Protecting Critical Infrastructure Against the Next Stuxnet

Doug Nibbelink

Davenport University

CAPS 795

Dr. Lonnie Decker

March 20, 2013

Abstract

The Stuxnet worm served as a global wake-up call that a highly sophisticated, targeted attack against critical infrastructure technology was not only plausible - it was possible. While Stuxnet specifically targeted a uranium enrichment facility in Iran (Sanger, 2012) it also impacted other organizations with similar equipment, including American oil and energy company Chevron (King, 2012). Stuxnet drew worldwide attention and increased concern about the safety and security of vital systems such as supervisory control and data acquisition (SCADA) for utility operations. One positive result of the Stuxnet worm is widespread awareness of the need for increased effort and vigilance toward protecting and defending the systems that provide reliable delivery of electricity, clean water, and wastewater treatment services. The hope of the author is that stakeholders responsible for securing and maintaining control systems will undertake significant efforts and make substantial improvements toward better security across all areas of critical infrastructure.

This research project will explore the significance of the Stuxnet worm as a call to action and focus attention on protecting, defending, detecting possibly malicious activity, and responding to security incidents as well as mitigating risks that impact critical infrastructure. Mitigation techniques will be shared for minimizing risk and preventing possible service disruption caused by attacks like Stuxnet, and similar threats in the future. The United States and other nations with modern and complex systems providing core infrastructure services must be protected, or grave consequences could affect our safety, security, and way of life.

Control system security is critical to the utility sector. Stuxnet demonstrated how vulnerable systems are to attack, with the all too real risk of disruption to electric, water, and wastewater treatment services. Given the likelihood of highly-sophisticated attacks targeting critical infrastructure as evidenced by the Stuxnet worm, new methods and best practices must be developed and implemented to ensure protection of utility infrastructure operations.

Control system security expert Ralph Langner is widely regarded as one of the primary people credited with analyzing and deciphering the Stuxnet worm source code. Mr. Langner has presented the findings of his analysis of Stuxnet around the world, including a TED talk and at the exclusive invite-only S4 Conference which is recognized as the elite event for control systems security subject matter experts. The following excerpt from the preface to Ralph Langner's 2012 book, Robust Control System Networks: How to Achieve Reliable Control After Stuxnet is an accurate and compelling statement on the significance of the Stuxnet worm:

> *"[Stuxnet] hit the Western world like the Sputnik shock. The sophistication and aggressiveness of this computer virus was at a level that few people had anticipated. Compared to office IT malware as we know it, this would be like going from 1980s-style password guessing to botnets in one step. It was, indeed, shocking. Instead of a learning curve for both the attackers and the defenders that the general development and trend of malware had been experiencing in the IT world, there was one big leap.*

> *The industrialized nations continue to face a significant threat from post-Stuxnet malware for which they are by no means prepared. Stuxnet was discovered, and where we continue to be: unprepared and vulnerable. The sober insight from this is that the concept of risk has been abused more often to argue risk away rather than being used as motivation and guidance to arrive at more reliable and secure systems."* (Langner, 2012).

Table of Contents

Introduction

The Stuxnet worm began what may one day be called the age of security enlightenment within the control system space. Reliance on technologies that well into the 21st century still contain vulnerabilities similar to those found in software predating the graphical user interface (GUI) and the Internet is a disconcerting and unfortunate reality. Suffice it to say that there is no shortage of work to be done by those tasked with protecting and securing supervisory control and data acquisition (SCADA) systems. This paper will cover the Stuxnet worm as well as methods for preventing a similar attack against utility systems. While Stuxnet has received a significant amount of media attention, the application of the lessons learned and expanding upon defense in depth principles of information security is an area lacking in comprehensive coverage. As Dale Peterson president of ICS security consulting firm Digital Bond, the company behind the annual S4 conference, said in an article for SC Magazine titled Waking the Sleeping Giant in November of 2012: *“These systems are expensive and insecure by design.”* (Peterson, 2012).

This paper is intended to contribute to the community in helping to close the loop specifically focusing on electric, water, and wastewater treatment services. Producing and delivering electricity, clean water, and the removal and treatment of wastewater are foundations of everyday life. Without these core services, society cannot function as it does today.

Background

Stuxnet is the first known example of a nation-state creating and using malicious software in a targeted attack against an enemy. In the case of Stuxnet, the bull’s-eye was the Iranian nuclear enrichment facility in Natanz. It is estimated that the Stuxnet worm caused damage to more than 1,000 of the 9,000 centrifuges at the Natanz site used for refining uranium (Warrick, 2011). Political leaders in Iran have stated the plant in Natanz is solely for creating fuel for nuclear power production, but the international community fears Iran intends to refine uranium for use in building nuclear weapons. The possibility of Iran possessing nuclear weapons concerns many countries including the United States, and a sophisticated electronic attack was created to slow down Iran's nuclear advancement. Stuxnet forever changed the digital world by demonstrating the use of a computer worm as a weapon by one nation against another.

The use of computer code as a means of attack by a government has been discussed for years but until information about Stuxnet began to circulate in 2010, the concept of a cyber weapon was primarily hypothetical. Analysis by control system expert Ralph Langner and staff at Symantec Corporation revealed Stuxnet to be among the most sophisticated computer attacks in recorded history. Stuxnet was able to compromise a computer using any one of four zero-day vulnerabilities in the Windows operating system as an entry point. Once it had gained access, Stuxnet then exploited a flaw in Siemens process control software to manipulate the operation of centrifuges (Cherry & Langner, 2010). Stuxnet was also so specific with regard to its target that it would activate only when it identified specific centrifuges running at a very high speed and in a certain arrangement. Furthermore

Stuxnet effectively hid the manipulation of centrifuge operation from the control system staff at the plant (Falliere, Murchu, & Chien, 2011). Clearly Stuxnet truly raised the bar in the complexity of a targeted cyber weapon.

In addition to being the current pinnacle of complex specialized attack code, Stuxnet is also unique in that it was created by the US government as reported by the New York Times on June 1, 2012 (Sanger, 2012). Some sources indicate the Israeli government may also have been involved (Broad, Markoff, & Sanger, 2011). By some estimates Stuxnet would have taken a team of experts several years to complete which makes it vastly different than much of the rather simplistic code written by criminals and/or black hat hackers for the purpose of quick financial gain or command and control botnets such as those used by spammers. Retired General Michael Hayden, the former Director of both the NSA and the CIA in an interview on the CBS television program 60 Minutes said that the surprise with Stuxnet was not that it could be done, but that a first world government would make the decision to use cyber for such an attack (Messick, 2012).

In order to understand the significance of Stuxnet, a comparison to the first use of the atomic bomb in Japan near the end of World War II is appropriate. Like the atomic bomb, Stuxnet was a demonstration of power and technical capability. While Stuxnet did not cause any deaths, it did destroy important and costly critical infrastructure equipment. It is difficult to predict the future ramifications of Stuxnet, especially in light of the fact that allegedly the source code for Stuxnet can be found on the Internet. General Hayden described the difference between a nuclear weapon and a cyber weapon as follows: “When you use a physical weapon [such as a bomb], it destroys itself” (Messick, 2012). While it is believed that Stuxnet was never intended to be discovered let alone the source code made available online, the issue with anything taking place in the digital world is that it is possible (even likely) that activity can be analyzed and once acquired - compiled code can be reverse engineered. As information about Stuxnet began to spread through media channels, The New York Times article on Stuxnet quotes a source who stated that President Obama at one point asked his national security advisors, “Should we shut this thing down?” (Sanger, 2012). Putting anything back into Pandora’s Box is as difficult as removing all digital traces of information from the Internet.

Stuxnet and Control System Security

Beyond military, political, and technological significance the Stuxnet worm was a historic moment in the realm of industrial and utility control system security. Subject matter experts such as Dale Peterson have argued that the control systems space has been sorely neglected while business information security continues to evolve and mature. A recent blog post for Mr. Peterson's consulting company Digital Bond sums up his chillingly accurate assessment of the current state of affairs:

> "*Stuxnet demonstrated to the world that an Internet connection to the target is not required to launch a devastating cyber attack. A target that is probably better defended against attacks from the Internet than most installations in US critical infrastructure got hit anyway, and it wasn’t magic. Critical infrastructure SCADA and DCS need to be robust and secure, full stop*." (Peterson, 2013).

Traditional air gaps used to protect control systems by separation have been disappearing as business needs for real time data and inter-connected networks become the norm. While connectivity has brought better access to information needed by stakeholders and decision-makers, the security of critical infrastructure has not been addressed as well as more mature defense in depth best practices already in use by companies for protecting business systems and data assets.

Critical Infrastructure Security and President Policy Directive 21

Knowing the risks to critical infrastructure both before and since Stuxnet, the US government created Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience. PPD-21 "advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure" (DHS, 2013). PPD-21 is a directive to increase awareness, focus attention, and improve the security of systems used in the utility sector as well as fifteen other areas identified as key to the safety and security of the United States. Regarding the utility industry (both public and private), PPD-21 includes the Energy Sector, the Water Sector, the Dams Sector as well as the Nuclear and Chemical Sectors. The Dams Sector is related to the Energy Sector as many dams are used to create electricity. The Nuclear Sector includes the nuclear power industry. And the Chemical Sector is related to the Energy and Water sectors because of the many chemicals required for both the Energy and Water Sectors to function. While PPD-21 is a positive step toward increased visibility for the future security of critical infrastructure, it cannot possibly solve the myriad risks, threats, and security vulnerabilities present in many of the key systems taken for granted by the majority of people in the United States and other countries around the globe.

Existing Methodologies and Guidance for Securing ICS

NERC CIP 002-009

Businesses across all economic sectors have benefited from best practice guides to defense in depth and compliance regulations that act as a road map on the long, arduous journey toward a strong and mature security posture. Rather than attempting to create a secure utility infrastructure in a haphazard piecemeal fashion, the utility sector can take advantage of best practice guidelines from NIST or DHS as well as compliance regulations such as NERC CIP 002-009 which spell out methods and controls for protecting utility systems and production processes.

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) regulations were created as a response to rolling blackouts that struck the Midwest in 2003 and caused widespread power outages to customers as far east as New York. The blackouts occurred in August which is traditionally a high power usage time of the year with summer heat creating large loads from the use of air conditioning. It is estimated that over 50 million people were affected by the power outages (NERC, 2003). The sudden awareness that the US electric grid was not resilient to the point that an incident – whether accidental or intentional – could cause major outages in other areas raised a red flag for utilities and related governing organizations. NERC created a body of regulatory requirements in an effort to improve the reliability and sustainability of the electric grid. Version 1 of NERC CIP was adopted by the Federal Energy Regulatory Commission (FERC) in 2005. NERC CIP contains specific requirements for control system security practices, policies and procedures. The portions of NERC CIP regulations related to ICS security are numbered 002 through 009. NERC CIP 002-009 regulations are summarized on the NERC website as follows:

> *"NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System (BES).*
>
> *These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.*
>
> *Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets."* (NERC, 2013).

National Institute of Standards Special Publication 800-82

In addition to NERC CIP 002-009, utility organizations that are not required to comply with the FERC and NERC requirements can look to NIST and DHS for guidance regarding security techniques for protecting industrial control systems (ICS). The National Institute of Standards (NIST) Special Publication (SP) 800-82 is a helpful document for utility stakeholders. Published in June 2011 and subtitled Guide to Industrial Control Systems (ICS) Security, the NIST document executive summary describes the contents in a nutshell:

> *"This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors. ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.) SCADA systems are generally used to control dispersed assets using centralized data acquisition and supervisory control. DCS are generally used to control production systems within a local area such as a factory using supervisory and regulatory control. PLCs are*

> *generally used for discrete control for specific applications and generally provide regulatory control. These control systems are vital to the operation of the U.S. critical infrastructures that are often highly interconnected and mutually dependent systems. It is important to note that approximately 90 percent of the nation's critical infrastructures are privately owned and operated. Federal agencies also operate many of the ICS mentioned above; other examples include air traffic control and materials handling (e.g., Postal Service mail handling.) This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks."* (NIST, 2011).

DHS Resources for Securing ICS

The United States Department of Homeland Security also offers a number of documents aimed at helping stakeholders and asset owners secure their control systems. One such document is Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies. Published in October 2009, this document provides thorough guidance on ways ICS can be protected. The following excerpt from the Executive Summary indicates the contents of the publication:

> *"Industrial control systems are an integral part of critical infrastructure, helping facilitate operations in vital sectors such as electricity, oil and gas, water, transportation, and chemical. A growing issue with cybersecurity and its impact on industrial control systems have highlighted some fundamental risks to critical infrastructures. To address cybersecurity issues for industrial control systems, a clear understanding of the security challenges and specific defensive countermeasures is required. A holistic approach, one that uses specific countermeasures to create an aggregated security posture, can help defend against cybersecurity threats and vulnerabilities that affect an industrial control system. This approach, often referred to as "defense-in-depth," can be applied to industrial control systems and can provide for a flexible and usable framework for improving cybersecurity defenses."* (DHS, 2009).

No Panacea for Utility Security

While the NERC, NIST and DHS guidance for improving the security posture of critical infrastructure are extremely helpful in applying business InfoSec defense-in-depth to ICS, the need for specific techniques for utility infrastructure remains. Small and medium utility organizations have the same needs for security as large corporate entities. The publicly owned state and local government-run utilities provide a large portion of electric, water and wastewater services. According to the

American Public Power Association (APPA) more than 2,000 publicly owned electric utilities provide power to more than 47 million Americans (APPA, 2013). According to the Department of Homeland Security, over 80% of the US receives clean water from publicly owned water utilities and more than 75% of wastewater treatment services are provided by municipal utility organizations (DHS, 2013). While statistics about the size (by number of employees) of the many public utilities are not readily available, the author has talked to people at both APPA and American Water Works Association (AWWA) conferences and events and the small/medium size organizations are a significant source of utility services across the United States. The author's employer currently employs approximately 176 people. With statistics such as these in mind, it is evident that clear guidance for the time, expertise, and money-constrained utilities that have the challenging task of providing affordable, reliable utility services and securing critical infrastructure from both internal and external threats including future attacks similar to the Stuxnet worm.

Preventing a Stuxnet-like Attack

Stuxnet is a prime example of an advanced cyber threat to critical infrastructure systems including utility organizations. With Stuxnet's discovery and the subsequent research into how the worm entered the Natanz control system network, and the likelihood of similar attacks occurring in the future; stakeholders and system owners must take action to protect key cyber assets from disruption and harm from the action of those who intend to gain unauthorized access or to shut down core services such as the production and delivery of electricity and clean water. With the risks to utility services and the possibility of a cyber incident seemingly lurking both inside and outside the networks of utility plants across the nation, what unique methods are available for securing specific utility infrastructures? As in other areas of information security, thoroughly written and firmly enforced policies and procedures play a foundational role. Proper governance including policies and procedures are extremely important, but without the wise application of mitigating preventative and detective technical controls; mission-critical systems will remain insecure. How can a mid-size utility organization secure critical control systems with limited budget, time and staff expertise? All hope is not lost. While some of the methods below are not new ideas or unique to the utility control system environment, variation of existing methods is required to mitigate the possibility of a Stuxnet-like attack.

The methods for improving utility security to be covered are as follows:

- Restrict the use of USB media & other portable storage devices and enforce encryption of sensitive data
- Air gap control system networks where possible and restrict connection points to other networks using specialized firewalls and/or one-way data transmission devices
- Utilize a rigid and methodical procedure for moving code to and from production networks and control systems
- Make use of a dedicated source code management system for control system/PLC code allowing for version control and rollback to a known good version when

unexpected/undesirable behavior occurs after a modification is made

Even with the methodical application of defense in depth techniques and the thorough implementation of information security best practices, protecting systems from an advanced targeted threat such as the Stuxnet worm is a challenge for even the most skilled information security practitioners. Protecting critical infrastructure against a persistent and highly skilled adversary is extremely difficult at best and perhaps (arguably) impossible given enough time, expertise, and knowledge of the target environment.

Portable Storage Media - Risks and Mitigation Techniques

While restricting the use of USB storage devices prevents one entry vector for a threat such as Stuxnet, for isolated networks such as the air gapped control systems used in nuclear power generation facilities the use of portable storage media is one of the only ways to move data between physically separate networks. Routine IT operations such as installing software upgrades or patches, operating system updates, and data backups take place on a regular basis. Even for systems not connected physically via wired or wireless to any other network or the Internet, frequent backups are paramount for disaster recovery and business continuity functions. These activities become significantly more tedious and time consuming when the only data transfer method is the old fashioned sneaker net. The type of storage device(s) used as well as the procedures necessary to ensure that none of the portable storage media contain malicious software also poses a significant challenge. Considering Stuxnet was believed to have exploited a previously unknown or zero-day vulnerability, it is a significant challenge to come up with a vetting process or method for mitigating the risks posed by use of portable storage media. One possible method for risk reduction for portable storage media is to use WORM (write-once read many) storage for backups. For example the use of DVD discs would be one method of accomplishing relatively safe backup storage from the control system network. Data stored on key assets could be burned to DVDs from one or more of the computers on the control system network and then the backup DVDs could then be taken off-site for storage.

Another possible procedure for minimizing the risks introduced by the use of USB storage media would be to perform a low level format of all USB devices on a stand-alone computer running a boot-able operating system such as Knoppix Linux. A PC or laptop running a version of Knoppix (or another boot-able Linux distribution) is a technique used by a number of organizations for sensitive financial transactions and also by information security professionals to avoid the possibility of using a malware infected computer/operating system for performing certain computing activities in a secure manner. Once a USB or CD/DVD disc is created from an ISO image downloaded from a trusted/known good source repository the ISO can be validated using an MD5 or SHA-1 checksum to ensure the operating system image has not been tampered with. Then when a system is booted from the disc or USB drive that was also formatted fresh before making it bootable, the system can be trusted for use in formatting portable USB memory devices such as a hard drive and/or a flash memory stick/thumb drive. After formatting is complete the device(s) can be used on control system computers knowing that extensive precautions have been taken to minimize risks introduced by portable storage media.

Because Stuxnet was believed to have been introduced using USB media most likely by one or more of the contractors/integrators working on the configuration of the nuclear enrichment facility in Iran in the city of Natanz, the above precautions and procedures would be necessary for aiding in the prevention/risk mitigation of protecting key assets/systems from a threat similar to Stuxnet.

The fact that Stuxnet is reported to have been able to take advantage of not one but four zero-day vulnerabilities in the Windows operating system even a completely up to date/patched Windows system would have been easily exploited by the Stuxnet worm. This fact is a frightening one in that Windows Updates and current anti-virus software with the latest signatures would not have stopped Stuxnet from being able to take action against a compromised system connected to a control system network.

Policies and Procedures

The Importance of Human Behavior for ICS Security

As in other information security practice, policy and procedures that are communicated and enforced effectively are one of the most significant methods necessary for protecting utility control systems. With the growth in awareness of the dangers of social engineering and related human-targeted attacks, it is important to remember that the human factors related to protecting critical infrastructure systems cannot be neglected. All of the mitigating controls and state of the art defense-in-depth gear in the marketplace today will not prevent a serious incident from occurring if we as utility employees and stakeholders do not take the appropriate level of caution and due diligence in our day to day work that directly impacts ICS and SCADA systems, devices and related/connected equipment. While beyond the scope of this paper, employee security awareness training and the precise, methodical, repeatable implementation and enforced adherence to security-minded human behavior cannot be underestimated. As such the methods for moving data such as PLC code from a business network to a control system network will be different for each utility operational environment and are realistically outside the scope of this paper. However the usage of SCMS described in later sections and the cautious usage of portable storage media backed by procedures tailored for specific network and plant environments will address secure and trustworthy treatment of data in motion.

Air Gaps and Modern Network Infrastructure

The use of air gaps as a means of protecting systems and devices by separation from other systems and/or networks has been used for decades as a security precaution. The rapid growth of LAN (local area network) technology years ago and the breakneck pace of the growth of Internet from its infancy as a DARPA experimental test bed did not mean that every system ought to be inter-connected. Air gaps by definition are just what the name implies – separation from other networks and the risks and threats introduced by network connectivity. Network-borne and/or Internet-based threats can cause compromise of mission-critical software and/or hardware necessary for the uninterrupted delivery of utility services including electricity and clean water to homes and businesses as well as the transfer of waste water to treatment/processing facilities. Methods used to spread malicious software to victim systems include the use of compromised websites, email via file attachments or website links, or from one infected computer to another via wired or wireless networks including the Internet. Such methods have been utilized for nearly as long as systems have been inter-connected. From early computer systems that used terminals connected to a central mainframe or mini-frame to the invention of Ethernet technology in the early 1970s the communication of computer systems and other devices has been exploited throughout history. Before computing as we now know it was in use both curious and malicious technically-minded people have been discovering vulnerabilities and taking advantage of them. Two examples of precedent-setting hacking activities are so-called phone 'phreakers' who manipulated telecommunication systems as far back as 1971, and the Morris worm in 1988 which spread rapidly to an estimated 6,000 systems via the ARPANet network after being released by Robert T. Morris who was at the time a Cornell University graduate student (CERT, 1997).

It is clear from historic events from the Morris worm to the current trend of at least one or more significant breach incident hitting the news every week that connectivity exposes a system or network to serious threats. With the risks inherent in connecting a production control system network to internal business network(s) that may be connected to the Internet, is an air gap the only solution? Thankfully not, as utility stakeholders and executives frequently demand access to real time data in order to monitor utility functions and make decisions such as whether to generate electricity or purchase it from another facility from the open market. Fortunately it is possible to secure control systems in situations when business requirements force connectivity to key business systems and often indirectly to the Internet.

Securing Networked Control Systems

One solution for allowing network communication while minimizing risk is the use of unidirectional security gateways. These devices behave like a one-way firewall, allowing data to flow from allowed sending devices on one network to one or more receiving devices on another network. An example use case for a unidirectional security gateway would be to allow data backups to be copied from the control system server(s) to a storage system such as a NAS/SAN on the business network. A second example would be allowing control system computers to retrieve Windows operating system patches from a Microsoft WSUS server on the business network once appropriate testing and validation has been performed to ensure the updates do not impact SCADA applications. A third example would be an Intranet web server pulling data about up to the minute electric load and generation, transmission and distribution system status. Several manufacturers offer products for one-way data transmission, and as demand for this particular niche product increases and costs decline the author's employer and other small/medium utilities can take advantage of technology that is beyond what traditional firewalls can offer as far as peace of mind.

While an air gapped network is certainly preferred simply for the benefit of a physical separation from other Internet-connected systems and networks, the difficulty of having visibility into operations and performing routine system maintenance functions as mentioned previously becomes challenging. The importance of the security of critical infrastructure technology such as SCADA control systems cannot be underestimated. At the same time (as is the norm with regard to information security decisions), risk must be analyzed and compared with the business case for connectivity to enable data sharing as well as patch management and backups.

The Real World – Two Examples Requiring Secure Solutions

Example 1: Contractor/Consultant Access

Securing network connectivity points and protecting control systems/networks through implementation of strictly configured firewalls and unidirectional security gateways are both useful methods for strengthening ICS security. However there are a number of scenarios whereby the need for moving data from a system not attached to a control system to the production ICS network. A frequently occurring example of this would be a consultant performing system improvements, upgrades and/or integration tasks on production control systems. Today's utility production environment is significantly complex and especially for the small/medium utility space, frequently requires outside expertise for assistance in upgrades, configuration changes and modifications to existing system configurations. While utilities are careful with the selection of trusted vendors and contractors who have vast amounts of experience as well as an understanding of the security risks and threats, as Stuxnet demonstrated the possibility of malicious software entering a control system network via trusted partners is not hypothetical. Mitigating controls and strict policies/procedures must be in place to protect critical infrastructure systems. Two protection technologies uniquely suited for protecting utility control systems are unidirectional security solutions and specialized networking gear, example commercial solutions of each will be covered in depth.

Solution 1: Unidirectional Security Solutions

As described previously, technology providing security and peace of mind beyond what traditional firewall and router technologies such as Access Control Lists (ACLs) and IDS/IPS solutions can provide are necessary. Protecting utility and industrial control systems (ICS) as well as SCADA created a niche for companies to develop products for implicitly one-way networks. One such company is Waterfall Security Solutions. Waterfall offers an extensive and broad base of solutions all utilizing their proprietary one-way diode technology to secure sensitive systems for implementations where air gaps are not possible and/or feasibly practical. The Waterfall website contains a helpful visualization of how their solution can be installed and configured to protect control system networks:

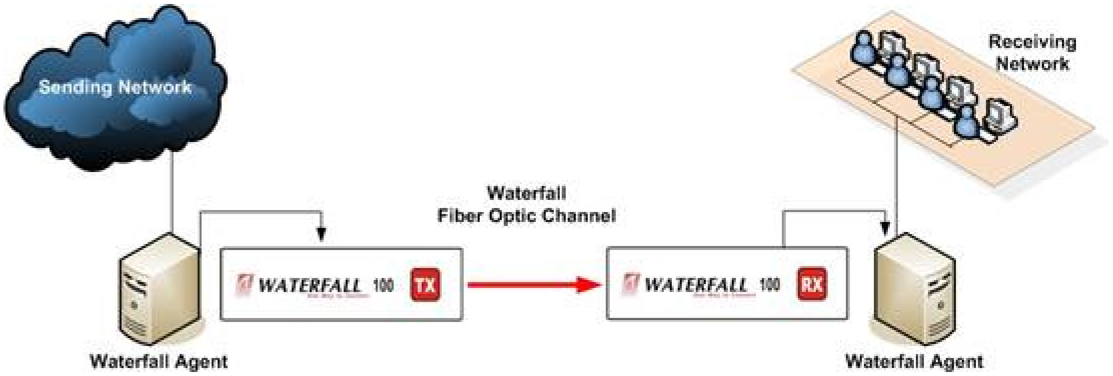

Diagram courtesy of Waterfall (Waterfall, 2013).

As shown above the Waterfall software and hardware operate a specialized fiber optic network that strictly controls the transmission and receiving of datagrams/packets. Using this approach, security concerns with regard to the protocol implementation and design of Ethernet and TCP/IP are avoided. Use of one-way diode and/or patented fiber-optic communication technology, Waterfall gear handles the low level network flow control, and the Waterfall Agent software takes care of everything happening on the wire; including but not limited to the OSI layers as well as offering completely customizable configuration of the application stack (Waterfall, 2013). Waterfall's solutions are impressively thorough, the description below describes the extent of the security controls:

> *"The unique Waterfall architecture and its attributes provide two basic benefits for all Waterfall One-Way installations and deployments:*
>
> - ***Complete protection against external cyber attacks*** *– hacking sessions are an interactive process in which a hacker initiates a working session with his target node, elicits a response, and accordingly makes his next move. When trying to hack across a Waterfall One-Way, the hacker will be unable to initiate a successful session.*
> - ***No data backflow*** *– The hardware based appliance core of the Waterfall One-Way enforces unidirectional data flow at the physical layer (Layer 1 of the OSI model), which in turn ensures unidirectional communication will be totally preserved at all higher layers of the protocol stack, regardless of the communication protocol chosen and the applications being used. Thus, regardless of networks and applications used, there will be no data backflow across a Waterfall One-Way.*

- ***Non Routable Protocols*** *– Waterfall One-Way is a Non-routable communication system, as referred to in the relevant NERC-CIP definitions. This means that the communication path cannot be exploited to route messages or information to undesired or unplanned destinations.*
- ***Integral Application White listing*** *– Waterfall One-Way, using the unique "Waterfall connectors framework", enables only allowed application's data and protocols to pass via the unidirectional gateway. Any other protocol, not set up at the gateway, is not supported and shall not pass."* (Waterfall, 2013).

Waterfall is not the only provider of security solutions specifically tailored to the utility control systems space. RAD is a company specializing in network gear for critical infrastructure and other sectors which require highly secure implementations. RAD describes their solution as follows:

> *"**Your Needs**: Secure SCADA installations throughout the power grid to protect from cyber security threats.*
>
> ***Our Solution**: Use secure Ethernet switches with built-in firewall/VPN to reliably connect and safeguard SCADA equipment from "insider" attacks. Ruggedized Ethernet switches use highly secure firewall to monitor application*

> *traffic and stop unauthorized and potentially damaging activity.*
>
> ***Benefits***
>
> - *Protection of Ethernet-based and serial SCADA devices*
> - *Ruggedized switch ensures operation in harsh environments, standard compliant with IEC 61850-3, IEEE 1613 EMI*
> - *Integrated firewall on each port provides a network-based distributed security solution equivalent to the use of personal firewalls on each system in the network, with service-aware inspection of traffic in every end-point and role-based validation of SCADA flows*
> - *Full security functions in a single switch: Service validation, remote access, inter-site VPN and access control*
> - *Built-in QoS to support mission critical services " (RAD, 2013).*

Clearly RAD's solutions offer a variation on, and a novel application of traditional technology implementations. After initial research for this paper, it is the author's opinion that RAD does not appear to provide the same level of security certainty as the products offered by Waterfall Security Solutions.

Example 2: Field and Remote Work - Data Storage

A second example of data transfer with significant security ramifications would be backing up PLC configuration and ladder-logic programming code from an employee's company-issued laptop to a USB thumb drive. Frequently industrial controls technicians and engineers are working at locations that may or may not have wired or wireless LAN access and/or Internet access. There is also the issue of determining the appropriate level of trust for different network connection points. Simply because an Ethernet port or a Wi-Fi connection is available does not necessarily mean it ought to be used to copy files of a sensitive nature such as the last known good configuration from production control system devices. With the dual concerns of access to a trustworthy network as well as the possibility of a remote site that does not have cellular coverage let alone computer network connectivity, the use of a laptop hard drive and USB storage are frequently used to configure ICS devices and make backups when working on-site. Fundamental security constraints including operating system configuration, the application of OS patches, and running up to date anti-virus software do have an impact in the given scenario as well as strong passwords for administrator/root level access to systems and devices but are beyond the scope of this paper.

Solution 2: Securing Data Storage – Encryption to the Rescue

Assuming that the internal hard drive in a laptop and/or USB storage devices are acceptable ways for staff and properly vetted consultants or contractors to do their work, how can data be secured? Thankfully this is a question that can be answered with one word: encryption. The use of encryption for storage media is an inexpensive method for securing data. Three readily available methods include a commercially available USB flash drive product such as IronKey which features AES 256-bit hardware encryption (Imation, 2013). Microsoft provides full-disk encryption known as BitLocker for Windows 7 and Windows 8. BitLocker provides either 128-bit or 256-bit AES encryption, and on systems with a supported TPM chip further security measures are available for key storage (Microsoft, 2012). A third option is to use properly vetted free and open-source encryption software such as TrueCrypt, which has been approved by cryptography expert Bruce Schneier. TrueCrypt has a wide variety of choices for encryption methods including AES, Twofish, and Serpent algorithms (TrueCrypt, 2013). With the three options described and many more available it is clear that data encryption is a mature technology sector. Encryption should be used for sensitive data including the storage of code, configuration information and files needed for production utility operations that must function reliably around the clock.

ICS Source Code Control and Management Systems

Example 1: Rockwell Automation's FactoryTalk AssetCentre

Business software development environments have long benefited from the use of source code management systems (SCMS). These systems provide a centralized location and repository for programming code including live production as well as development. In addition, versioning allows for the review of all changes made to code over time as well as the quick and easy rollback to a last known good version in the case of unexpected behavior and/or errors.

The fact that some ICS solution providers have begun to offer products with SCMS functionality specifically for the control systems space is encouraging. Although the relative newness of ICS SCMS is evidence that the maturity of control systems overall is again proving to be behind when compared to the status quo of IT and security in non-utility sector environments.

Rockwell Automation is one of the very large players in the ICS space. The Rockwell Automation corporate website boasts being "the world's largest company dedicated to industrial automation." (Rockwell, 2013). Currently Rockwell Automation has over 22,000 employees. Rockwell's software product line is named FactoryTalk®, and their SCMS-product is called AssetCentre (Rockwell, 2013). AssetCentre offers a full feature set of functionality for the management of ICS code including acting as the centralized repository for secure storage and version control. The list below identifies the AssetCentre feature set:

- *"Source Control — leverages a centralized database to provide automatic version control. This allows proper file management and single master relationships.*
- *Disaster Recovery — ability to perform automated backup or backup and compare of Rockwell Automation and certain third-party assets improving MTBF and compliance to operating practices.*
- *Calibration Management — centrally schedule, manage, track and report calibration activities enabling compliance to regulatory or in-house quality procedures.*

- *Process Device Configuration — ability to centrally configure and troubleshoot smart process devices improving diagnostic capabilities, maintenance efficiency and MTBF performance.*
- *Audits — gather information centrally that is generated by user interactions with Rockwell Automation FactoryTalk-enabled applications, including FactoryTalk® AssetCentre. The audit trail consists of user, device, computer, time and action taken.*
- *Events — gather system-generated information centrally from FactoryTalk-enabled applications, including FactoryTalk AssetCentre. Typical event information may include time, source generating or messaging.*
- *Security — leverage powerful features of FactoryTalk Security to administer users and passwords on operator interfaces, historians, engineering and maintenance workstations. It even enforces security rights when machines are disconnected from the LAN.*
- *Reporting — scheduled and on-demand searches and traceability information from FactoryTalk Audit, Events or Source Control.*

- *Scheduler — runs periodic disaster recovery or reports. These are assigned to FactoryTalk AssetCentre-designated computers, or agents, and are load-balanced automatically across all agents."* (Rockwell, 2013).

Clearly Rockwell's AssetCentre is a mature product with a comprehensive feature-set on par with SCMSs that have been in use for well over a decade by large commercial software development companies.

Example 2: Trihedral's VTS Application Version Control

Not surprisingly, AssetCentre is not the only choice available for utility organizations looking to implement an ICS SCMS. Trihedral Engineering Limited is a company offering HMI software solutions. Trihedral's core product is called Virtual Tag System (VTS). VTScada is Trihedral's flagship product built on the VTS platform targeted specifically to the water and wastewater industry. VTScada offers an add-on module called VTS Application Version Control for providing SCMS functionality. Key VTS Application Version Control features listed on the Trihedral website are shown below:

See a full configuration change history of the application by all users on all servers.

- *"Review change details before deployment of local changes to all servers.*
- *Quickly trace problems back to their source.*
- *Identify incremental changes made in each version.*
- *Switch to any previous known good version.*
- *Merge versions together.*

- *Manage application changes in a multi-developer environment.*
- *View the current version running on each computers."* (Trihedral, 2013).

Trihedral's solution offers the majority of features that a utility would desire in the use of an SCMS for control systems. However the author's research indicates that VTScada Application Version Control is not as comprehensive as Rockwell Automation's solution. Yet as in other areas of security solutions for critical infrastructure, one size does not fit the needs of every utility with uniquely varied installations and configurations. The variation within real-world ICS environments is far more diverse than more traditional business IT systems and networks where it is common to have organizations of different sizes may have a very similar network topology, with primary differentiators being scale and scope.

Recommendations

Coverage has been given to identify the methods for protecting ICS systems and data - both at rest (in storage) as well as data in motion (during transfer). Use of encryption allows for the safe and secure storage of data – whether on a laptop hard drive or USB media. SCMS solutions provide secure access to control system configuration as well as backups from networked systems. In addition, products such as those offered by Waterfall Security Solutions fill a niche for increasing the security level of network-connected control systems beyond what is possible through the implementation of firewalls, routers with strict ACLs, and IDS/IPS solutions. The author is encouraged by the research performed and plans to utilize the knowledge gained during the researching and writing of this paper to apply the methods discussed directly to the utility operations and plant environments of the author's employer. The hope is for improved security overall, and a more structured approach to security beyond what has been done until now. If the end result of this paper is one utility better able to protect and defend against a Stuxnet-like attack, all of the time and effort given toward the MSIA and this thesis will pay dividends well beyond today toward securing the future and providing of reliable and affordable electricity, water and wastewater treatment to thousands of residents and businesses in a Michigan community.

Final Results and Reflections

There are a wide variety of methods and procedures for improving the security of critical infrastructure systems and specifically the small/medium utility space. The author's research has been rewarding and educational as an eye-opening view of the depth, breadth and scope of solutions available both from the commercial offerings as well as the options for implementing strategic methodologies for protecting key cyber assets from threats similar in nature to the Stuxnet worm. As stated by Michael Moll from DHS, there is “no silver bullet” or single product/process solution that can single-handedly solve every problem facing the author and others with the sizeable and intimidating task of securing, protecting and defending utility control systems and infrastructure from disruption on the cyber front. Network connectivity including direct and indirect paths to the Internet, software vulnerabilities, and challenging implementation scenarios seen in municipal utility plants both at home and abroad create a dizzying mixture of risks and threats to the consistent, reliable delivery of services that most Americans all too often take for granted - until a disruption or outage occurs. The security of utility control systems, ICS and SCADA are paramount for society to continue to function. Electricity, water and wastewater treatment are foundational to personal life and business productivity. Neglecting the security of the systems that make service delivery by utility operations possible is a dangerous and foolish proposition. Stakeholders and security practitioners in the utility space must make every effort possible despite the frequently opposing forces of time, budget and staff expertise in order to aid in the rapid maturity of utility sector security. As demonstrated by the author, the security stance and posture of the utility sector is sadly lacking. It is the hope of the author that this document will in some small way contribute to the continuous improvement of security for the author's employer as well as the utility industry as a whole. Organizations such as DHS, Idaho National Laboratory, ICS-CERT and many others are carrying the torch for improving critical infrastructure and utility security. However too many organizations are not heeding the clarion call for more concerted effort on the front lines of cyber security. Hackers and perhaps even more frightening terrorist groups as well as nation-state sponsored and trained cyber attackers are preparing for the equivalent of a war on the 5th battlefront known more commonly as the Internet. Without the dedicated and cooperative efforts of the good people desiring to see continued safe, secure and reliable utility services delivered without interruption there will continue to be serious incidents and exploitation of vulnerabilities wherever there are risks that go unmitigated, for whatever reason be it knowingly or unknowingly. If all who can contribute toward better security do all that is within our power to make improvements, the author hopes and dreams that the work taking place every day will lead to a brighter and more secure future for the utility industry overall. It is a bleak vision for the future if electric services as well as water and wastewater become unstable and unreliable due to poor security and the abuse by attackers of unprotected systems. It is very difficult to make use of the technology we as IT professionals and the general public rely on every day if there is no electricity with which to power and charge all of our devices. The author's thesis is now complete, but his journey toward vastly more secure and resilient control systems for one municipal utility organization and speaking as an evangelist to encourage others to take the same journey has only begun...

Subject Matter Expert Interview 1

Michael Moll, DHS

Brief Biography

Michael Moll is the U.S. Department of Homeland Security (DHS) Protective Security Advisor (PSA) for Region 6 which includes West Michigan. Mr. Moll has worked for DHS for 10 years, and previously was a Public Safety Director

The author spoke with Mike by phone on Tuesday, March 19. Mr. Moll made the following statements regarding the current state of cyber security in the utility and critical infrastructure sector:

> *"DHS has identified the following as our top 3 threat streams:*
>
> 1. *IEDs (underwear bomber, NY Times Square attempt)*
>   *3 plots foiled over the last several years*
> 2. *active shooter (New Town & Aurora tragedies)*
> 3. *cyber security"*

> *"As we discussed earlier, for us the biggest/most disconcerting area is cyber security as it is growing rapidly as an area of concern. SCADA and Process Control Systems (PCS) that are directly/indirectly connected to the Internet are open to any variety of people who desire to gain unauthorized access and/or cause disruption. One example demonstrating the significance of the cyber*

*security risks to utilities would be the Aurora Vulnerability generator demonstration a few years ago. The generator that was accessed by government employees acting as a hacker/terrorist group would were able to not only gain access to the generator control system; they were able to manipulate the controls to alternate the current in such a way that the generator was destroyed. Imagine if this generator was in use in the dam sector - the exact same successful attack could cause massive flooding in the US." *Also, the scientists involved in this project were spooked not at what they did, but how quickly and easily they were able to do it..."*

"The utility sector provides core services we all rely on every day - whether power, water or wastewater treatment. Customers expect reliability, and as such security really is a way of continuing to ensure reliability."

"The Stuxnet and Aurora generator [security demonstration whereby generator destruction occurred after remote breach of control systems to attain unauthorized access and full control of SCADA HMI software] events demonstrated how an incident of a larger scope or scale could cause major disruption, up to

> *and including the requirement for a large scale evacuation to take place. Look at MISO (Midwest Independent System Operator), the group tasked with overseeing much of the electric grid in West Michigan, and the entire Midwest. If someone gained access to the MISO systems, they could cut power to a lot of people and businesses. The cyber security threat is very real, nation-state actors/hackers could make something happen on the scale of some of the severe weather that occurs in other parts of the country. Or look at the area of satellite communications - can we prevent things from happening like an enemy nation taking control of our drones? These examples of what could realistically happen are very disconcerting."*

> *"I feel a lot of the information about the all too real threats along the lines of Stuxnet are falling on deaf ears when it comes to the utility space. Most organizations give in to the desire for connectivity over the goal of securing mission critical systems. It is a scary thing that many SCADA and Production Control Systems (PCS) are directly or indirectly connected to the Internet. Unfortunately we don't have any silver bullets for this, and to make matters worse we have a lot of enemies*

> *around the world that are taking action. State-sponsored groups of highly trained people are targeting critical infrastructure as an attack target. Look at China - they have tens of thousands of people working for the Chinese government that are taking IP (intellectual property) from the US and others every day, and it is also highly likely that China and other countries are already looking for ways to disrupt the 18 critical infrastructure sectors in the United States as defined in PPD-21."*

Subject Matter Expert Interview 2

Dr. Wesley McGrew, Mississippi State University

Brief Biography:

Dr. Wesley McGrew is an instructor at Mississippi State University's Center for Computer Security Research (CCSR). He has been performing vulnerability analysis on control system software for approximately 4 years. His primary focus is finding vulns in SCADA HMI (human/machine interface) software. He has presented at a wide variety of InfoSec conferences including BlackHat, DefCon, SANS Scada Summit and BSides Jackson as well as a number of academic conferences including CISSE and SSTC. In addition, Dr. McGrew has reported numerous vulnerabilities that he discovered to the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT). [Author's note: ICS-CERT is the organization tasked with publishing vulnerabilities in readily available and widely used ICS and SCADA software and systems and working with vendors to share information and work toward mitigation of identified vulnerabilities through patching and/or mitigating controls.]

The author spoke with Wesley by phone on Monday, March 18. Below are quotes from Dr. McGrew regarding the current state of software (in)security in the utility and ICS sector:

> *"[In the ICS space] there is a lot of legacy code. The security features in much of the HMI software that I have analyzed contains security features that might meet a checkbox requirement - but they are frequently not*

properly implemented, with known best-practices such as salting and hashing, and definitely not tested adequately for proper implementation. In addition I have found that it is possible to turn off auditing of HMI activity so that what I or an actual attacker is doing can be hidden from log files in the possibility of an investigation after an incident or breach has occurred."

"While low level network protection technologies such as Waterfall and others are interesting and solve some problems with ICS security, the application layer is where the vulnerabilities that I have found exist. All of the data layer protection and defense-in-depth methods will not help protect a system if I can escalate privileges and gain control of the HMI. If I start with gaining unauthorized access to a read-only screen I have found it is often possible to jump outside of the HMI in order to gain full control administrator level access at which point I can turn off pumps or manipulate the connected equipment to cause disruption."

References

American Public Power Association (APPA). (2013). About APPA .

Retrieved from:

https://www.publicpower.org/aboutappa/index.cfm?ItemNumber=28371&navItemNumber=29004

Broad, Markoff, Sanger. (2011, January 15). Israeli Test on Worm Called Crucial in Iran Nuclear Delay. *New York Times*.

Retrieved from:

http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html

Computer Emergency Response Team (CERT). (1997). Security of the Internet.

Retrieved from:

http://www.cert.org/encyc_article/tocencyc.html

Cherry, Stephen. (2010, October 13). *How* Stuxnet Is Rewriting the Cyberterrorism Playbook (Interview with Ralph Langner). *IEEE Podcast*.

Retrieved from:

http://spectrum.ieee.org/podcast/telecom/security/how-stuxnet-is-rewriting-the-cyberterrorism-playbook

Department of Homeland Security (DHS). (2013). Water Sector: Critical Infrastructure Sector Overview.

Retrieved from:

http://www.dhs.gov/water-sector

Department of Homeland Security (DHS) Control Systems Security Program (CSSP) National Cyber Security Division (NCSD).(2009, October). Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies.

Retrieved from:

http://ics-cert.us-cert.gov/practices/documents/Defense_in_Depth_Oct09.pdf

Falliere, Murchu, Chien. (2011). W32.Stuxnet Dossier. *Symantec*.

Retrieved from:

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Hilt, David W. (2006). August 14, 2003, Northeast Blackout Impacts and Actions and the Energy Policy Act of 2005. *North American Electric Reliability Council*.

Retrieved from:

http://www.nerc.com/docs/docs/blackout/ISPE%20Annual%20Conf%20-%20August%2014%20Blackout%20EPA%20of%202005.pdf

Jager, Chris. (2013, March 18). NERC CIP Version 5 Background

Retrieved from:

http://www.digitalbond.com/blog/2013/03/18/nerc-cip-version-5-background/

Imation (2013). IronKey™ Enterprise S250 and D250 Flash Drives, Serious Drives for Safeguarding Serious Data with Management Service Option. Imation.

Retrieved from:

http://www.ironkey.com/en-US/secure-portable-storage/250-enterprise.html

King, Rachel (2012). Virus Aimed at Iran Infected Chevron Network. *Wall Street Journal*

Retrieved from:

http://online.wsj.com/article/SB10001424127887324894104578107223667421796.html

Kroft, Messick. (2012, July 1,). Stuxnet: Computer worm opens new era of warfare. *60 Minutes*.

Retrieved from:

http://www.cbsnews.com/video/watch/?id=7413520n

Langner, Ralph. (2012). *Robust Control System Networks: How to Achieve Reliable Control After Stuxnet*. Momentum Press. New York, NY.

Little, Chris and Sooley, Blair. (2012 September). Moving Your SCADA System Forward with Confidence: Integrated version control for water and wastewater control systems. *Modern Pumping Today Magazine*. Highlands Publications. Birmingham, AL.

Microsoft. (2012, March 22). Windows BitLocker Drive Encryption Frequently Asked Questions. *Microsoft*.

Retrieved from:

http://technet.microsoft.com/en-us/library/cc766200%28v=ws.10%29.aspx

National Institute of Standards and Technology (NIST) Computer Security Division. (2011, June). Guide to Industrial Control Systems (ICS) Security.

Retrieved from:

http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

North American Electric Reliability Corporation (NERC). (2013). NERC Standards: Reliability Standards.

Retrieved from:

http://www.nerc.com/page.php?cid=2|20

Rockwell Automation. (2013). Asset Management - FactoryTalk AssetCentre.

Retrieved from:

http://www.rockwellautomation.com/rockwellsoftware/assetmgmt/assetcentre/overview.page

Peterson, D. (2013, March 8). DHS OIG Review of ICS-CERT & DHS. *Digital Bond*.

Retrieved from:

http://www.digitalbond.com/blog/2013/03/08/dhs-oig-review-of-ics-cert-dhs/

Radcliff, Deb. (2012, November). Waking the Sleeping Giant. *SC Magazine*. Haymarket Media Inc. New York, NY.

Sanger, David E. (2012, June 1). Obama Order Sped Up Wave of Cyberattacks Against Iran. *New York Times*.

Retrieved from:

http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all

Trihedral. (2013). VTS Application Version Control

Retrieved from:

http://www.trihedral.com/products/vts-version-control/

TrueCrypt. (2013). Encryption Algorithms. *TrueCrypt*.

Retrieved from:

http://www.truecrypt.org/docs/

Warrick, Joby. (2011, February 16). Iran's Natanz nuclear facility recovered quickly from Stuxnet cyberattack. *Washington Post*.

Retrieved from:

http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021506501.html