Secure VM for Monitoring Industrial Process Controllers

Dipankar Dasgupta
Mohd Hasan Ali
Center for Information Assurance
The University of Memphis
365 Innovation Drive, Suite 335A
Memphis, TN 38512
Telephone number, incl. country code
dasgupta@memphis.edu
mhaili@memphis.edu

Robert K. Abercrombie
Bob G. Schlicher
Frederick T. Sheldon
Oak Ridge National Laboratory
P.O. Box 2008
Oak Ridge, TN 37831-6085
011-865-241-6537/574-4988/576-1339
abercormbier@ornl.gov
schlicerbg@ornl.gov
sheldonft@ornl.gov

Marco Carvalho
Florida Institute for Human and
Machine Cognition
15 SE Osecola Ave
Ocala, FL 34471
001-850-202-4406
mcarvalho@ihmc.us

ABSTRACT

The biological immune system is distributed in nature and provides a rich metaphor for its artificial counterpart. Our research focuses on immunological metaphors for information gathering, analysis, decision making and deployment of attack responses. In particular, we are interested in the detection and prevention of malware which affect Industrial Process Control (IPC) systems such as SCADA (Supervisory Control And Data Acquisition). This paper describes an on-going research effort to include a secure VM (or a dedicated host) to the SCADA Network to monitor process behavior and all software updates.

Categories and Subject Descriptors

D.4.6, D.6.5 [**Security and Protection**]

General Terms

Measurement, Performance, Reliability, Security, Standardization, Verification.

Keywords

Cyber Security, SCADA Threat Mitigation, Bio-inspired Computing, Signaling.

1. INTRODUCTION

With the increased use of the public Internet for the operation, control and management of industrial systems, and power grids, security of such infrastructure has become critical. In June 2010, a sophisticated computer malware worm (Stuxnet) targeting Siemens WinCC industrial control system software was discovered [1]. It exploited multiple Zero-day vulnerabilities, and surmounts “air gaps” using infected USB thumb drives. This malware targeted against high speed variable-frequency programmable logic motor controllers (PLC) from a specific vendor. When the controllers are running at 807Hz to 1210Hz, the malware makes the frequency of those controllers vary from 1410Hz to 2Hz to 1064Hz. It is the first discovered malware that subverts industrial systems, and the first to infect a PLC rootkit [2]. Once installed on a Windows system, Stuxnet infects project files belonging to Siemens' WinCC/PCS 7 SCADA (Supervisory Control And Data Acquisition) control software. It subverts a file of WinCC called s7otbxdx.dll. After that it intercepts communications between the WinCC software and the target Siemens PLC devices. In this way, the malware is able to install itself on PLC devices unnoticed, and subsequently to mask its presence from WinCC if the control software attempts to read an infected block of memory from the PLC system. A similar malware (Duqu, a clone of Stuxnet with different payload) recently surfaced as reported [3, 4] by Symantec on October 14, 2011, which is a Remote Access Trojan (RAT) specifically designed for intelligence gathering such as enumerating the network, recording keystrokes, and gathering system information. It then lightly encrypted and compressed the log file in order to exfiltrate using a command and control (C&C) protocol.

In order to protect the industrial process control systems from such targeted attacks, we need an interconnected signaling mechanism that can pass information on unusual events in real-time to SCADA module and human-in-the-loop to make decisions.

1.1 Industrial Control Systems (ICSs)

Industrial automation is no longer limited by the walls of a production facility. More and more automation is being handled via remote communication, whether it’s from the office or from the comfort of our own home. Today’s PLCs give us the ability to access our control system to handle such tasks as monitoring via a website to determine the condition of a machine or check other statistics. With the latest PLC technology, almost anything that can be accomplished sitting in front of the machine can be accomplished from a distance, wherever there is an Internet connection.

When a process is controlled by a PLC it uses inputs from sensors to make decisions and update outputs to drive actuators, as shown in Figure 1. The process changes over time as actuators drive the

The submitted manuscript has been authored by a contractor of the U.S. Government under contract DE-AC05-00OR22725. Accordingly, the U.S Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or allow others to do so, for U.S. Government purposes.

CSIIRW’11, October 12-14, 2011, Oak Ridge, Tennessee, USA
Copyright 2011 ACM 978-1-4503-0945-5 ISBM … $5.00

system to new states or modes of operation. This means that the controller response is limited by the sensors available, if an input is not available, the controller has no way to detect the condition and act. The control loop is a continuous cycle of the PLC reading inputs solving the ladder logic and then changing the outputs. Figure 2 shows the basic operation cycle of a PLC. When power is turned on, the PLC does a quick sanity check to ensure that the hardware is working properly. If there is any fault, the PLC halts indicating an error.

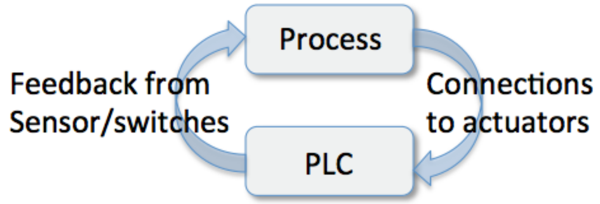


Figure 1. Separation of the Controller and Processes.

For example, if the PLC power is dropping and about to go off this will result in one type of fault. If the PLC passes the sanity check it will then scan (read) all the inputs. After the inputs values are stored in memory the ladder logic will be scanned (solved) using the stored values - not the current values. This is done to prevent logic problems when inputs change during the ladder logic scan. When the ladder logic scan is complete the outputs will be scanned (the output values will be changed). After this the system goes back to do a sanity check, and the loop continues indefinitely. Unlike normal computers, the entire program will be *run* every scan. Typical time-period for each of the stages is in the order of milliseconds.

1.2 How Communications with PLC are Made?

Industrial process controllers [5] are used for monitoring and controlling physical devices such as valves, actuators, etc. Modern PLCs have built in communication ports, usually 9-pin RS-232, but optionally EIA-485 or Ethernet. Modbus, BACnet or DF1 is usually included as one of the communications protocols [6]. Other options include various field buses such as DeviceNet or Profibus. Most modern PLCs can communicate over a network to some other system, such as a computer running a SCADA system or web browser. PLCs used in larger I/O systems may have peer-to-peer (P2P) communication among processors. This allows separate parts of a complex process to have individual control while allowing the subsystems to coordinate over the communication link. These communication links are often used for Human Machine Interface (HMI) devices such as keypads or PC-type workstation.

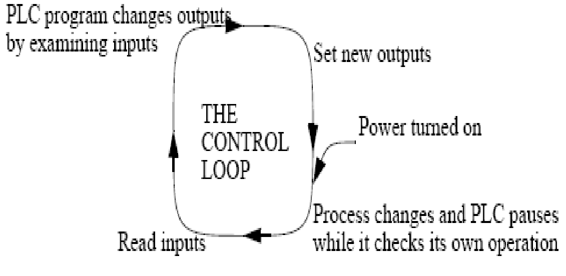

PLC program changes outputs
by examining inputs
Set new outputs
THE
CONTROL
LOOP
Power turned on
Process changes and PLC pauses
while it checks its own operation
Read inputs

Figure 2. The Scan Cycle of a PLC.

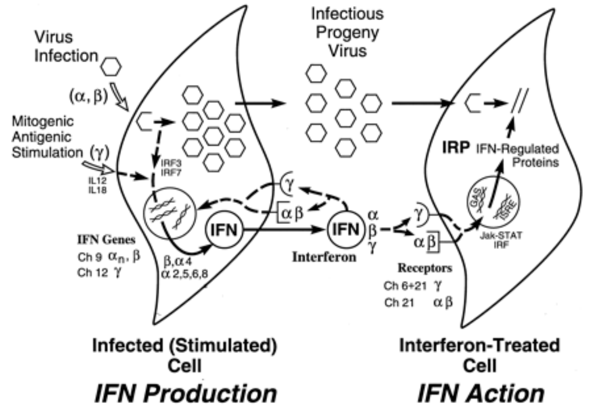


Figure 3. Interferon (IFN) Signaling Mechanisms

2. BIOLOGICAL SIGNALING EXAMPLES

The intercellular or intracellular transfer of information (biological activation/inhibition) occurs through a complex signal pathway [7]. All signals received by cells first interact with specialized proteins in the cells called receptors. An example of such process is depicted in Figure 3. It illustrates that when cell infected by viruses, it sends a special signal (called Interferon) to its neighboring cells alerting them, and they in turn release bio chemical to form a coating so that viral progeny cannot puncture their cell membrane. Also a series of biochemical changes occur within the cell through the membrane by the movement of ions in or out of the cell.

2.1 The Goal of Signaling

The signaling results in changes to the cell, allowing the cell to appropriately respond to the stimulus. This process of cellular communication results in: surface marker changes, environmental changes and destruction of foreign invaders and repair of cells. The degree of granularity of “sensors” and “actuators” available in biological systems is several orders greater. Our skin is laced with a diverse population of receptors. Each type of receptor in the skin responds to a specific stimuli: light, touch, heavy touch, pressure, vibration or pain. Some of these sensory receptors attached to finely controlled muscles with each muscle fiber having its own nerve supply.

In the context of protecting ICSs, a similar signaling mechanism can be adopted both among local PLCs and remote ones in order to alert the supervisory module of SCADA and/or human-in-the loop to prevent system malfunction or failure.

3. BIO-INSPIRED ALERT MODEL

As we investigate this analogous model, certain characteristics emerge. These have been articulated in Table 1. The information or health conditions of PLCs are being sent through different messaging, which are hierarchically managed/based on the application/circuit level, and are identified with the observed process behavior. Once that is identified, the modeled alerts will be the basis to investigate protections needed in an industrial control environment.

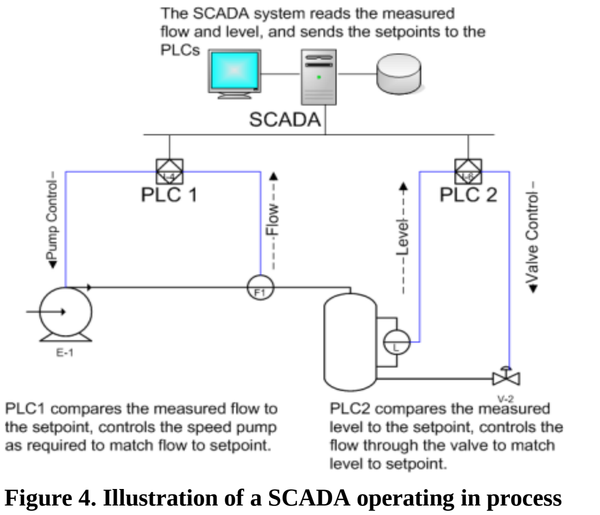
Table 1. Use of different levels of signaling

Information Type	Description	Alert Signals
Application-level Behavioral Information	Observed behavior of the monitored application/ process in a PLC.	Periodically send to the Secure VM.
Device-level Anomaly Detection	Various measures indicating significant variations in resource usage (such as memory, cpu, bandwidth etc.).	Messages may be piggy-backed and exchanged when needed.
Checking for Specific PLC Attacks	Compare with known attacks and virus signatures (using AV, NVD, US-CERT).	Event-driven messages, scheduling scanners
Other Attack Indicators	Software update attempts	Alert human-in-the-loop.

4. PROPOSED APPROACH TO DETECT ANOMALY/MAILWARE IN ICSs

A generic illustration [8] of a SCADA operating in a process control environment is depicted in Figure 4. The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs. Here PLC1 (and other PLCs as needed) compares the measured flow to the setpoint, controls the speed pump as required to match flow to the setpoint. If the information between the SCADA and PLC is altered then the flow may get disrupted; also if the setpoint in PLC is changed the flow can change significantly.

The analysis of Struxnet indicates [9] that it modifies the PLC programming logic, causing physical processes to malfunction. The malware hides the modified PLC programs and designed to change the output frequencies of specific Variable Frequency Drives (VFDs).


The SCADA system reads the measured flow and level, and sends the setpoints to the PLCs

PLC1 compares the measured flow to the setpoint, controls the speed pump as required to match flow to setpoint.

PLC2 compares the measured level to the setpoint, controls the flow through the valve to match level to setpoint.

Figure 4. Illustration of a SCADA operating in process control

4.1 Secure VM for Monitoring ILCs

In order to detect Stuxnet like industrial PLC malware, we propose to include a secure Virtual Machine (VM) or a dedicated host to the SCADA Network (as shown in Figure 5). This VM will keep a legitimate copy of the code installed during the system setup and/or during installations. Any future update will be tested in the secure VM for validity under expert's supervision); if the secure VM detects any unauthorized update or abnormal behavior, it will send multiple (aggregated) alert signals through different communication channels to a different segment of the SCADA network and operators through HMI.

As shown in Figure 5 (modified from [10]), a secure VM will monitor the Main System and RTUs/PLCs/Plant Management Interfaces for abnormal activities. Also, there is a need to establish a second channel of communication for security-related information. The sole purpose of the secure VM is to monitor PLCs operations and keep track of whether they get compromised by attack or evasion.

We believe this approach will prevent the current vulnerabilities and threats generally categorized (i.e., grouped) as follows: (1) Naturally Occurring Threats, (2) Individual and Organizational Threats (i.e. manmade), (3) Impacts on Availability (4), Financial Impacts, and (5) Likelihood of Attack. From assessments following this taxonomy, it is apparent that a comprehensive and flexible "defense in depth" management approach using independent VMs as part of the total defense is crucial to ensuring resilient (to both natural and manmade attack/failures) control systems.

However, other SCADA network security approaches [11] have been recommended and could be adopted. For example, it may be an appropriate security measure to select a controller that utilizes an embedded operating system (OS) not popularly used by the general public. This helps to keep the PLC from being vulnerable and become a target of attackers using known exploits of the OS because the knowledge base is much smaller. "Security through Obscurity" is the phrase coined by this type of security measure.

In addition, a properly configured router can provide effective protection for the control network from potential attacks. Lack of access to end-to-end connectivity prevents most unsolicited requests for communication outside the local area network. When setting up a router, be sure to limit the amount of open ports. For example, an open FTP port can lead to a possible exploit by uploading a program to override the operation of the controller. The best rule of thumb is never keep a port open that is not being used regularly.

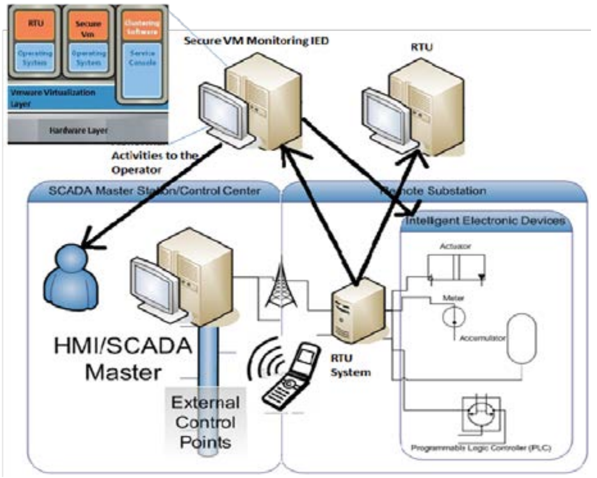


Figure 5. Detecting Stuxnet – Modified from Source.

For increased protection, a virtual private network (VPN) should be used in the SCADA network which encrypts the transmitted data when traveling over a public network - such as the Internet. Instead of opening all the ports that are needed to handle communications to the control network, one single authenticated network port should be allowed through the firewall. Since the ICSs need to operate in real time, light-weight encryption must be used to meet latency requirements.

5. CONCLUSIONS

We have presented our perspective on independent VM management and discussed some key issues within the life cycle of an independent VM designed to achieve the following: 1) control systems designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function, and 2) widespread implementation of methods for the retrograde deployment to secure SCADA that is scalable and cost-effective to deploy.

At Check Point's Conference in Sydney, Australia (September 5-6, 2011) [12], Check Point Israel security expert, Tomer Teller, said he analyzed the code of the Stuxnet worm and concluded that the possibility of it being used to take control of a nuclear warhead is high, due to the complexity and sophistication of the code contained within the Stuxnet worm [13]. What this suggests is that Stuxnet will probably not be an isolated event and we as a community to develop sophisticated responses to this line of attack.

6. ACKNOWLEDGMENTS

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the authors' academic institutions or companies, the Department of Energy, or the U.S. Government.

7. REFERENCES

[1] E. Byres, A. Ginter, and J. Langill, "How Stuxnet Spreads – A Study of Infection Paths in Best Practice Systems, White Paper, Version 1.0," Tofino Security, Abterra Technologies, SCADAhacker.com February 21, 2011.

[2] "Stuxnet," in Wikipedia, ed, 2011.

[3] "W32.Duqu: The Precursor to the Next Stuxnet," in Symantec Security Response Blog (available at http://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet), ed, 2011.

[4] "W32.Duqu: The precursor to the next Stuxnet," Symantec 2011.

[5] P. Li and J. Li, "Application of Communication and Remote Control in PLC Based on ZigBee," in Proceedings of the International Conference on Computational Intelligence and Security (CIS '09), Beijing 2009, pp. 533-536.

[6] "Programmable Logic Controller - Communications," in Wikipedia, ed, 2011.

[7] D. Dasgupta and L. F. Nino, Immunological Computation Theory and Applications. Boca Raton: CRC Press, Auerbach Publications, Taylor & Francis Group, 2009.

[8] "SCADA (supervisory control and data acquisition) ", ed: Answers Corporation, 2011.

[9] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon,," IEEE Security and Privacy, vol. 9, pp. 49-51, May/June 2011.

[10] "Distributed Network Protocol 3," ed: Answers Corporation, 2011.

[11] E. B. Fernandez, J. Wu, M. M. Larrondo-Petrie, and Y. Shao, "On Building Secure SCADA Systems Using Security Patterns," in Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee, 2009, pp. 1-4.

[12] "Overview - Many Business Threats," in Check Point Experience 2011, Sydney, Australia, 2011.

[13] H. Barwick. (2011, September 9) Nuclear Warheads Could Be Next Stuxnet Target: Check Point - Code in Stuxnet worm can be modified with right skills, says security expert. ComputerWorld. Available: http://www.computerworld.com.au/article/400299/nuclear_warheads_could_next_stuxnet_target_check_point/.