Q showed how FHSS was not inherently secure and how to crack it in 900 Mhz wireless devices using the CC1111EMK 868-915 Evaluation Module Kit programmed with Goodfet, using SmartRFstudio and 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. One must have the hopping pattern; must break the PRBG associated with the algorithm to obtain spread codes, analyze channel data in time domain fast enough to catch the hops until releases start to occur, and generate the entire pattern for all clock values[65].

The goal of their project was to build some devices that can be configured for known ISM bands, automatically analyze channel spacing, can decode FHSS hopping patterns, and utilize a custom code base. The hardware they selected was the CC111EMK868-915 Evaluation Kit because it was CC111-based, all the pins were broken out, it was programmable via Goodfet, and Goodfet interacts via Data Debug. The CC111 is the USB-enabled version of TI's popular <1 GHz radio, and is the same radio used in the majority of today's smart meters.

Their resulting firmware, after stripping Specan firmware code to remove display and shrink the frequency range and leveraging Goodfet for dumping Data Debug, using Python scripts for halting display, was maxscan, a spectrum analyzer, hoptrans to create a carrier wave where number of channels, channel spacing, and hop timing, is known, and minscan, to detect channel hops. Minscan initializes frequencies, scans frequencies for minimum RSSI, monitors jumps in RSSA, stores detected spikes, dumps data via Goodfet, and data is then analyzed offline.

Their project was still in development; they reported that channel identification was broken but close, there were some bugs in data storage and dumping, they still need to analyze and coalesce the final data better. One of their goals was to port it to the CC1110 of the IM-ME dongle (the "pink pager").

The code is available at http://code.google.com/p/hedyattack/

VII. METHODS THAT I AM WORKING ON TO SNIFF WATER METERS

The above cases, as well as other research, have informed my present efforts to devise one or more methods to sniff the signals from a 900 mhz wireless water meter and hack into the network. Although it seems obvious that it should be possible to do so, one cannot rest on such an assumption but must show how it can be done.

Because most US wireless water meters use the 902 – 928 Mhz ISM band, there are no suitable "off the shelf" devices to easily use, so it took some doing to see what could be put together. As of the date of the submittal of this paper, July 13, I have been working on the following potential methods to sniff & hack a 900 Mhz wireless water meter, and hope to show some success on at least one of these methods when I present this paper on August 3:

[65] They cite *Building an All-Channel Bluetooth Monitor* by Michael Ossman and Dominic Spill from Shmoocon 2009.

(1) **Itron FS3 Handheld Reader,** used, purchased on Ebay. This is the same unit used by water utility's to read the wireless meters onsite. Haven't gotten it to work yet.
(2) **Atmel RZ600 Development Kit.** Has a 900 Mhz antenna and is advertised to be capable of being used as a development platform or just for packet sniffing. However, it did not work right out of the box with the software supplied in the kit, and then their help desk informed me that they don't yet provide the software to use it for packet sniffing. I am experimenting with some software to link it to Wireshark, but no success to date.
(3) **Texas Instruments CC1111 868-915 Mhz Evaluation Module Kit.** Will use to try to replicate the FHSS technique demonstrated by atlas, cutaway & Q, after making a working Goodfet. (Thanks to Travis Goodspeed for sending me 5 Goodfet 31 circuit boards, hopefully I won't break all of them.) May also try Bus Pirate and a TI CC Debugger.
(4) **RFM DNT900DK.** The kit includes: two DNT900P radios installed in DNT900 interface boards, two 2 dBi dipole antennas with two U.FL coaxial jumper cables, two 9 V wall-plug power suppliers, 120/240 VAC, plus two 9 V batteries, and two RJ-45/DB-9F cable assemblies, one RJ-11/DB-9F cable assembly, and two A/B USB cables. Looks promising but haven't tried it yet.
(1) **FunCUBE Dongle Pro.** Just received it as of the date of submission of this paper. The FunCUBE Pro is advertised as a software defined radio that operates in the 64 – 1,700 Mhz range. I will see if I can use it to replicate Havelt's methodology.
(2) **IM-Me.** I am dying to replicate the uses of this pager which was demonstrated in "*Real Men Carry Pink Pagers*" by Travis Goodspeed and Michael Ossmann at ToorCon 2010, and see what other uses I can get out of it. I will try this if I have time.

VIII. 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.

REFERENCES

Advanced Metering Infrastructure Attack Methodology, Inguardians, Version 1.0, January 5, 2009.

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.

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

Anatomy of a Subway Hack, Russell Ryan, Zack Anderson, Alessandro Chiesa, presentation scheduled for DEF CON 16, 2008.

Common Cybersecurity Vulnerabilities in Industrial Control Systems, by Control Systems Security Program, National Cyber Security Division, at the Department of Homeland Security, May 2011

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.

The Dark Side of the Smart Grid – Smart Meters (in)Security, C4 security, September, 2009. http://www.c4-security.com/The%20Dark%20Side%20of%20the%20Smart%20Grid%20-%20Smart%20Meters%20%28in%29Security.pdf

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

Electricity for Free? The Dirty Underbelly of SCADA and Smart Meters, Jonathan Pollet, Black Hat USA, 2010

In the Dark: Crucial Industries Confront Cyberattack, by McAfee and the Center for Strategic and International Studies (CSIS), April 19, 2011

ITT *Value of Water Survey*, October, 2010. http://www.itt.com/valueofwater/media/ITT%20Value%20of%20Water%20Survey.pdf

GAO-04-29, *DRINKING WATER: Experts' Views on How Future Federal Funding Can Best Be Spent to Improve Security*, October, 2003

GAO -04-354, *Challenges and Efforts to Secure Control Systems*, March 2004

Gleick, Peter H., *Water and Terrorism*, Water Policy, Vol. 8 pp. 481-503, 2006. http://www.pacinst.org/reports/water_terrorism.pdf

Gleick, Peter H., *Water Conflict Chronology*, http://worldwater.org/conflictchronology.pdf

Global Energy Cyberattacks: "Night Dragon" white paper by McAfee Foundstone Professional Services and McAfee Labs, February 10, 2011.

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, NSTIR 7628, National Institute of Standards and Technology, August 2010

Hop Hacking Hedy, atlas, cutaway and Q, Shmoocon 2011, http://www.shmoocon.org/speakers#hedy

Hydrosense: Infrastructure-Mediated Single-Point Sensing of Whole-Home Water Activity, Froelich, Jon, Eric Larson, Tim Campbell, Conor Haggerty, James Fogarty, and Shwetak N. Patel, Ubicomp 2009, Orlando, Florida.

In the Crossfire: Critical Infrastructure in the Age of Cyberwar, McAfee Report, January 28, 2010.

Kroll, Dan., "*Water distribution monitoring: opportunities and challenges for enhancing water quality and security*." Hach Homeland Security Technologies White Paper July 2010, http://www.hachhst.com/wp-content/uploads/2010/07/White-Paper_-Enhancing-Security-in-Water-Distribution-System.pdf

Making a Secure Smart Grid a Reality, David Baker, Journal of Energy Security, October, 2009

Measuring Water Security Progress, L. Vance Taylor, Catalyst Partners, LLC, AWWA Water Security Congress, September 21, 2010, National Harbor, Maryland. http://awwa.omnibooksonline.com/DSS2010/main.html

NAWMS: Nonintrusive Autonomous Water Monitoring System, Kim, Younghun, Thomas Schmid, Zainul M. Charbiwaia, Jonathan Friedman, and Mani B. Srivastava, *SenSys 2008*

Not quite ZigBee; or How to sniff a strange radio, Travis Goodspeed, Source Boston, 2010

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.

Practical ZigBee Exploitation Framework or "Wireless Hacking and the Kinetic world", Joshua Wright, Toorcon 11, Quahogcon, 2010.

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

Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats, by GreyLogic, January 21, 2010.

Roadmap to Secure Control Systems in the Water Sector, Water Sector Coordinating Council Cyber Security Working Group, March 2008

Review of policies, practices, and procedures of the City of Brockton's Water and Sewer Department, The Abrahams Group, Woodward & Curran, June, 2011.

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

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

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

Smart Grid Device Security, Mike Davis, Black Hat USA 2009

"Smart" Parking Meter Implementations, Globalism, and You, Joe Grand, Jacob Applebaum, & Chris Tarnovsky, Blackhat USA 2009,

Testing the Water: Smart Metering for Water Utilities, Oracle Utilities, January 2010

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

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

Wang, Jian-Weng and Li-Li Rong, *Cascade-based attack vulnerability on the US power grid*, Safety Science, Volume 47, Issue 10, December 2009, pp. 1332-1336

Water meter calibration, repair, and replacement program, Georgia Environmental Protection Division, August 2007.

WATTR: A method for self-powered wireless sensing of water activity in the home, Campbell, Tim, Eric Larson, Gabe Cohen, Jon Froelich, Ramses Alcaide, & Shwetak N. Patel, *UbiComp, 2010*.

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]

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]

Yes it is Too WiFi, and No It's Not Inherently Secure, Rob Havelt, Black Hat Europe 2009.