IMPACT OF THE STUXNET VIRUS ON INDUSTRIAL CONTROL SYSTEMS

Marcia M. Combs
PhD Technology Management Graduate Student

Indiana State University
Terre Haute, Indiana, USA

Abstract

The purpose of this literature review is to analyze the Industrial Control System Stuxnet virus and present the impact of the virus to the ICS community. The paper outlines Stuxnet's five major impacts: 1) the Stuxnet virus exploited security vulnerabilities in ICS system vendors and suppliers software programming; 2) Stuxnet's circumvented traditional security measures, therefore, security management systems could not stop the virus infection; 3) Stuxnet's highlighted of the lack of responsibility between ICS software vendors and operating system manufactures; 4) Stuxnet demonstrated all data networks are vulnerable to attacks despite the security measures deployed, and finally, 5) the real impact of Stuxnet is it accomplished what many thought impossible or unrealistic, therefore, new security measures and instruments are required to protect ICS networks against future cyber attacks.

Keywords: Stuxnet, Industrial Networks, Cyber warfare, Intellectual Property theft.

I. INTRODUCTION

Stuxnet was the first worm that publicly targeted industrial network and control systems (Piggin, 2010). It was a complicated Internet worm that used the combination of four zero-day exploits, command & control abilities, multiple propagation methods, two stolen VeriSign driver certificates, plus a root kit to infect Industrial Control System (ICS) hosts exclusively running Windows CC/Step 7. Its single purpose was to alternate the frequency of two particular models of frequency converter motors.

It executed programming code to perform precise physical actions that caused real-world physical damage (Waterman, 2010). Throughout the industrial network and security industries the discovery of Stuxnet triggered countless questions and wild speculations. When was it released? Who were the targets? Who created the worm? How safe are our industrial networks? How do we protect our ICS networks now? Is this cyber warfare or cyber terrorism?

On July 17, 2010, the Belarusian security company, VirusBlokAda, discovered the root kit "Rootkit.TmpHider" (Falliere, O Murchu, & Chien, 2011), they were uncertain of the rootkit's origin but later announced one of their Iranian dealer's computers had been infected with the TmpHider rootkit (Reuters, 2010). This rootkit would eventually become known as the Industrial Control System virus, entitled Stuxnet. It only infected Microsoft Windows industrial networking control hosts running Siemens SIMATIC WinCC/Step 7 controller software (Schneier, 2010). Once the industrial network control host was compromised, the worm had specific targets. It exclusively searched the network for two Siemens programmable logic controllers (PLC) the $6ES_{7\text{-}315\text{-}2}$ and the $6ES_{7\text{-}417}$ (Byres & Howard, 2011) that controlled the Finnish Vacon or Iranian Fararo Paya frequency converter drives operating specifically at 807 Hz and 1210 Hz (Falliere et al., 2011). The Stuxnet worm, then, altered the PLC's programming causing the frequency converter to operate outside it's normal frequency range at a frequency of 2 Hz and 1410 Hz (Falliere et al., 2011). A frequency converter drive converts 50 Hz AC power to a higher oscillating frequency that power high speed motor applications, such as nuclear centrifuges. By altering the frequency of the converter, the centrifuge will spin faster or slower depending on the frequency output. According to Orla Cox, a chief researcher at Symantec, the 807 Hz and 1210 Hz frequency range is the assigned frequency for converters drives designed specifically for spinning centrifuges during the uranium enrichment process (Marks, 2010). Stuxnet's ultimate mission was to destroy nuclear centrifuges. By fluctuating the speed of the centrifuge, Stuxnet damaged or destroyed the centrifuge (Homeland Security Newswire, 2010) or possibly degraded the quality of uranium during the enrichment process (Marks, 2010).

By the end of the summer of 2010, approximately 100,000 ICS hosts were infected with the Stuxnet virus. Overall, the worm targeted five specific organizations between June 2009 and May 2010 in three different attack waves (Falliere et al., 2011). According to Microsoft, industrial networks in Indonesia, India, Ecuador, the United States, Pakistan, and Taiwan (Clayton, 2010b) were infected totaling 22 manufacturing sites (Byres, 2011). Security experts are uncertain when Stuxnet or any it's variants were first detected but security powerhouses, Symantec and

Kaspersky identified early variants in June (Falliere et al., 2011) and July of 2009, unfortunately, experts believe Stuxnet went undetected for months.

Despite uncertainty surrounding Stuxnet's release or detection date, security experts agreed it was a sophisticated worm, a "game changer" (Gross, 2010), or possibly the "best" malware ever written (Keizer, 2010a). Roel Schouwenbert, a senior antivirus researcher for Kaspersky Lab called Stuxnet "groundbreaking" (Keizer, 2010a).

What makes Stuxnet a security game changer? The Symantec Security Response team who analyzed Stuxnet stated "Stuxnet is the most complex threat we have analyzed" (Falliere et al., 2011). Using four zero-day attacks and two stolen driver certificates from JMircon and Realtek Semiconductor, Stuxnet was able to by-pass Windows and anti-virus security software and escalate it's permissions from local to administrative, it then spread from host to host via inflected USB flash drives, administrative network shares, or shared network drives.

It also injected itself into Siemens WinCC project files and even well-known antivirus executable files such as Symantec's ccSvcHst.exe and rtvscan.exe, Kaspersky KAV's avp.exe, and Mcafee's Mcshield.exe. Stuxnet was able to update itself through a Command and Control (C&C) mechanism.

Once Stuxnet invaded a host it would seek Internet connectivity, if found, it would contact one of two command and control servers www.mypremierfutbol.com or www.todaysfutbol.com located in Malaysia and Denmark and exchange pertinent information such as OS version, machine and workgroup name. The C&C servers would respond with one of two controls back to the infected host, execute a remote procedure call (RPC) or execute encrypted binary code, either code provided Stuxnet with backdoor functionality (Falliere et al., 2011).

Bruce Schneier, security expert and cryptographer, stated Stuxnet was expensive to create, he estimated it took six to eight people six months just to write the Stuxnet code (Schneier, 2010) not including the theft of the VeriSign certificates. Eric Chien, Technical Director of Symantec Security Response team, believes Stuxnet was written in stages with each stage becoming more aggressive. After creating the malware, the cyber criminals needed a physical test bed to analyze the code's performance and efficiency. Symantec suggests the attackers, at a heavy expense, replicated an entire Industrial Control Systems environment from PLC's to the actual centrifuge to properly test their code.

II. INDUSTRIAL CONTROL SYSTEMS PRE-STUXNET

Industrial Control Systems (ICS) have fallen victim to cyber attacks before Stuxnet's release. For example, in 2000, a disgruntled employee accessed the SCADA system at Marooch Water Services in Nambour, Australia and spilled raw sewage into waterways (McMillian, 2007).

Again in 2005, a Zotob infected laptop connected to Daimler Chrysler's network infecting their business and industrial control network causing thirteen manufacturing plants to shut down production lines at a cost of $1.4M (Dunn, 2010). In 2007, an electrical supervisor, at the California Tehama Colusa Canal Authority, installed unauthorized software on the Supervisory Control and Data Acquisition (SCADA) system in an attempt to misdirect the water in the canal system. Also in September of 2007, the Idaho National Laboratory demonstrated a SCADA attack on a power generator reversing the polarity, which physically destroyed the generator (McMillian, 2007). Again in 2008, researchers discovered a bug in Microsoft Windows SCADA control software package Wonderwear SuiteLink. The bug allowed cyber attackers to remotely access the control host, disclose proprietary information, and disrupt service (Kaplan, 2008). As recent as 2009, the security company, McAfee identified concentrated cyber attacks from China against global oil, energy, and petrochemical companies. McAfee dubbed the advanced persistent threats cyber attacks "Night Dragon". Multiple, focused attacks are known as advanced persistent threats (APT) (Clayton, 2010b). McAfee proposed these concentrated cyber attacks utilized a combination of social engineering manipulation, spear-phishing attacks, exploitation of Microsoft Windows operating system vulnerabilities, Microsoft Active Directory exploitations, and remote administrative tools for the single purpose of stealing intellectual property in the form of project bids and finances from global oil, energy, and petro-chemical companies' (McAfee® Foundstone® Professional Services and McAfee Labs, 2011).

III. CYBER CRIMINAL'S MOTIVES

Why would cyber criminals break into corporate networks and ICS? Typically cyber criminals are organized crime syndicates, terrorists, hactivists and ordinary hackers. Hactivists are anti-establishment individuals or groups "out to prove a point" often with publicity as their main objective. They attack information system networks, servers, and supervisory control and data acquisition (SCADA) systems for various reasons. Their motives for breaching networks vary from hacking-for-ransom, hacking-for-theft, hacking-for-monetary purposes, cyber terrorism and cyber warfare (Elms, LaPrade, & Maurer, 2008).

Traditional, hacking-for-theft and hacking-for-monetary purposes meant stealing and selling individual bank account information, stealing personal financial data, and sending SPAM email throughout the Internet. Cyber criminals regularly advertise "bank accounts" on underground forums for as little as $1 or up to $1,500. Individual financial information is particularly interesting to criminals who forge bankcards. In 2007 a group of Brazilian cyber criminals were able to withdraw $4.74 million from bank accounts using stolen financial information. Botnet harvested email addresses are frequently sold to spammers, a list of one million email addresses sell for $20 to $100 (Namestnikov, 2009).

A relatively new wave in cyber crime activities is breaching corporate and industrial networks to gather political intelligence and/or steal intellectual property (IP). According to NERC's Vice President and Chief Security Officer, Mark Weatherford, "the intellectual property based businesses and entrepreneurs drive more economic growth in the United States than any other sector" (Weatherford, 2010). Trade secrets and intellectual property is valuable information to foreign competitors and worthy of theft. Intellectual property theft is illustrated by the APT Hydraq attack on Google (Zetter, 2010b) and the Night Dragon attack on petroleum companies (Symantec Corporation, 2011). The Information Technology industries estimate the loss of intellectual property theft equates to the loss of $250 billion and 750,000 jobs per year (Weatherford, 2010). Security predictions assert intellectual property theft will continue and targeted host include industrial networks, mobile devices and possibly cloud computing storage networks (Cisco, 2010).

Security experts have theorized about Stuxnet creators, the criminals could have been a single person acting alone, a disgruntled employee with insider knowledge, commercial competitors seeking a competitive advantage, state-sponsored spies, or cyber terrorist (Fitzgerald, 2010). Symantec believes the intricacies of the Stuxnet virus required insider knowledge of the ICS, meaning an employee assisted the Stuxnet creators (Falliere et al., 2011). In a National Public Radio (NPR) interview, Mr. James Lewis, Director of and Public Policy Program at the Center for Strategic and International Studies, shared his doubts about the Stuxnet virus and it's involvement with a military operation. He is hesitant to say Stuxnet is part of a military act but it feels more of an intelligence exploit, a demonstration of capability. Mr. Lewis suggests the "guys who wrote this wanted to be found ... and that's what we have to figure out" (Flatow, n.d.)

IV. IS STUXNET ESPIONAGE OR CYBER WARFARE?

If Stuxnet required insider network information and device configuration, could Stuxnet be the result of a disgruntled employees sabotage or possibly, government espionage? Security experts and technical writers have openly stated they believed Stuxnet was a deliberate government tool of espionage. The German security researcher, Ralph Langer highly speculated that Israel targeted the Iranian Bushehr nuclear facility with the Stuxnet worm with the sole purpose of destroying or delaying Iran's nuclear initiatives (Clayton, 2010a). Mr. Langer's main speaking point was 60% of the infected Industrial Control Systems were located in Iran (Falliere et al., 2011), therefore, Israel must be responsible for creating and releasing Stuxnet on Iran. Mr. Langer has not offered any technical evidence of Israel's involvement with Stuxnet but only offers speculation that he himself admits (Ragan, 2010a). Mr. Bruce Schneier summarized Israel's involvement with Stuxnet in a National Public Radio Talk of the Nation Science Friday interview as, "correlation doesn't mean causality" (Flatow, n.d.).

In another article, a New York Times author reported that Israel was secretly beta-testing Stuxnet at the Israeli Dimona complex with centrifuges virtually identical to Iran's Natanz nuclear facility (Broad, Markoff, & Sanger, 2011). Other theories accused Israel of creating Stuxnet, due to the existence of the word "myrtus" in the worm's code. Myrtus comes from the 4th century B.C, when Queen Esther, also known as Queen Hadassah, saved the Persian Jews from genocide. The Hebrew translation of Hadassah means mytle. Could this be an Israeli code marker? Not necessarily, the term myrtus could be an artifact left over from the compiler and left by mistake (Schneier, 2010).

Even Symantec speculated about Israel's involvement in the creation of Stuxnet. Code analysis revealed, before infecting a host, Stuxnet readed the "NTVDM TRACE" value in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\MS-DOS registry, if the value is equal to 19790509, Stuxnet stops its' attack. While Symantec W32.Dossier authors suggest the "do not infect" marker could be a random number or a birthdate, they do, however, offer the notion the numeric value 19790509 has Jewish historical significance. The W32.Dossier citeed Wikipedia stating May 5, 1979 is anniversary date of the first Jewish civilian's, Habib Elghanian, execution by the new Iranian Islamic government. Symantec authors reminded readers that attackers have a "natural" tendency to implicate others in their wrong doings (Falliere et al., 2011).

As of yet, no proof has come forward that Israel is responsible for creating Stuxnet (Schneier, 2010). Some security experts even discourage use of the term "cyber warfare" and state-government military cyber attacks (Flatow, n.d.). Ironically, however, that in November 2010, Iranian President Mahmoud Ahmadinejad confirmed that Stuxnet did delay Iran's nuclear ambitions (Nagesh, 2010). Espionage? Cyber warfare? The attacker may not ever reveal themselves.

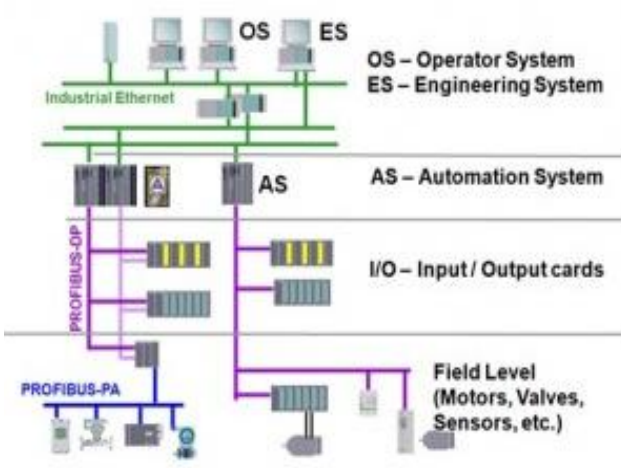
V. IMPACT OF STUXNET'S DISCOVERIES

By reverse engineering Stuxnet, security analyst ascertained Stuxnet's propagation methods, root kit injection points, and covert operations. Analysis of Stuxnet's code revealed four critical impacts to the industrial control system industry, as well as, information technology security.

Understanding Siemens PCS 7 System

It is beneficial to understand Siemens SIMATIC PCS7 terminology and how Siemens control systems function prior to discussing Stuxnet's details. The SIMATIC PCS 7 system is an Siemens integrated solution consisting of S7 PLC's, WinCC software, and the STEP 7 configuration software which is to specifically designed to configure and program Siemens' S7 line of controllers. SIMATIC is a comprehensive term covering all of Siemens automation solutions such

as machine vision to distributed I/O systems and includes programmable controllers. Siemens SIMATIC PCS7 system is broken into three functional groups, Operator System (OS), Engineering System (ES), and Automation Systems (AS) as seen in the diagram below.



Core Components of Siements SIMATIC PCS7 Control System (Byres, Ginter, & Langill, 2011)

The Engineering System's main responsibility is to configure the OS and/or AS functional groups. The Automation System is the name given to a classification of PLC's that include the Microsoft PC based software controller and the S7-300 and S7-400 lines of hardware controllers. The Operator System is a client/server function that enables secure interaction between the operator and the automated process under the control of the PCS7 system. The OS server accesses system level information from the PLC's and presents the process data to the OS Clients, as well as, archives the collected data. One of the components of the OS is the WinCC server which acts as the core component for the Human Machine Interface (HMI). It is physically connected to the "terminal bus" or Process Control Network and the "plant bus" or Control System Network. The WinCC Client is visualization software used to monitor and control the manufacturing process. WinCC Server/Client operates on Microsoft operating systems such as Windows XP and later versions of the MS operating systems. Step 7 software's responsibility is the configuration and programming of the S7 line of controllers.

Software vulnerabilities

WinCC/Step 7 utilizes a Microsoft SQL database to record PLC configurations such as Internet Protocol (IP) addresses and field device types, as well as index system log events. WinCC accesses the SQL database with a pre-configured login user account of WinCCAdmin with a password='2WSXcde' and a SQL connector login name of WinCCConnect with a password of'2WSXcder' (Radsoft, n.d.). Unfortunately, Siemens hard-coded the MS SQL back-end database default password directly into the software and Process and Control Engineers were unable to change the password. Unbeknownst to ICS professionals, the WinCCAdmin and WinCConnect passwords were publicly accessible and circulated on the Internet for several years prior to Stuxnet's release. In 2008, the WinCC default database login account and passwords were published in a Siemens technical forum but were quickly removed by the moderator.

Stuxnet exploited the hard-coded password by attaching to the SQL database and extracting PROFIBUS field device information, such a PLC model number and IP addresses. Equipped with device names and IP addresses, Stuxnet systematically searched the network for Siemens $6ES_{7\text{-}315\text{-}2}$ and the $6ES_{7\text{-}417}$ PLC's controlling Vacon and Fararo Paya frequency converters (Byres & Howard, 2011). In fact, even after the Stuxnet attack, Siemens warned customers if they changed the default password the Win/CC internal process authentication would fail, causing a severe ICS system disruption (McMillian, 2010).

Siemens is not the only ICS vendor with hardcoded passwords. In 2010, Wired Magazine reported that more than 50% of control system suppliers hard-code passwords into software or firmware (Zetter, 2010a). Regardless of the circulation of default passwords, one of the four major impacts of the Stuxnet virus was exposing Siemens WinCC and other ICS software vendors poor programming oversights as a major security flaws in ICS systems.

OS patch management

In addition to Siemens password indifference, Stuxnet exploited a "so-called" Microsoft Windows Print Spooler zero-day vulnerability. Using the MS Print Spooler, Stuxnet was able to replicate itself across the ICS network by copying itself to the %System% directory of vulnerable hosts. There is conflicting information of "when" Microsoft knew about the Print Spooler vulnerability. In a 2009 issue of the Polish publication, Hackin9, researcher Carsten Kohler detailed how to abuse the Print Spooler service and hijack a Windows host. Did Microsoft ignore the vulnerability? Did Hackin9 privately report the bug to Microsoft but yet Microsoft refused to address the vulnerability? In a 2010 email to ComputerWorld, Microsoft spokesman, Dave Forstrom stated Microsoft (MS) was not directly made aware of the 2009 Hackin9 publication and the Print Spooler bug and it was independently re-discovered during the Stuxnet investigation (Keizer, 2010b).

Would Stuxnet's destructive outcome been different if MS had released an earlier Print Spooler fix? Unlikely, even an aggressive OS patch management system would not have countered Stuxnet's use of four zero-day vulnerabilities. Stuxnet's second impact on ICS, is traditional OS patch management systems would not have negated the virus infection.

Lack of software assurance

Where does the line of security responsibility and liability for defective software begin and end? Is Siemens liable for damages to ICS since Process Control Engineers could not change the default password? Dr. Steve Bellovin, a Columbia University Computer Scientist and security expert, calls Siemens actions negligent (Zetter, 2010a). Dr. Bellovin is not alone in his criticism of software vendors and developers. In a 2005,

Santa Clara Computer & High Technology Law Journal, the authors argue since the software development industry is no longer operating from garages and basements but have become a dominate sector of our economy, consequently, it is appropriate to hold them liable just as the judicial systems holds automobile and pharmaceutical companies liable for defective products especially in the case of serious human physical harm or death (F. E. Zollers, McMullin, Andrew, Hurd, Sandra N., Shears, Peter,, 2005). The authors of "The Tort of Negligent Enablement of Cyber Crime" propose a new tort of negligence enablement holding software vendors liable for defective, insecure products that enable cyber criminals to exploit known vulnerabilities and commit crimes against the consumer (Rustad, 2005). As in the point with Siemens, they were knowledgeable of the SQL username and password vulnerability but did not address the issue with a software update and eventually paved the way for cyber criminals to exploit the PROFIBUS network.

Interestingly, at the 2011 "Information Security for Electrical Grids, Substations and Power Plants" conference hosted in Frankfort, Germany, Georg Trummer, Simatic Head of Development and Security of Siemens A&D, argued that all of Stuxnet security issues were at the PC level and no issues with PLC's (Peterson & Beirer, 2011). While Mr. Trummer does not elaborate on Siemens' lack of responsibility or their inability to take ownership regarding WinCC security issues, Siemens, did however, in a 2010 press release blame Microsoft for the Stuxnet "security breach" (Siemens, 2010).

To hold Microsoft and Siemens liable, the Uniform Commercial Code (UCC) product liability code must be applied to software sales and contracts. Legal counsel must determine if software is a service or a product. Unfortunately, the intangible nature of software prevents it from being classified as a good, even if proven otherwise, manufacturers and vendors include contract of sale language that limits their liability and damages for defects as permitted in the UCC (F. E. Zollers, McMullin, Hurd, & Shears, 2005).

Providing that software vendors are excluded from liability lawsuits under the language of the UCC and software vendors refuse to accept responsibility for poorly written programming code, in the wake of Stuxnet, Mark Weatherford, vice president and chief security officer at North American Electric Reliability Corporation (NERC) stated in a 2010 Internet article, "Addressing Stuxnet goes beyond using quality security controls. The industry needs to demand high quality software that is free from defects" (Cusimano, 2011a).

Stuxnet uncovered weaknesses within ICS software's integration, security is an emergent property, all processes and paths of software development must be assessed for security (Chisckowski, 2008). ICS Software Assurance includes integration points, tools, imbedded code, code generators, firmware, and testing practices (Ticknor, 2008).

Stuxnet's third impact to ICS is exposing the void of responsibility between ICS software vendors and operating system manufactures. ICS Process/Control Engineers are helpless to the ever-ending blame game between vendors and software developers.

All data networks are vulnerable

A digital certificate is used for encryption and digital file signing. In the case of digital file signature, a trusted third party such as VeriSign issues digital certificates to software developers for the purpose of digitally sign their software or drivers. Digital signatures ensure electronic files or software are authentic, meaning it originated from the author who originally digitally signed the file (How Stuff Works.com, 2011). Operating system such as MS Windows include a safety feature that will only permit the installation of digitally signed drivers.

Stuxnet equipped with stolen certificates were able to digitally sign their malware code, by-pass MS digitally signed driver security option, and continue its installation and infection. In a 2010 interview, VeriSign stated they, nor Realtek, were aware of the malicious use of their digital certificates and quickly revoked the Realtek certificates (Ragan, 2010b). Days after Realtek's certifications revocation, Stuxnet surfaced with another VeriSign certificate, this time stolen from JMicron Technology. No one knows how Stuxnet authors obtained the stolen certificates but rumors speculated it was an inside job, due to the fact that Realtek and JMicron both have offices in the same Taiwanese industrial park (Poroshyn, 2011).

Stuxnet and other malware painfully illustrate the vulnerabilities of all information technology corporations including the security companies themselves. Just recently, the top-ranked, security firm, RSA was the victim of an "extremely sophisticated" hack (Zetter, 2011). RSA's public response was unnerving; they would not say how their system was compromised or what type of threats customers should expect (Markoff, 2011). The public assumption was RSA, VeriSign, are Google were protected from cyber criminals, but these attacks, especially Stuxnet, demonstrates all data networks, even air-gapped nuclear facilities, are vulnerable to attacks despite the security measures deployed.

VI. CONCLUSION

In November of 2010, 70% of Siemens sales market was industrial control companies migrating from legacy process control systems to higher efficient communication standards such as PROFIBUS and Ethernet. Newer ICS standards offer more complex product tracking and management with richer data sets (Dunn, 2010). With the number of digital devices growing, Stuxnet demands security professionals to view ICS and Operational Technology (OT) security in a new perspective. Stuxnet is a wake up call for both public and private corporations.

What was ICS control and process engineers' lessons learned from Stuxnet? In 2010, the information technology research firm, Gartner Research, released a report entitled "Security Lessons Learned from Stuxnet". Systems?" The article was informative and helpful with

risk mitigation methodology, but in the words of blogger, and security expert, Andrew Ginter “none of the lessons learned seemed drawn from the Stuxnet worm” (Ginter, 2010). The real impact of Stuxnet is it accomplished what many thought impossible or unrealistic (Cusimano, 2011b), therefore, new security measures and instruments must be developed and required to protect ICS networks against future cyber attacks.

Stuxnet demonstrated the impossible was possible and Industrial Control System security experts, along side with Information Technology security experts must counter the new cyber threats with flexible, imaginative, security measures. Bruce Schneier reminds us, “Whenever humans connect to a network, there is a way in” (Flatow, n.d.).

REFERENCES

[1] Broad, W. J., Markoff, J., & Sanger, D. E. (2011). Stuxnet Worm Used Against Iran Was Tested in Israel. from http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1

[2] Byres, E. (2011). What Does Stuxnet Mean for Industrial Control Systems? Retrieved from TOFINO Security website: http://www.tofinosecurity.com/professional/what-does-stuxnet-mean-industrial-control-systems

[3] Byres, E., Ginter, A., & Langill, J. (2011). Stuxnet Report: A System Attack. Retrieved April 16, 2011, 2011, from http://www.isssource.com/stuxnet-report-a-system-attack/

[4] Byres, E., & Howard, S. (2011). Analysis of the Siemens WinCC/PCS 7 "Stuxnet" Malware for Industrial Control System Professionals: Tofino Security.

[5] Chandler, N. (2010). 57.9 Million Smart Meters Currently Planned for Installation in the United States. Retrieved April 17, 2011, 2011, from http://smartenergyportal.net/article/579-million-smart-meters-currently-planned-installation-united-states

[6] Chisckowski, E. (2008). BUILT-IN SECURITY. [Article]. *Baseline*(90), 36.

[7] Cisco. (2010). The Cisco® Annual Security Report

[8] Clayton, M. (2010a). Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant? [Article]. *Christian Science Monitor*, N.PAG.

[9] Clayton, M. (2010b). Stuxnet spyware targets industrial facilities, via USB memory stick. Retrieved April 9, 2011, from http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick

[10] Cusimano, J. (2011a). Demanding Software Security Assurance. Retrieved March 20, 2011, 2011, from http://www.exida.com/index.php/features/indepth/demanding_software_security_assurance/

[11] Cusimano, J. (2011b, March 28, 2011). The Real Impact of Stuxnet. Retrieved from http://www.exida.com/index.php/blog/indepth/the_real_impact_of_stuxnet/

[12] Dunn, J. (2010). Virus on the attack. [Article]. *Food Manufacture*, *85*(11), 63.

[13] Elms, E. R., LaPrade, J. D., & Maurer, M. L. (2008). Hacking of Corporate Information Systems: Increasing Threats and Potential Risk Management Techniques. [Article]. *CPCU eJournal*, *61*(2), 1.

[14] Falliere, N., O Murchu, L., & Chien, E. (2011). W32.Stuxnet Dossier v1.4: Symantec Security Response.

[15] Fitzgerald, P. (2010, March 20, 2011). The Hackers Behind Stuxnet. Retrieved from http://www.symantec.com/connect/blogs/hackers-behind-stuxnet

[16] Flatow, I. (n.d.). *Are 'Stuxnet' Worm Attacks Cyberwarfare?* Talk of the Nation/Science Friday (NPR). Retrieved from nfh database.

[17] Frontline. (2003). CyberWar! Retrieved March 28, 2011, 2011, from http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar

[18] Ginter, A. (2010, April 17, 2011). Gartner: Security Lessons Learned from Stuxnet. Retrieved from http://findingsfromthefield.com/?p=655

[19] Gross, G. (2010). Stuxnet changed cybersecurity. [Article]. *Network World*, *27*(22), 10-10.

[20] Homeland Security Newswire. (2010). Symantec: Stuxnet targeted Iran's uranium enrichment program. Retrieved April 8, 2011, from http://homelandsecuritynewswire.com/symantec-stuxnet-targeted-irans-uranium-enrichment-program

[21] How Stuff Works.com. (2011). What is a digital signature? Retrieved April 16, 2011, 2011, from http://computer.howstuffworks.com/digital-signature.htm

[22] Kaplan, D. (2008). Rare SCADA vulnerability discovered. Retrieved March 27, 2011, from http://www.scmagazineus.com/rare-scada-vulnerability-discovered/article/109956/

[23] Keizer, G. (2010a). Is Stuxnet the 'best' malware ever? Retrieved March 19, 2011, from http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_

[24] Keizer, G. (2010b). Microsoft Confirms It Missed Stuxnet Print Spooler 'Zero-Day' - PCWorld. Retrieved March 19, 2011, from http://www.pcworld.com/article/206010/microsoft_confirms_it_missed_stuxnet_print_spooler_zeroday.html?CID=

[25] Liberman, P. (2011). LA Times, Threatpost Reveal Gaping Security Holes in Utilities Sector. Retrieved April 17, 2011, 2011, from http://www.identityweek.com/la-times-threatpost-reveal-gaping-security-holes-in-utilities-sector/

[26] Markoff, J. (2011). Maker of SecurID Is Vague About an Attack. Retrieved March 19, 2011, 2011, from http://www.nytimes.com/2011/03/19/technology/19secure.html?partner=rss&emc=rss

[27] Marks, P. (2010). New Scientist : Nuke watchdog could help prevent future stuxnets. Retrieved April 8, 2011, from http://www.newscientist.com/article/dn19735-after-stuxnet-nuclear-watchdog-could-gain-computer-security-role.html

[28] McAfee® Foundstone® Professional Services and McAfee Labs. (2011). Global Energy Cyberattacks: “Night Dragon”. Retrieved from http://www.mcafee.com/es/about/night-dragon.aspx

[29] McMillian, R. (2007). Insider charged with hacking California canal system. Retrieved March 27, 2011, 2011, from http://www.computerworld.com/s/article/9050098/Insider_charged_with_hacking_California_canal_system?nlid=&source=NLTSEC

[30] McMillian, R. (2010). After Worm, Siemens Says Don't Change Passwords. Retrieved April 14, 2011, from http://www.cio.com/article/599816/After_Worm_Siemens_Says_Don_t_Change_Passwords

[31] Nagesh, G. (2010). Iran blames a computer virus for damage to nuclear program. [Article]. *Hill*, *17*(122), 20.

[32] Namestnikov, Y. (2009). KASPERSKY Secure List : The economics of Botnets. Retrieved April 4, 2011, from http://www.securelist.com/en/analysis/204792068/The_economics_of_Botnets

[33] Peterson, D., & Beirer, S. (2011). Special European Report: VDE/DKE Electric Sector ICS Security Event Report. Retrieved April 16, 2011, from http://www.digitalbond.com/2011/01/25/special-european-report-vdedke-electric-sector-ics-security-event-report/

[34] Piggin, R. (2010). The reality of cyber terrorism. [Article]. *Engineering & Technology (17509637)*, *5*(17), 36-38. doi: 10.1049/et.2010.1721

[35] Poroshyn, R. (2011). Can You Trust VeriSign After Stuxnet? Retrieved March 30, 2011, 2011, from http://www.associatedcontent.com/article/7841836/can_you_trust_verisign_after_stuxnet.html?cat=15

[36] Radsoft. (n.d.). Siemens - The USB attack running rampant in the wild targets Siemens SCADA systems. Retrieved April 14, 2011, from http://radsoft.net/security/20100720,00.shtml

[37] Ragan, S. (2010a). Stuxnet was a directed attack with insider knowledge expert says. Retrieved April 12, 2011, from http://www.thetechherald.com/article.php/201038/6185/Stuxnet-was-a-directed-attack-with-insider-knowledge-expert-says

[38] Ragan, S. (2010b). VeriSign working to mitigate Stuxnet digital signature theft. Retrieved March 20, 2011, 2011, from http://www.thetechherald.com/article.php/201029/5921/VeriSign-working-to-mitigate-Stuxnet-digital-signature-theft

[39] Reuters. (2010). Reuters: Factbox: What is Stuxnet? Retrieved April 8, 2011, from http://www.reuters.com/article/2010/10/28/us-security-cyber-iran-idUKTRE69R1NU20101028?pageNumber=2

[40] Rustad, M. L., Koenig, Thomas H. (2005). The Tort of Negligent Enablement of Cybercrime. *Berkeley Technology Law Journal, 20*.
[41] Schneier, B. (2010). The Story Behind The Stuxnet Virus. Retrieved Febuary 17, 2010, from http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html
[42] Siemens. (2010). Siemens Media Advisory regarding the virus affecting Simatic WinCC SCADA Systems. Retrieved April 16, 2011, 2011, from http://community.controlglobal.com/content/siemens-media-advisory-regarding-virus-affecting-simatic-wincc-scada-systems
[43] Symantec Corporation. (2011). Symantec Internet Security Threat Report.
[44] Ticknor, T. (2008). Software Assurance, Attacking Security Threats Head On. [Article]. *Journal of the Quality Assurance Institute, 22*(2), 18-18.
[45] Waterman, S. (2010). Computer worm creates an opening for copycats (pp. 1-1): The Washington Times.
[46] Weatherford, M. (2010). Mark Weatherford Security Predictions 2011 - 2012. Retrieved April 4, 2011, from http://www.sans.edu/research/security-laboratory/article/weatherford
[47] Zetter, K. (2010a). SCADA System's Hard-Coded Password Circulated Online for Years. Retrieved March 20, 2011, from http://www.wired.com/threatlevel/2010/07/siemens-scada/
[48] Zetter, K. (2010b). Wired: Google Hackers Targeted Source Code of More Than 30 Companies. Retrieved April 4, 2011, from http://www.wired.com/threatlevel/2010/01/google-hack-attack/
[49] Zetter, K. (2011). Hacker Spies Hit Security Firm RSA. Retrieved March 19, 2011, 2011, from http://www.wired.com/threatlevel/2011/03/rsa-hacked/
[50] Zollers, F. E., McMullin, A., Hurd, S. N., & Shears, P. (2005). No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age. *Santa Clara Computer & High Tech L.J., 21*(4), 745-782.
[51] Zollers, F. E., McMullin, Andrew, Hurd, Sandra N., Shears, Peter,. (2005). No More Soft Landings for Software: Liability for Defects in an Industry That Has Come of Age. *Santa Clara Computer & High Tech L.J., 21*(4), 745-782.