ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 4, April 2014

Cyber Espionage Malware and Defensive Measures for Industrial SCADA security

P.Sai Krishna[1], Arshad Shaik[2], Mohammed Tashkeel Shaaz[3]

Assistant Professor, Electrical Engineering Department, Muffakham Jah College of Engineering and Technology, Hyderabad, India[1]

UG Student, Electrical Engineering Department, Muffakham Jah College of Engineering and Technology, Hyderabad, India[2]

UG Student, Electrical Engineering Department, Muffakham Jah College of Engineering and Technology, Hyderabad, India[3]

Abstract: Supervisory Control and Data Acquisition (SCADA) systems are deeply implanted and used in the areas of critical infrastructure sectors and related environments. These computerized real-time process control systems, over geographically dispersed continuous distribution operations, are increasingly subject to serious damage and disruption by cyber means due to their standardization and connectivity to other networks. SCADA systems generally have little protection from the escalating cyber threats. In order to understand the potential danger and to protect SCADA systems, in this paper, we present a unique possible threat in the form of a malware and its countermeasures implemented on flow control system monitored by SCADA in the laboratory. We have attempted to demonstrate the vulnerability of SCADA systems to such threats and have focused more on the defensive measures and methods that are need of the day to prevent such attacks in process automation and control sectors.

Keywords: SCADA security, Instrumentation & control systems (ICS), Cyber espionage, malware, HMI (Human Machine Interface), Defensive methodologies, Intrusion Detection and Prevention System (IDPS)

I. INTRODUCTION

Supervisory Control and Data Acquisition systems abbreviated as SCADA systems are specialized and dedicated computer networks and devices that work in concert to monitor and control key processes involved in the management of machinery, equipment and production facilities. These systems operate with coded signals over communication channels so as to provide control of remote equipment (using typically one communication channel per remote station). The supervisory system may be combined with a data acquisition system by adding the use of coded signals over communication channels to acquire information about the status of the remote equipment for display or for recording functions and control. [1]

SCADA runs on a PC and is usually connected to various PLCs and other peripheral devices. It is employed to generate applications for the most demanding requirements of plant engineers, operators, supervisors and managers tailored precisely to the needs of each plant. SCADA constantly gathers data from the plant in real time, stores and processes it in the database, evaluates and generates alarms, displays information to the plant operators, supervisors and managers and can issue instructions to PLCs on the plant floor.

Over the past 30 years, SCADA devices with varying functions have been deployed nearly everywhere in the world. SCADA devices' history is rooted on distribution applications like power and water pipelines, which need to gather remote data through unreliable or intermittent low-bandwidth or high-latency links [2] While SCADA devices have had very successful deployments worldwide, they suffer one primary oversight i.e lack of security implementation.

The current state of SCADA deployments does not vary much from 30 years ago. While technological advancements have been made to these, they have not improved in terms of information security. From software development to server deployment, information security is often an afterthought in SCADA environments. Despite several documented security issues in relation to SCADA devices, little has been achieved in the past 10 years to help secure them. SCADA deployment has consistently risen. Lack of information security implementation and advancements in SCADA technology to use standardized communication protocols have dramatically increased security risks worldwide with likely far-reaching consequences.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 4, April 2014

While SCADA deployment variances are seen worldwide, one of the biggest changes in deployment methodologies is related to cloud-based deployment considerations. Several security concerns related to cloud-based SCADA deployment have been published worldwide and these considerations should be closely monitored. [3] In addition to cloud deployments, we should also consider the industry types and countries that utilize SCADA devices. Enterprises in China, for instance, largely use SCADA devices in the manufacturing industry. In the United States, SCADA devices are most utilized in the building automation and manufacturing industries. Finally, in Japan, SCADA devices are most utilized in the automotive industry.

Many countries are starting to develop and implement standards to secure SCADA environments. The United States, for instance, has come up with the National Institute of Standards and Technology (NIST) Special Publication 800-82 and IEC 62443. [4] Japan, which has a robust automotive industry, meanwhile, adheres to IEC 62443. The country's Information- Technology Promotion Agency (IPA) is also starting to implement the Embedded Device Security Assurance Certification Program with provisions for SCADA devices. [5]

II. SCADA SECURITY

Remote locations and proprietary industrial networks used to give SCADA system a considerable degree of protection through isolation [8], [9]. But in practice most industrial plants now employ networked process historian servers or data historian servers for storing process data and other possible business and process interfaces. The adoption of Ethernet and Transmission Control Protocol/Internet Protocol TCP/IP for process control networks and wireless technologies such as IEEE 802.x and Bluetooth has further reduced the isolation of SCADA networks. The connectivity and de-isolation of SCADA system is manifested in Figure 1. [6] and the related statistics of security incidents by entry point is shown in the figure 2 and figure 3.

Furthermore, the recent trend in standardization of software and hardware used in SCADA systems makes it even easier to mount SCADA specific attacks. Thus the security for SCADA systems can no longer rely on obscurity or on being a function of locking down a system.

Risk = Threat x Vulnerability x Impact

These attacks can disrupt and damage critical infrastructural operations, cause major economic losses, contaminate ecological environment and even more dangerously, claim human lives.

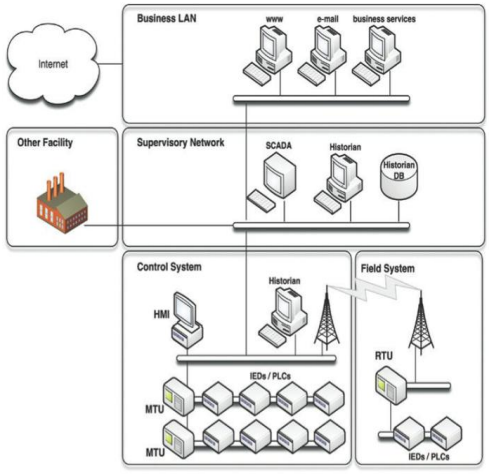

Figure.1. Sample Industrial Automated Control System Network

A. *ICS Risks and Threats*

Risks and threats to SCADA devices are now becoming common phenomena. Many of the risks surrounding SCADA device use are related to the use of HMI (Human Machine Interface) also known as MMI (Man Machine Interface) and data historians (Data loggers). Data historians or data loggers are used to record trends which are either graphical or pictorial and historical information about industrial processes for future reference. [7]

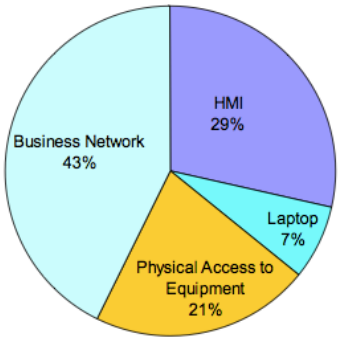

Figure. 2. Internal Security Incidents by Entry Point

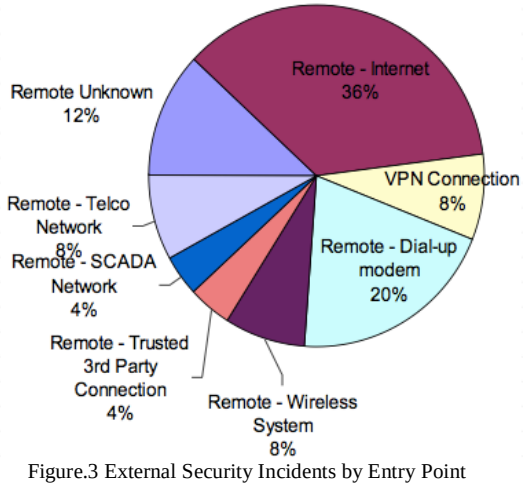

Figure.3 External Security Incidents by Entry Point

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 4, April 2014

The use of HMI, meanwhile, can also be plagued by traditional web application vulnerabilities like SQL injection and cross-site scripting (XSS) and buffer overflow bugs. HMIs can also be affected by traditional server-side vulnerabilities. If an HMI, for instance, runs on a Windows® Server® 2003, an attacker could locate unpatched vulnerabilities to exploit and, therefore, gain access to the HMI. HMI threats are likely to be introduced via connections from an insufficiently secure demilitarized zone (DMZ) or business network to a secure SCADA environment. Set points, which are deviation checks, ensure that specific control is maintained within a controlled segment or control objective. For instance, a thermostatically controlled home heating application would have a high set point for high temperature and a low one for low temperature. If the low set point is triggered by a very low ambient temperature, the heating unit will automatically turn on. Compromising an HMI in any fashion can open communications to a secure area and result in modifications to set points or controls that are similar in nature.

B. ICS Attacks publicized in the past

The following table-1 [12] publicizes the incidents of threats to ICS in some of the countries which clearly emphasizes the vulnerability of ICS systems to such threats.

Table 1. Publicized attacks on SCADA in the past

S.No	Attacks on SCADA in the past		
	Year	**Incident**	**Location**
1	2000	Sewage-processing plant attack by a former employee	Maroochy, Australia
2	2003	Nuclear power plant system was disabled via the Slammer worm	Ohio, USA
3	2008	Train derailment due to hacking	Lodz, Poland
4	2009	Traffic signal system hacked	LA, California, USA
5	2010	Stuxnet worm destroyed uranium centrifuge operations	Natanz, Iran
6	2011	Ambulance service disrupted via a malware infection	New Zealand
7	2013	Banking and broadcasting services were disrupted	South Korea

III. VULNERABILITIES

The present SCADA systems employed in industrial data acquisition and control applications and other I&C Systems are susceptible to various forms of vulnerabilities. To name a few, the entrenched factors are not limited to public information like a company's network infrastructure, insecure network architecture, Operating System Vulnerabilities enabled trap doors to unauthorized users and the use of wireless devices.

Cyber attacks on SCADA system can take routes through internet connections, business or enterprise network connections or connections to other networks, to the layer of control networks then down the level of field devices. More specifically, the common attack vectors are:

- Holes and backdoors in network perimeter
- Vulnerabilities in common protocols
- Attacks on ICS field devices through cyber means
- Attacks on crucial ICS data base
- Communications hijacking and *Man-in-the-middle* attacks
- *Cinderella* attack on synchronization and time provision.[10]

IV. SCADA SECURITY HOW IS IT DIFFERENT FROM CONVENTIONAL IT SECURITY

In SCADA systems, used in industrial process control environment the fact that any logic execution within the system has a direct impact in the physical world dictates safety to be paramount feature. Being on the first frontier to directly face human lives and ecological environment, the field devices in SCADA systems are deemed with no less importance than central hosts [11].

Also certain operating systems and applications running on SCADA systems, which are unconventional to typical IT personnel, may not operate correctly with commercial off-the-shelf IT cyber security solutions.

Furthermore, factors like the continuous availability demand, time-criticality, constrained computation resources on edge devices, large physical base, wide interface between digital and analog signals, social acceptance including cost effectiveness and user reluctance to change, legacy issues and so on make SCADA system a peculiar security engineering task. SCADA systems are hard real-time systems [13] because the completion of an operation after its deadline is considered useless and potentially can cause cascading effect in the physical world. The operational deadlines from event to system response imposes stringent constraints: missing deadline constitutes a complete failure of the system.

Latency is very destructive to SCADA system's performance: the system does not react in a certain time

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 4, April 2014

frame would cause great loss in safety, such as damaging the surroundings or threatening human lives.

It's not the length of time frame but whether meeting the deadline or not distinguishes hard real-time system from soft real-time system In contrast, soft real-time systems, such as live audio-video systems, may tolerate certain latency and respond with decreased service quality, eg. dropping frames while displaying a video. Non-major violation of time constraints in soft real-time systems leads to degraded quality rather than system failure.

Furthermore due to the physical nature, tasks performed by SCADA system and the processes within each task are often needed to be interrupted and restarted. The timing aspect and task interrupts can preclude the use of conventional encryption block algorithms.

As Real-time operating system (RTOS), SCADA's vulnerability also rises from the fact that memory allocation is even more critical in an RTOS than in other operating systems. Many field level devices in SCADA system are embedded systems that run years without rebooting but accumulating fragmentation. Thus, buffer overflow is more problematic in SCADA than in traditional IT.

V. ATTACKS ON SOFTWARE

SCADA system employs a variety of software to meet its functionality demands. Also there are large databases residing in data historians besides many relational database applications used in plant sessions.
Deploying centralized database, data historians contain vital and potentially confidential process information and data which should not be vulnerable to external attacks which may result in network crash to which they have been deployed. These data are not only indispensable for technical reasons, such as that many control algorithms rely on past process data to make correct decisions, but also for business purposes, such as electricity pricing, cabling and workstation design.
Although the algorithms of these softwares are assumed to be trustworthy, there are still vulnerabilities associated with their implementations. The most common implementation flaw is buffer overflow among others such as format string, integer overflow and etc. The fact that most control applications are written in C language requires us to take extra precaution with this vulnerability.

A. No Privilege Separation in Embedded Operating System

VxWorks a platform developed by Wind River systems was the most popular embedded operating system in 2005 and claimed 300 million devices in 2006 [14], and has since been acquired by Intel [15]. VxWorks has been used to power everything from the Apple Airport Extreme access points to the Mars rovers and the C-130 Hercules aircraft [16]. VxWorks itself is essentially a monolithic kernel with applications implemented as kernel tasks, This means that all tasks generally run with the highest privileges and there is little memory protection between these tasks.

B. Buffer Overflow

Many attacks boil down to cause buffer overflow as their eventual means to corrupt the intended behavior of the program and cause it to run amok. Some general methods are stack smashing and manipulating function pointer.
The effect of such attacks can take forms such as resetting passwords, modifying content, running malicious code and so on.

The buffer overflow problem in SCADA system takes two fronts. One front is on the workstations and servers which are similar to standard IT systems.

For example, WellinTech KingView 6.53 HistorySvr, an industrial automation software for historian sever widely used in China, has a heap buffer overflow vulnerability that could potentially become the risk of a Stuxnet type mishap if not matched. [17]

The other front manifests itself in field devices and other components that rely on RTOS thereof inherent the susceptible memory challenge. Exploits can take advantage of thefixed memory allocation time requirement in RTOS system to have more successful launchings. Let alone that many field devices run for years without rebooting. Therefore, these SCADA components, especially in legacy networks, are subject to accumulated memory fragmentation, which leads to program stall.
The Hardware/Software Address Protection (HSAP) technique offered by [18] including hardware boundary check method and function pointer XOR method to deal with stack smashing attack and function pointer attack in embedded systems , respectively.

C. Antivirus Software

It is a computer software used to detect, remove and prevent malicious programs.

A variety of strategies are typically employed.

- Signature-based detection involves searching for known patterns of data within executable code.
- Heuristics -it is possible for a computer to be infected with new malware for which no signature is yet known; and malware is often modified to change its signature without affecting functionality. To counter such so called zero-day threats, heuristics can be used.
- Sandbox-Some antivirus software can also predict what a file will do by running it in a sandbox and analyzing what it does to see if it performs any actions which could be malicious.

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 4, April 2014

VI. CYBER ESPIONAGE MALWARE

A. *Metasploit Framework*

Metasploit Framework, is a software platform for developing, testing, and executing exploits. It can be used to create security testing tools and exploit modules and also as a penetration testing system.

The Metasploit Framework also offers a shellcode database. Shellcode is a type of exploit code in which bytecode is inserted to accomplish a particular objective. Common shellcode objectives include adding a rootkit or performing a reverse telnet back to the attacker's machine. Metasploit also offers a payload database, allowing the pen tester to mix and match exploit code and objectives.

B. *Meterpreter*

Meterpreter is an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime. It communicates over the stager socket and provides a comprehensive client-side Ruby API. It features command history, tab completion, channels, and more.

C. *Laboratory Implementation*

The laboratory SCADA system for flow control setup uses Windows XP SP 3 machine with commercial anti-virus software suite installed. The GUI of the SCADA software controlling the entire process is shown in figure 4.

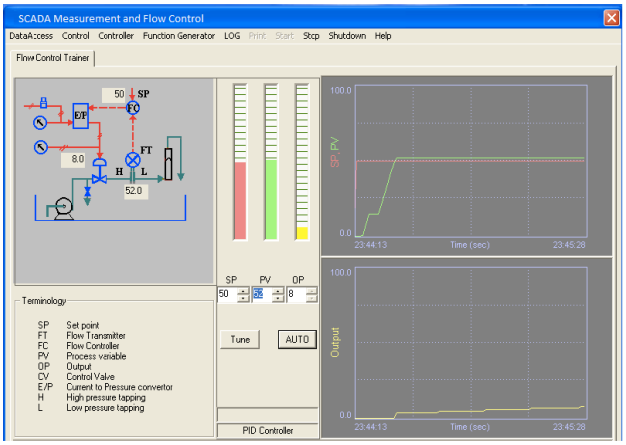

Figure. 4. SCADA GUI

The SCADA software used to control and monitor flow had a stack based buffer overflow vulnerability. This vulnerability was used to compromise the system and get a VNC session on the attackers terminal using metasploit framework without triggering the antivirus alarms as shown in the figure 5.

The vulnerability was further used to send the meterpreter stage and steal the administrator tokens to get the complete system access to the SCADA master server which can execute any malicious code and can permanently sabotage

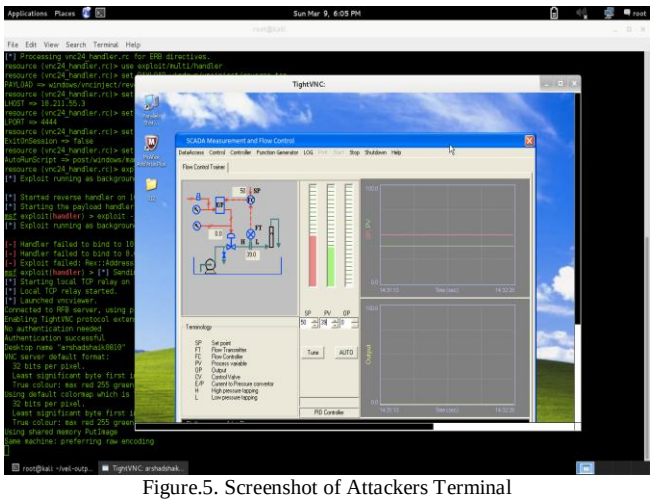

Figure.5. Screenshot of Attackers Terminal

the devices which are connected to the network. Similar techniques can be used by hackers to attack critical infrastructure and cause havoc.

To prevent such intrusions by hackers, the following defense strategies are recommended to protect the SCADA systems.

VII. DEFENSE STRATEGIES

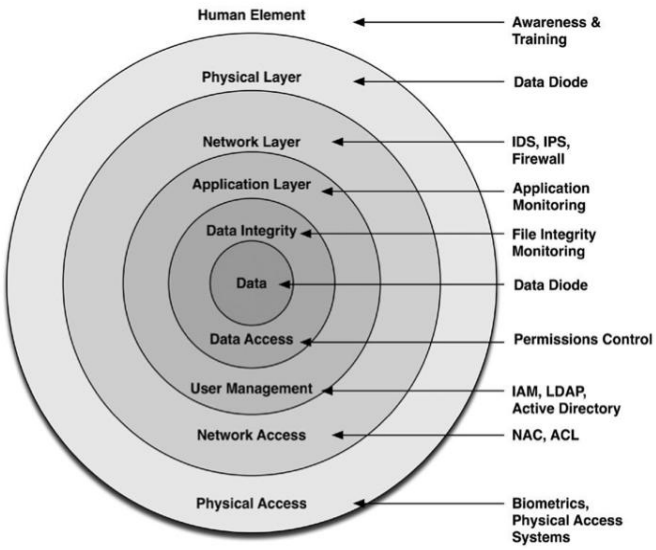

Figure.6. Layer wise defensive measures

A. *Defense In Depth*

All standards organizations, regulations, and recommendations indicate that a defense-in-depth strategy should be implemented. Although the definitions of "defense in depth" vary somewhat, the philosophy of a layered or tiered defensive strategy is considered a best practice. Figure 6.[6] illustrates a common defense-in-depth model, mapping logical defensive levels to common security tools and techniques.

Interestingly, because of the segregated nature of most industrial systems, the term "defense in depth" can and

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 2, Issue 4, April 2014

should be applied in more than one context, including

- The layers of the Open Systems Interconnection (OSI) model, from physical (Layer-1) to Application (Layer-7).
- Physical or Topological layers consisting of subnetworks and/or functional groups. Policy layers, consisting of users, roles, and privileges. Multiple layers of defense devices at any given demarcation point (such as implementing a firewall and an IDS or IPS).

Intrusion Detection and Prevention Systems

Intrusion prevention systems (IPS), also known as intrusion detection and prevention systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

Stateful Protocol Analysis Detection method identifies deviations of protocol states by comparing observed events with "predetermined profiles of generally accepted definitions of benign activity [19].

VIII. CONCLUSION

The cyber espionage malware can be blocked effectively by using Stateful Protocol Analysis Detection technology in IDPS. in addition to the above recommended defense strategies shown in the figure 6. In the laboratory test, the malicious file executed but the access to the attacker was blocked at the network level rendering the file useless by using Symantec IDPS.

REFERENCES

[1] Fortinet, "Securing SCADA Infrasructure" Available:http://www.fortinet.com/sites/default/files/whitepapers/WP_SCADA.pdf

[2] Wikimedia Foundation, Inc. (July 10, 2013). Wikipedia. "Industrial Control System." Available: http://en.wikipedia.org/wiki/Industrial_control_system.

[3] Kyle Wilhoit. (2013). "SCADA in the Cloud: A Security Conundrum?" Available: http://www.trendmicro.com/ cloud-content/us/pdfs/security-intelligence/white-papers/wp-scada-in-the-cloud.pdf.

[4] Keith Stouffer, Joe Falco, and Karen Scarfone.(June 2011). "Guide to Industrial Control Systems (ICS) Security." Available:http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf; Tom Phinney. "IEC 62443: Industrial Network and System Security."Available: http://www.isa.org/autowest/pdf/Industrial-Networking-and-Security/ Phinneydone.pdf.

[5] ISA SECURE. (April 15, 2013). "Establishment of ISASecure Japanese Scheme and Publication of ISASecure Embedded Device Security Assurance Certification Program Specifications in Japan." Available:http://isasecure.org/NewsRoom/PressReleases/Establishment-of-ISASecure-Japanese-Scheme-and-Pub.aspx.

[6] Eric D. Knapp, "Industrial Network Security" 1st ed. Waltham, MA 02451, USA

[7] Wikimedia Foundation, Inc. (July 10, 2013). Wikipedia. "Operational Historian." Available: http://en.wikipedia. org/wiki/Operational_historianhistorian.

[8] Ronald L. Krutz, "Securing SCADA systems" ,Wiley, 2006.

[9] United States Government Accountability Office, March 2004"Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems", Available: http://www.gao.gov/new.items/d04354.pdf.

[10] Bonnie Zhu, Anthony Joseph, Shankar Sastry, "A Taxonomy of Cyber Attacks on SCADA Systems" IEEE Computer Society, 2011, Pages 380-388

[11] Eric Byres, Joel Carter, Amr Elramly, Dan Hoffman Worlds in Collision: Ethernet on the Plant Floor, ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society, Chicago, October (2002).

[12] Dancho Danchev's Blog—Mind Streams of Information Security Knowledge. (October 5, 2006). "SCADA Security Incidents and Critical Infrastructure Insecurities

[13] Abraham Silberschatz, Peter Baer Galvin, Greg Gagne, "Operating System Concepts", 7th edition, Wiley & Sons, 2005

[14] P.J. Pingree, The Deep Impact Test Benches &# 8211; Two Spacecraft, Twice the Fun, Proceedings of IEEE Aerospace Conference, Page 1–9, 2006

[15] HD Moore, "Fun with VxWorks", Available:http://dev.metasploit.com/data/confs/bsideslv2010/FunWithVxWorks.pdf

[16] Metasploit Blog, August, 2010 Available: http://blog.metasploit.com/2010/08/vxworks-vulnerabilities.h

[17] Dillon Beresford, "The sauce of utter pwnage", January 2011 Available: http://thesauceofutterpwnage.blogspot.com/

[18] Zili Shao, Qingfeng Zhuge, Yi He, Edwin H.-M. Sha,"Defending Embedded Systems Against Buffer Overflow via Hardware/Software",Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC 2003)

[19] Michael E. Whitman; Herbert J. Mattord (2009). "Principles of Information Security". June 2010.