INL/CON-11-20953
PREPRINT

DOE/DHS Industrial Control System Cyber Security Programs: A Model for Use in Nuclear Facility Safeguards and Security

INMM 2011

Robert Anderson
Trond Bjornard
Mark Schanfein
Paul Moskowitz

July 2011

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

DOE/DHS INDUSTRIAL CONTROL SYSTEM CYBER SECURITY PROGRAMS: A MODEL FOR USE IN NUCLEAR FACILITY SAFEGUARDS AND SECURITY

Robert Anderson, Trond Bjornard, Mark Schanfein and Paul Moskowitz
Idaho National Laboratory
P.O. Box 1625, MS 2608, Idaho Falls, ID 83415

ABSTRACT

Many critical infrastructure sectors have been investigating cyber security issues for several years especially with the help of two primary government programs. The U.S. Department of Energy (DOE) National SCADA Test Bed and the U.S. Department of Homeland Security (DHS) Control Systems Security Program have both implemented activities aimed at securing the industrial control systems (ICSs) that operate the North American electric grid along with several other critical infrastructure sectors. These programs have spent the last 7 years working with industry including asset owners, educational institutions, standards and regulating bodies, and control system vendors. The programs' common mission is to provide outreach, identification of cyber vulnerabilities to ICSs, and mitigation strategies to enhance security postures. The success of these programs indicates that a similar approach can be successfully translated into other sectors including nuclear operations, safeguards, and security. The industry regulating bodies have included cyber security requirements and in some cases, have incorporated sets of standards with penalties for noncompliance such as the North American Electric Reliability Corporation Critical Infrastructure Protection standards. These DOE and DHS programs that address security improvements by both suppliers and end users provide an excellent model for nuclear facility personnel concerned with safeguards and security cyber vulnerabilities and countermeasures. It is not a stretch to imagine complete surreptitious collapse of protection against the removal of nuclear material or even initiation of a criticality event as witnessed at Three Mile Island or Chernobyl in a nuclear ICS inadequately protected against the cyber threat.

INTRODUCTION

Cyber security is a field that has grown in magnitude, complexity, and importance and continues to move into new uncharted territory. The effects from a cyber attack are only partially known, but the ones known cause great concern. As the adversaries have historically concentrated most of their efforts finding new ways to manipulate microprocessor-based business information systems, the industrial control systems (ICSs) are becoming more of a target because they control so much of society's critical infrastructure including nuclear facility control and monitor operations, safeguards, and security systems. Any security discussion without the mention of cyber security is remiss. Nearly all modern infrastructures are operated and controlled by digital systems that if left unprotected can be manipulated via software and firmware to perform in a manner not intended by the developers or operators. Manipulation can be accomplished via denial of service, defeat, disruption, deception, and potentially through achieving access to other connected networks. It is not a stretch to imagine complete surreptitious collapse of protection against the removal of nuclear material or even initiation of a criticality event as witnessed at Three Mile Island or Chernobyl in a nuclear ICS inadequately protected against the cyber threat.

In 2003, the U.S. Department of Energy (DOE) and Department of Homeland Security (DHS) launched two multi-million dollar programs that addressed the growing cyber concern for U.S. critical infrastructure and key resources (CIKR); the DOE National SCADA Test Bed and the DHS Control Systems Security Program. The programs' goal was to create a national-level capability to coordinate

and support government and industry efforts to reduce ICS vulnerabilities, respond to associated threats, while enhancing the cyber security posture for the nation. A majority of the supervisory control and data acquisition (SCADA) vendors and a few asset owners have been processed through these programs. Multiple DOE national laboratories participate and provide a potential template that can be duplicated for nuclear operations, safeguards, and security. Because industry owns, operates, and controls the majority of the critical infrastructure in the U.S., the U.S. government is somewhat limited in its involvement and enforcement of tight cyber security policies. However, the government can advise, offer support, and encourage industry participation via these programs toward a proactive response to cyber threats. The ultimate goal for these two government programs is to enhance the security posture of the nation's critical infrastructure including the control systems themselves, enhanced secure installations, increased cyber security training and awareness, and regulations that help enforce the best cyber security practices known to be effective. As a result of these programs, the critical infrastructure security posture has been hardened. An investigation into these programs may help nuclear operations, safeguards, and security programs mimic similar attributes to defend against common cyber threats.

Several key elements of these programs are discussed in the following paragraphs. Each element describes various attributes, functions, and implementations within the programs.

ASSESSMENTS

Fundamental to each U.S. government program is the ability to gain access to typical ICSs for cyber vulnerability assessments. With knowledge and analysis of these systems, vulnerabilities can be identified, mitigations recommended, and corrective actions can be developed providing enhanced protection against successful penetration and manipulation.

Two types of assessment are performed by the programs. The first is a laboratory assessment. The programs will solicit vendors that represent 80% of the market share in a particular sector to volunteer their equipment for an assessment. Upon acceptance, a nondisclosure agreement is approved to protect both the vendor proprietary information and any newly discovered vulnerability that are found. The vendor will provide a representative test system to the laboratory. It is configured in a typical user configuration with the latest version of hardware, software, and firmware. Researchers are given a set amount of hours to examine the whole system and determine weak points that may be exploitable. Penetration testing is not normally performed during this assessment. Rather, the cyber researchers assume an adversary has already gained a presence on the network and follows logical pathways an attacker would take to attain control of the system. Once vulnerabilities have been found, reports are written documenting the findings, how they were identified, and suggested mitigations. A standard vulnerability scoring is applied to help prioritize the mitigation process. The vendor receives the report and proceeds to mitigate the vulnerabilities found. A short time afterward, patches are received back from the vendor and applied to the test system. A validation of the mitigations is performed. If funding is available and the program determines the need, more detailed assessments are performed. The goal of this type of assessment is to educate the vendor about how to discover cyber flaws in their systems and the best methods to mitigate or eliminate the vulnerabilities found. Ultimately, the ICS should provide the most hardened surface to cyber attacks.

The second type is an onsite assessment where the systems analyzed in the laboratory are assessed at the end users facility for installation and configuration vulnerabilities. If an ICS is hardened to a cyber attack, but the installation and configuration allows for remote access and easily compromised system or

user access, then the entire operation is compromised. Onsite assessments are concentrated toward educating the users of the systems so that the best cyber security practices are followed providing the most secure methods to prevent the attacker from entering and manipulating the systems. Common installation and configuration practices are reviewed such as security programs and policies, firewall rules, intrusion detection systems, logging policies, third-party application uses, remote access policies, network architectures, user access policies, and many more. Analyzing these factors provides a complete assessment. Part of the education process is to provide the end user a better understanding of why certain policies are adequate or inadequate. Concepts, such as cyber forensics, are typically not well understood. Organizations must be taught that waiting until a breach has occurred is too late to begin thinking about forensic topics.

In order to provide this level of assessment, four foundation blocks must be in place; namely cyber researchers that are best in class, test beds that can support such equipment with the capability to be organized in a variety of configurations, agreements with the vendors so that discovered vulnerabilities and suggested mitigations found can be protected for dissemination, and finally a fundamental paradigm change that builds cyber security protections directly into new designs.

1. Cyber Researchers

Well-educated and trained personnel must be available for cyber security assessments. Universities have recently begun to offer specialized degrees for cyber research careers with an emphasis on well-written code, software quality assurance, security development life cycles (SDLC), reverse engineering, social engineering techniques, penetration testing, specific application assessments, and many other specific focus areas. Regardless of the researchers selected, whether in-house personnel or a well known security organization, the final product (assessment) must provide value to all consumers of the assessment including the end users. A false sense of security is the last outcome any organization should come away with because cyber protection is never one 100% secure.

2. Test Beds

Environments must exist that can support assessments both in the laboratory and in the field. In addition, the right test beds are required to produce a near complete assessment of the particular equipment being assessed, whether it is Information Technology (IT) or ICSs. The electrical infrastructure test beds may be more difficult for a small organization to produce. Within the national laboratories, several electric transmission and distribution systems already existed and, therefore, were capable of supporting electrical assessments. A dedicated substation was assigned at the Idaho National Laboratory to be used exclusively for power infrastructure assessments including local intelligent electronic devices, large SCADA systems, representative corporate business networks, and onsite installations. In addition to physical electrical infrastructure, control systems and IT test beds must be available and configurable to operate in a typical utility setup for effective assessment results.

3. Nondisclosure Agreements

Proprietary and critical infrastructure assessment information acquired must be protected from adversaries who are intent on exploiting or manipulating critical infrastructure systems for their gain. To be successful at protecting our infrastructure and to make a difference, secure information handling is critical to the success of any program. Information must be shared to incite change, but must also protect organizations and infrastructure from complete devastation whether it be industry financial ruin or the collapse of a city or nation. Information must be shared at a broad summary level to the general public

for education and awareness of vulnerabilities that may be similar to other organizations. Nondisclosure agreements allow the negotiation for such information to be released without harm to any participating party.

4. Cyber Security by Design

One of the program goals of any assessment performed is to educate the vendors and asset owners toward the concept of addressing cyber security directly into original designs and installations so that more comprehensive and fundamental protection against cyber attacks is addressed. When software and firmware are designed with an eye toward adversary abuse, misuse, or data entry manipulation, it forces the design team to add appropriate checks and techniques to allow only acceptable responses within the operating parameters of the application itself. Getting vendors and asset owners to invest in education and training for cyber security methods and techniques is a paradigm shift because these concepts have never been traditionally a part of the requirements. Initially, vendors and end users may see this investment as a cost. However, in the long run, it may help prevent a catastrophic event.

OUTREACH/TRAINING

In order to fully embrace the benefits of government cyber security programs, all parties involved must understand the concepts, terminology, vulnerabilities, threats, and consequences of a cyber attack. For many years, the DOE and DHS programs have trained and educated personnel from private industry; universities; other governments, including local and state; asset owners; and law enforcement. Several mechanisms have been used to provide this outreach. Training courses have been produced that educate the beginner up to the advanced personnel responsible for the daily task of protecting operational systems. Some classes use classroom material while others incorporate advanced real-time simulators that pose (red) hackers and (blue) defenders against each other. In addition, (white cell) observers can manipulate the scenarios to bring real world experiences to the training. These courses bring cyber awareness to a heightened level.

Vendor user group meetings are also attended by experts from these programs to help answer questions the end users may have particularly concerning their specific (vendor) installed systems. Sometimes, with legal approval from both participating parties, a vetted summary level presentation of the laboratory assessment will be presented to the users. Coupled with this presentation is usually a vendor response explaining how the vendor proposes to mitigate the identified vulnerabilities and provide schedules detailing the patch or upgrade process. A tremendous response from the users knowing the vendor has proactively performed a cyber assessment and has promised mitigations in a timely manner.

Documentation has been developed that provides excellent resources for all interested parties to learn more about cyber vulnerabilities, threats, mitigations, and best practices programs that any organization can implement. Documents have been produced that help an asset owner know what cyber security procurement language to ask of their vendors when purchasing a new or upgraded system. Instructions on how to set up cyber security programs with all the necessary areas of interest including training, critical asset identification, assessments, forensics, patch and password management policies, maintenance, and incident response are available. Common vulnerabilities found among multiple assessments are identified, normalized, and categorized into common vulnerabilities documents to educate others of typical recurring vulnerabilities. These documents are posted on the DOE and DHS websites for download.

Conferences, workshops, standards committees, educational institutions or universities, and government hearings are just a few of the venues where these programs have provided expertise and presentations to help expand the knowledge base of cyber security and the threats cyber adversaries impose. These venues allow a great number of personnel to be educated at one time and generate lively discussions. In addition, information sharing and analysis centers (ISAC) around the country benefit from the information produced by these programs including incidents that may apply to one or more of these particular sectors.

Tools are useful to help asset owners self assess their security posture. A few tools have been produced that identify the appropriate regulations and standards associated with a particular infrastructure sector and apply those against the current owners' policies and procedures to determine compliance including a gap analysis. Identifying gaps can focus attention to those areas to concentrate efforts that provide the biggest improvement.

SIMULATION

DHS has funded advanced modeling, simulation, and analysis techniques for examining the link between ICS and CIKR sectors. Using the High Level Architecture (HLA) simulation bus for distributed computer simulation systems, existing detailed models can be incorporated to provide the dynamic responses necessary for accurate simulation and interdependencies between multiple infrastructure failures. The HLA architecture demonstrates a viable means for modeling infrastructure behavior under adverse effects including failures and damage. The interdependencies are modeled and shown how they impact each other during these disturbances. These simulations help personnel understand potential situational awareness scenarios.

STANDARDS

Both programs have participated in standards bodies. They have contributed to the development of requirements, the creation of the standards documents themselves, and the detailed review process necessary for a quality product that meets all interested parties' agendas. At times, the programs will also broker between vendors and asset owners as a neutral party when such a need arises. Mentoring those sectors, not historically known for incorporating cyber security into their industry, has also been one of the functions served by the programs.

In recent years, many of the nuclear agencies, institutes, and several other international agencies have begun to rigorously investigate cyber security initiatives collimating into policies, best practices, guidance documents, and other useful aides. Recently, documents, such as the Nuclear Energy Institute (NEI) 08-09 Rev 6 "Cyber Security Plan for Nuclear Power Reactors," Nuclear Regulatory Commission (NRC) Regulatory Guide 5.71 "Cyber Security Programs for Nuclear Facilities," and the International Atomic Energy Agency (IAEA) "Technical Guidance for Computer Security at Nuclear Facilities," promote and support guidance for protecting computer and cyber assets in nuclear facilities. These documents have been created with several industries' input including government cyber security programs and may be useful for the enhancement of a safeguards and security program.

INCIDENT RESPONSE

DHS supports an ICS cyber emergency response arm of the National Cyber Security Division (NCSD) called the Industrial Control System Cyber Emergency Response Team (ICS-CERT). It is responsible for handling critical infrastructure ICS cyber incidents primarily within the U.S. Their charter is to

provide critical infrastructure ICS cyber incident response, situational awareness, threat analysis, preparedness, and malware analysis. They share and coordinate vulnerability information and threat analysis through information products such as advisories and alerts for responsible disclosure. They also provide coordination with other Cyber Incident Response Teams (CIRT) throughout the country and globally.

A fully functional malware lab constantly researches new viruses, worms, trojan horses, spyware, etc., for attack vectors that may find their way into control systems. The malware lab also responds to incidents where infections have anchored themselves into a network and forensic analysis is required. During the forensic analysis, infected systems are analyzed to determine the severity, origin, and potential ramifications of contaminated systems. Decisions are made quickly to determine losses, mitigations, and restoration procedures.

NUCLEAR FACILITY SAFEGUARDS AND SECURITY APPLICABILITY

Nuclear facility safeguards and security must accept the fact that cyber attacks are growing at an alarming rate and that it demands immediate attention to incorporate best practices from similar sectors that can be used in a complete and comprehensive security program. Many of the key elements presented above have direct applicability to nuclear safeguards and security. Safeguards have traditionally been designed to protect against physical unauthorized tampering but may not have been designed to protect against unauthorized data tampering. As modern safeguards and physical security systems have incorporated standard communications protocols, they have also introduced common vulnerabilities that may be susceptible to exploitation. Where past inspectors had to manually retrieve data, today data retrieval is networked. Connecting multiple monitoring and control systems together provides a greater attack surface, which may facilitate greater adversary opportunities.

The modification or creation of a cyber security program within nuclear operations, safeguards, and security is current, thorough, and continuously reviewed for new and evolving threats. Cyber security represents a new frontier for attackers to own, manipulate, destroy, or deceive depending on the mission of interest and warrants a detailed and well-planned protection program. Defense-in-depth strategies are necessary to defend against a constant barrage of malware, social engineering attacks, and brute force attempts. Some key cyber security program elements for safeguards and security are discussed for applicability.

Education

Education, training, and awareness are potentially the first step toward a modified or new cyber security program. Until nuclear facility operators and managers understand the language, consequences, and attack vectors, cyber attacks are nearly impossible against which to defend. Personnel must be cognizant of the threats including any updates to the design basis threats at their facility's in order to protect against a constantly evolving adversary. Once an organization has been educated, the success of the program is improved.

Assessments and Audits

It is imperative that part of any comprehensive cyber security program, independent assessments, and audits are conducted to verify and validate whether the systems are meeting stated or implied security requirements including organizational policies. Cyber requirements must be clearly identified. Audits can obtain valuable information about activities from an audit trail. With constantly changing objectives,

cyber hacking methods and tools continue to evolve, become more complex, and offer a wide range of attack methods not currently identified or understood. These threats must always be assessed, analyzed, and mitigated in a continual process. A lapse in assessment frequency may provide the window of opportunity necessary for an attacker to execute an exploit. Assessments can be performed on physical equipment and on processes themselves.

Part of the ICS cyber assessment process is to identify firmware and software vulnerabilities that may lead to exploitation. Equipment must be both verified and validated through a rigorous vendor quality assurance process that meets the end user requirements or the equipment must be accessed through an independent cyber assessment. Either method must show evidence of a thorough process by which cyber vulnerabilities were identified and adequately mitigated. Failure to perform this type of vetting may lead to unacceptable exploitation.

Simulation

Simulation or table top exercises should include the creation and execution of cyber attack scenarios. These simulations or exercises must be credible as seen from the attacker point of view. Manipulating the system for surveillance may be the end goal. Using the system network as a means to reach other protected networks may be the ultimate objective. It is not good enough to simply measure the cyber consequence as a system that is either on or off; available or unavailable. The danger comes when the system is used against itself as a tool for the attacker without any knowledge by the user.

Standards

Standards development must be created to ensure the best possible cyber defenses are incorporated into each safeguard or security system. As new functionality is designed, cyber security standards must be available and provide guidance for such improvements. It is critical that safeguards and security personnel be given the opportunity to contribute to these standards so that specific safeguards and security attributes are reflected. Safeguard systems exhibit unique attributes that require special attention including international policies.

Incident Response

When unattended safeguard systems become erratic or unstable, policies and procedures must be in place to diagnose and identify root causes, including potential cyber attacks, artifact retrieval if necessary, system functionality restoration, analysis, and future protections. All these aspects must be fully embedded within a complete cyber security program. In addition, some means of malware identification must be accessible either within the organization or through an external, vetted, independent security firm.

SUMMARY

Whether ICS cyber security is included as part of an existing security program or it is created as a separate program, key components must be addressed and incorporated into a comprehensive security plan. Although several guidance documents exist to help with this effort, the aim is to apply the best, most recent cyber security practices into a formal security program that provides policies, procedures, and an overall security awareness that includes relevant cyber components. The DOE and DHS programs mentioned above can provide an outline for the application into nuclear safeguards and security. Certain components must be a part of a comprehensive program including outreach and education, assessments, table top exercises or simulations, support during incident responses, and input

toward the development of specific standards that meet the needs of nuclear safeguards and security. Inspectors need to understand their changing role as the experts in the field who can identify evidence of common hacking techniques that may lead to deception or disruption of data confidentiality, integrity, or availability.

Although existing nuclear security programs and plans may have addressed cyber or computer security, it must be emphasized that cyber breaches may not only shut down systems but rather be transformed as a tool for the adversary that can exfiltrate information, be manipulated as an accomplice to redirect actual events in support of diversions, or be used as a conduit to other connected networks of interest. Key to any effective strategy is the acknowledgment that cyber threats exist, that it is expanding in complexity, and that inaction is not satisfactory.

CONCLUSIONS

As the DOE and DHS critical infrastructure cyber security programs have been successful for the critical infrastructure industry, so should the programs that are responsible for the protection and accountability of nuclear material. Industry, end users, and governmental partnerships can be developed to assess and share information and education concerning cyber security protection. With recent cyber attacks on ICSs in nuclear facilities such as Stuxnet, with motives for espionage, sabotage, or the removal of special nuclear material, the time for action is immediate. Key elements of successful ICS cyber security critical infrastructure programs should be considered for potential application within the nuclear safeguards and security programs.

BIBLIOGRAPHY

1. Brochure, *CSSP Year in Review, FY 2010*, Department of Homeland Security.

2. *National SCADA Test Bed Fact Sheet*, Enhancing control systems security in the energy sector.

3. *DHS Control Systems Security Program Fact Sheet.*

4. *Nuclear Energy Institute 08-09 Rev. 6,* "Cyber Security Plan for Nuclear Power Reactors."

5. *Nuclear Regulatory Commission Regulatory Guide 5.71* "Cyber Security Programs for Nuclear Facilities."

6. *National Institute of Standards and Technology 800* series of computer security policies.

7. *International Atomic Energy Agency,* Technical Guidance for Computer Security at Nuclear Facilities.

8. *National Electric Reliability Corporation,* Critical Infrastructure Protection Standards