;

White Paper

Presented By: Liana Parakesyan, M.S. Cybersecurity Specialist, Cybersecurity Department
Enlightened, Inc.
1101 Connecticut Avenue, NW, Suite 800
Washington D.C. 20036
Company POC: Antwanye Ford, 202.728.7190, marketing@enlightened.com
Small Business Status: HUBZone; Small Business

ICS/SCADA INSECURITIES AND SOLUTIONS

JANUARY 2017

enlightened:
BEYOND EXPECTATION.

TABLE OF CONTENTS

TABLE OF FIGURES

1 EXECUTIVE SUMMARY

Enlightened, Inc. is a leading provider of Information Technology (IT), Management Consulting, and Cybersecurity consulting services founded in 1999 and maintains our Top Secret cleared headquarters in Washington, DC. We are certified as a small, HUBZone business holding CMMI-DEV Level 3 and CMMI-SVC Level 2 ratings. We are one of two approved Department of Defense (DoD) small business mentors in the DoD's Mentor Protégé Program (MPP) nationwide. Our MPP agreement is funded through the National Geospatial-Intelligence Agency (NGA). We have supported federal, state, and local government agencies in delivering services in Cyber Security, Software Development, Integration, and Management Consulting. We are dedicated to helping our clients achieve success in their most critical missions.

The Transportation Systems Sector is made up of aviation, highway and motor carrier, maritime transportation system, mass transit and passenger rail, pipeline systems, and freight rail. The mass transit and passenger rail includes buses, trolleybuses, monorail and heavy rail otherwise known as metros, which together in 2014 estimated 10.8 billion passenger trips (DHS, 2016).

There have been many events affecting Supervisory Control and Data Acquisition SCADA systems, such as the Stuxnet virus in 2010 impacting nuclear power plant hardware, and several incidents of transportation rail networks being affected by viruses. To help prevent such events from occurring and disrupting national security, and potentially causing loss of life, Enlightened is working to drive the technical solutions that will implement policies and standards to solve these problems. We are working to develop test beds by building Cybersecurity Integration Labs and testing software and malware frameworks.

The importance of cybersecurity in the SCADA arena is critical. Cyberspace has a reach into SCADA systems which run the country's infrastructure including transportation and the energy sector. The consequences of affected systems can be detrimental. Enlightened through teaming arrangements with cutting edge security companies have broadened our capabilities to better serve the defense of cyberspace operations and organizations including the transportation industry.

THINKSTOCK

2 CYBERSECURITY PERSPECTIVES IN ICS AND TRANSPORTATION

New vulnerabilities are discovered in computing systems that are part of Industrial Control Systems (ICS) every day. The Surface Transportation, as critical infrastructure of the United States, covers public transit systems and freight rail in the country The implications of vulnerabilities within transportation ICS systems can be detrimental to national security and life. The public and private sectors have started to address the issue of cybersecurity in informaiton systems, and have produced laws, regulations, and standards which then are used to implement technical security.

Given the importance public transportation plays in the success of businesses, the quality of life and the simplification of mobility; our ability to continually protect and enhance its functionality is critical to the advancement of business creation, expansion of robust communities and innovation that comes with dynamic mobility options. New York City, the most populated city in the United States, has a transportation system which includes one of the largest subway systems in the world and an extensive bus system in each of the five boroughs, and numerous taxis throughout the city which speaks to the value it provides across the board.

3 PROBLEMS IN SCADA AND TRANSPORTATION

Critical infrastructure sectors such as Transportation use special equipment to communicate commands and information to the various systems that are often spread over large physical locations. The integration of new technology into the Supervisory Control and Data Acquisition (SCADA) systems has introduced the existing vulnerabilities affecting today's information technology infrastructure into transportation.

Critical infrastructure are Industrial Control Systems that have components called Supervisory Control and Data Acquisition (SCADA). SCADA systems for metro transit specific environments provide the capability for remote control and monitoring of equipment located in passenger stations, and to power substations. Additionally, these systems provide control for traction power, and vehicle monitoring in heavy and light rail (APTA Part I, 2010). Vehicle monitoring systems in rail transit are part of the train control systems which includes automatic vehicle location (AVL), train control systems (TCS), and traction power control (APTA Part I, 2010).

The past several years have been filed with breaches of systems and targeted cyber crime and exploitation which have illustrated the growing concern and importance of cybersecurity. Information technology has been becoming integral part of how the transit systems operate. SCADA is the main component of how transit works today, and it is under treat from existing vulnerabilities and entities and individuals that have possible access vectors to it.

Each component in a SCADA architecture can potentially become an attack vector. Switches, routes, and firewalls are entry points into the network that connect many networks together. For example, the non-vital maintenance Wide Area Network (WAN) may not be as secure as the control office, however, it is still connecting to the control office, and presents possible threat.

To understand attack vectors and sources of cyber insecurity, the architecture of the systems is vital. The rail transit system is divided into the following components: transportation, control signaling system, communications, stations, notification methods, train-sets, and traction power systems (APTA Part II, 2013). There are various attack vectors that exist. There are several sources of threats; accidents and errors, intentional attacks, embedded software, insiders, and outside individuals wanting to cause harm. Table 1 illustrates various attack paths and scenarios.

The attack vectors focus on presenting malicious code the PLC. The PLC can also be any other vital controlling equipment within the transit infrastructure. Any device and equipment that has the ability to control or make changes to field equipment is considered vital. The Stuxnet virus that infected Iranian Nuclear power plant in 2010 targeted and infected the PLCs, and then was able to control the hardware equipment in the power plant (Symantec, 2010).

In addition to feeding malicious code to the PLC and other devices, malicious code can also be fed to the servers which control the SCADA application. Next gen SCADA applications sit on Windows servers and clients. The field equipment is then connected to the server. This makes the SCADA application further exposed to the present day computer vulnerabilities. These aspects are taken into consideration when building the attack tree and drawing the attack vectors.

4 SOLUTIONS FOR TRANSPORTATION ICS AND SCADA

The continuous focus on upgrading and improving the quality of the transit experience provides a strong baseline that strategically enhances the vibrancy of the region, which has also encumbered the responsibility to stay on the cutting edge of technology integration, securing human and capital assets. Integration of information technology and information systems into the transportation has given way to a new generation of threats which also yield a plethora of ways to increase the safety and quality of the experience for those who patronize public transportation, creating a culture that motivates more citizens to take advantage of public transportation. The ransomeware hack that occurred on November 28th, 2016 affecting the San Francisco Municipal Transportation Agency (SFMTA) is a perfect example of the growing threats that have the ability to affect trandition and new IT systems.

Enlightened provides holistic solutions that addresses integration of vulnerability assessments and identification, prevention through remediation, next generation cybersecurity solutions, and management integration to streamline operational and management processes. Enlightened is the epicenter of solutions listed in this section; Management Consulting, Security Assessments for SCADA and ICS, and Next Generation Solutions and Innovation to address a growing concern in the sensitive legacy environments.

5 MANAGEMENT CONSULTING

Enlightened's CMMI-SVC Level 2 business process methodologies are scalable to meet client needs such as WMATA, NJ Transit, CJCC, a small District of Columbia Government office, to Federal clients such as the U.S. Agency of International Development (USAID) and the U.S. Department of State (DOS). At CJCC, we incorporated our Customer-Oriented Process

Improvement Initiative (COPII) methodology based on a repeatable process to obtain baseline data collection requirements for a criminal justice information portal that facilitates real-time data exchange among multiple disparate systems. Similarly at USAID and DOL, Enlightened established the baseline environment and presented recommendations to migrate from the current state to the target state for a global food distribution system and personal property assessment, respectively. Enlightened does the same for WMATA, NJ Transit, and many more agencies. Regardless of the project size and scope, our methodology can be customized to address specific client needs.

Our team is lead by experts that have over 30 years of experience delivering innovative IT and business solutions to Federal, state, and local clients. The team consists of subject matter experts such as Technical Project Lead, Strategic Planners, Transportation Planner, and Cybersecurity and Legacy Systems Specialists. Methodology and Strategy

The Safety Directive 16-2 issued to WMATA in 2015 outlined many issues being operation and management issues. The issues included outdated policies, no tracking or implementing change management, Enlightened has utilized cybersecurity Subject Matter experts to map the issues found in Directive 16-2 to the NIST 800-53 families. The following families map to the deficiencies found in Safety Directive 16-2:

- Access Control
- Audit and Accountability
- Configuration Management
- Maintenance
- Personnel Security
- Physical and Environmental Protection
- Program Management
- System and Communications Protection
- System and Information Integrity

The issues in Safety Directive 16-2 affected the above nine NIST 800-53 families out of eighteen from the cybersecurity framework. This means while there has not been an active implementation of cybersecurity in the transit industry; about half of the issues can be resolved by implementing operational and management solutions. Implementation of management process that affects the above families will build a framework that affects security, efficiency, and safety positively.

The primary methodology to be used is Enlightened's Customer Oriented Process Improvement Initiative (COPII) illustrated in Figure 5. COPII was developed to employ a uniform, repeatable process review cycle focused on customer interests, needs, and expectations. Included under COPII are best practice studies, new process studies, process analysis, business-process improvement, process restructuring, and efficiency studies. The COPII approach is composed of four distinct phases as described below.

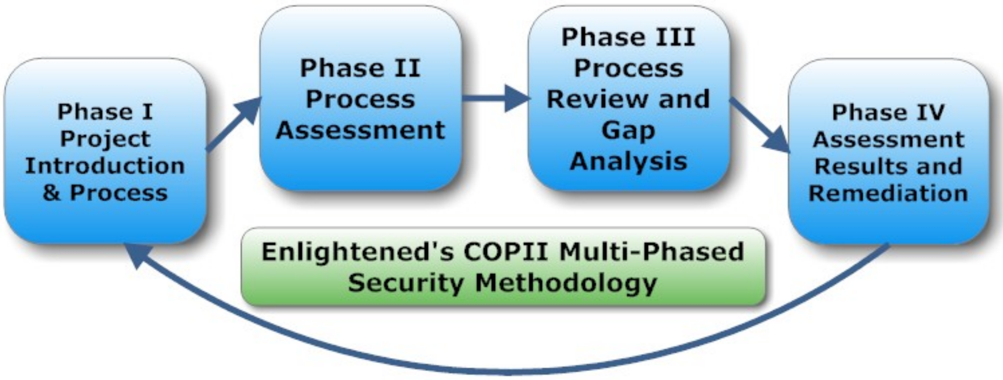

Phase I Project Introduction & Process
Phase II Process Assessment
Phase III Process Review and Gap Analysis
Phase IV Assessment Results and Remediation
Enlightened's COPII Multi-Phased Security Methodology

Figure 1 – Stages of the COPII methodology and the value each stage contributes objectives by defining the security posture of the organization and providing recommendations to establish a more effective and robust security posture

6 SECURITY ASSESSMENTS FOR SCADA AND ICS

Enlightened has developed the Cybersecurity Integration Lab where researchers and developers have a rapid, efficient, and effective test bed for developing and testing new cybersecurity technologies as well as new cybersecurity threats. Enlightened is one of two small business Department of Defense (DoD) mentors through the National Geospatial-Intelligence Agency (NGA) Mentor Protégé Program (MPP). Through our protégé's Cybersecurity Integration Lab, we are able to integrate and provide our federal clients with a test bed environment. Enlightened also utilized our Cybersecurity Lab to provide test beds and solutions.

Tools such as Wireshark provide non-intrusive methods to examine network traffic. One of the most important data to collect from the cybersecurity ICS assessment is network traffic output. This will give the ability to trace all the data entry points to the ICS, and can be done without any data packets being sent to the systems, minimizing risks of slowdowns to halt of network communication in sensitive environments.

Enlightened shall gather system information through system review and analyzing all systems and security documentation. Enlightened will identify the implemented security controls not just through the examination of documentation, but also by ensuring the control is implemented and being carried out as outlined in the documentation.

The lab will be used to run Wireshark and Nmap (this tool will only be used in the lab) on the backup systems to conduct asset discovery and port/service scanning. Enlightened uses Nmap to identify remote access paths in and out of the perimeter and Internet Protocol (IP) addresses of the firewalls, routers, Internet access points, the agency's major systems, and any point(s) of entry for remote access. Nmap identifies the network connections, open ports on a target host, and the services that run on the ports. This is done to assess the security posture of devices and network (e.g., designated computers or servers should not have certain ports open).

7 TECHNICAL SOLUTIONING WITH NEXT GEN TECHNOLOGY

Team Enlightened possesses a cybersecurity toolkit which can help remediate ICS/SCADA system and network vulnerabilities and deficiencies in multiple domains and paralleled perspectives. These tools help to secure individual components on the information system, but also the network activity associated with them in a normal functioning SCADA environment. Team Enlightened will use Defense in Depth approach to provide the most value to its customers, by solving a host of issues that affect the ICS/SCADA domain.

Enlightened develops test beds by building Cybersecurity Integration Labs with the goal of providing clients and industries with a space for the growing cyber capabilities and combating cyber threats.

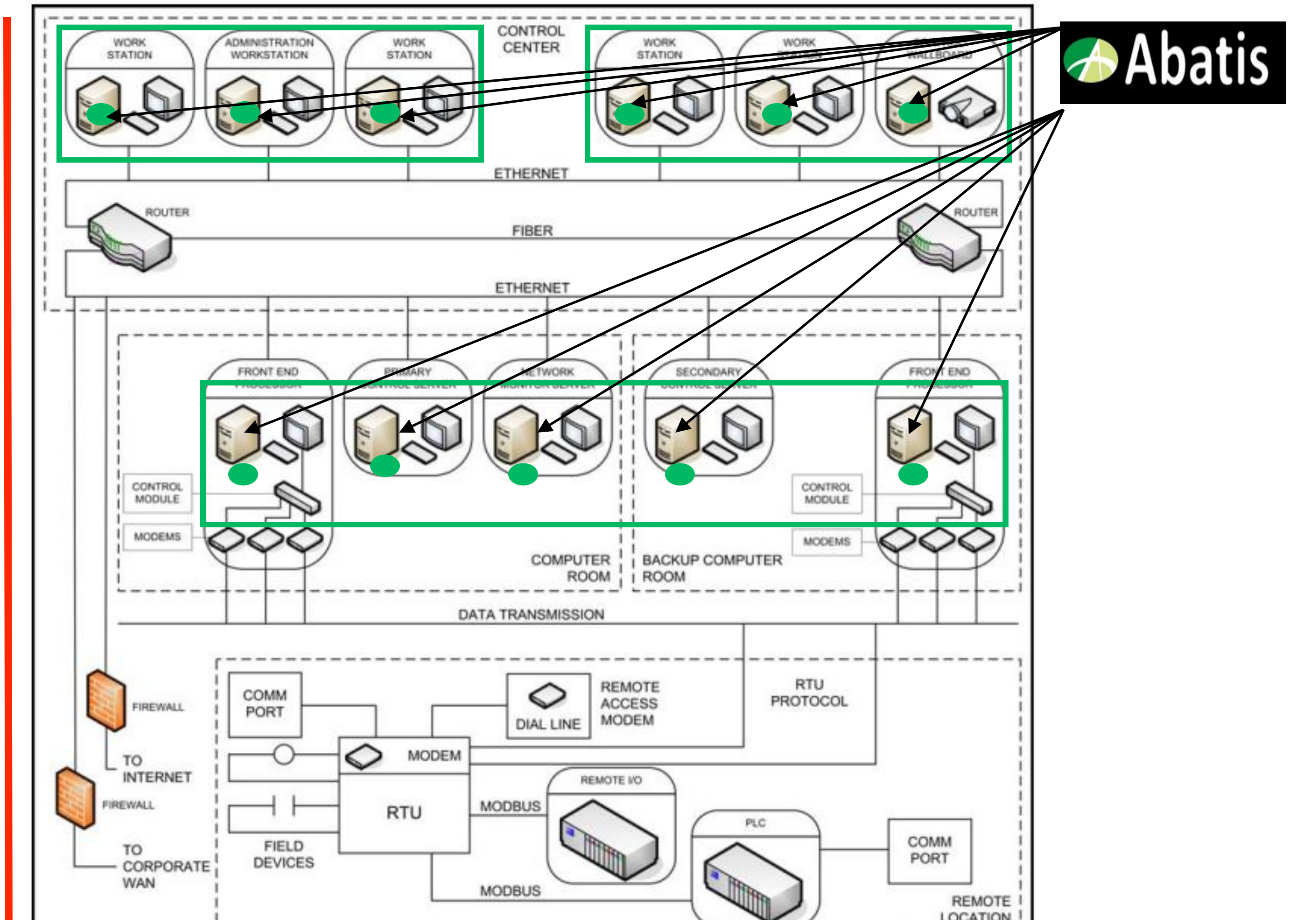
Enlightened has reacted quickly to the growing need of cybersecurity in the transportation arena which includes the world of Supervisory Control and Data Acquisition Systems (SCADA) research and development initiatives. Enlightened discovered that IT systems are being integrated into command and control systems, and the combination of these systems has increased cyber threats. To solve this problem, Enlightened has partnered with cutting edge proactive cybersecurity solution providers that focus on stopping malware before it reaches the vital parts of the information system. In accordance with developing and implementing cutting edge cybersecurity software Enlightened has been developing test beds.

The purpose of the cybersecurity lab is to assist the cybersecurity mission by studying, testing and developing cutting edge cybersecurity technologies for countering cyber threats. The Cybersecurity Lab shall support NGA, DIA, NSA Intelligence Communities and DOD mission requirements and shall directly support highly sensitive IC Information Technology Enterprise (IC ITE) mission initiatives. These requirements shall support the mission operations of the war fighter, the intelligence analyst and the national level decision makers. The Cybersecurity Lab provides agility and expanding space for cybersecurity testing, integration and training.

The use of the Cybersecurity Lab has lead to testing SCADA applications with cybersecurity tools that Enlightened is driving to integrate into the transportation industry. Events such as viruses affecting the hardware in SCADA systems that are used in transportation and nuclear reactors, and all other critical infrastructure sectors, have prompted the urgency in finding solutions. Cyberspace changes every day, and Enlightened's capabilities allow for the research and development of strategies and technologies to combat cyber threats that pose danger from small businesses to critical infrastructure of our country.

Our first tool ABATIS demonstrated in Figure 2, addresses host security deficiencies. ABATIS prevents unauthorized changes to the system and/or component's static environment. It prevents system modification at the kernel and device levels, so that the system remains locked down, in the event that an intrusion occurs and attempts to modify the system at the root level. WhiteCloud and iBoss are used to secure the additional layers providing Defense in Depth for all network components and functions.

Figure 2 – Implementing Cybersecurity Solutions in SCADA/ICS environment.



8 ABOUT ENLIGHTENED

Enlightened, Inc. is a leading provider of Information Technology (IT) consulting services founded in 1999 and headquartered in Washington, DC. We are certified as a small, HUBZone business; and one of the few to achieve Capability Maturity Model Integration (CMMI) Development Level 3 and CMMI Service Level 2 appraisals.

Enlightened develops and delivers strategic IT and management solutions to complex business problems of global, national and local significance. Enlightened provides expertise in the following capabilities:

- Management Consulting
- System Integration
- Information Assurance
- Business Process Outsourcing

Enlightened serves Federal (Defense and Civilian), state and local government agencies and private sector entities that face daunting challenges in achieving their mission.