SAND2012-10831C

CYBER SECURITY TRIAGE FOR SMALL WATER UTILITIES

Lon Dawson, Jennifer Stinebaugh, Anna Hernandez, Doug Dailey (URS), Will Atkins, Patrick Edgett, Keith Schwalm (DNK), Ray Finley, Robert Pollock

Sandia National Laboratories
PO Box 5800
Albuquerque, NM 87185

1 EXECUTIVE SUMMARY

Water utilities are at risk to a host of threats. In the United States, much attention has been placed on physical security of drinking water systems, particularly following the passage of the Bioterrorism Act of 2002 that required each large utility to complete a vulnerability assessment. Likewise, much research has gone into development of tools and protocols for contaminant warning systems in recent years. One area that is becoming increasingly important is the cyber security of water systems, as all utilities have a complex and increasing level of connectivity for their physical assets, their enterprise assets, and their control systems. While the Environmental Protection Agency (EPA) has direct responsibility for protection of the water sector, the Department of Homeland Security (DHS) has broad responsibility for cyber security of the nation's critical infrastructure and ensuring the resiliency of complex, interrelated systems including the US Water Sector. The DHS Control Systems Security Program (CSSP), now known as the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), sponsored the Critical Spares Project at Sandia National Laboratories to specifically focus on identifying how critical assets may be impacted via cyber connectivity. The water sector is one of four critical infrastructures evaluated in the Critical Spares Project. This project developed and then demonstrated a methodology for identifying security upgrades for the most critical cyber-connected components. The utility assessments brought to light the cyber security challenges utilities face from new enterprise applications such as those for energy efficiency, asset management, shared networks, physical security monitoring, and cloud computing. Utility SCADA Managers are being asked to integrate their control systems with these applications to reduce operational cost. Guidance is needed by SCADA Managers to implement these new applications while maintaining their cyber security. As part of the methodology development effort, several water utilities were assessed and cyber security threats and mitigations were developed for the vulnerabilities identified. We believe these utilities are representative of most utilities and the recommendations are appropriate for consideration on an industry-wide level.

The report includes a summary of the Critical Spares Methodology and extends to the assessment findings for a representative small water utility and first step recommendations to improve cyber security and resiliency. For this small utility we use the concept of "triage"—treating the highest risks first with the most impactful mitigations will result in the most improvement in overall cyber security. Our recommendations are consistent with established American Water Works Association (AWWA) and DHS guidance (e.g., Roadmap to Secure Control Systems in the Water Sector, March 2008) and, collectively, have the least effort/cost for implementation, represent common control system security practices, and target the lowest level adversary—a common hacker.

Although the Sandia methodology was found to be flexible and useful, the team noted that the CIKR sectors' general lack of threat understanding and ability to develop consequences of concern and relevant attack scenarios does not presently support transferring an unsupported methodology to the sectors.

2 INTRODUCTION

2.1 Project Background

The Department of Homeland Security (DHS), National Cyber Security Division (NSCD), Control Systems Security Program (CSSP) contracted Sandia National Laboratories (SNL) to develop a generic methodology for prioritizing cyber-vulnerable critical infrastructure assets and developing mitigation strategies against their loss or compromise. The initial project was divided into two phases with three discrete deliverables: (1) a generic methodology report suitable to all Critical Infrastructure and Key Resource (CIKR) sectors; (2) a sector-specific report for Electric Power Distribution; and (3) a sector-specific report for Water and Wastewater, to include generation, water treatment, and wastewater systems.

The generic methodology is summarized below. The final report can be found at http://prod.sandia.gov/techlib/access-control.cgi/2010/101845.pdf and includes:

- The tasks, resources, and key individuals necessary to identify and prioritize CIKR assets that could be damaged by the failure of automated control systems;
- How the assets could be lost or compromised; and
- The development of mitigation strategies to minimize the associated probability and/or consequences of such events.

The methodology is designed to apply across any CIKR sector, with the understanding that some modifications are necessary to conform to the needs of each sector. The process steps are illustrated in Figure 1.

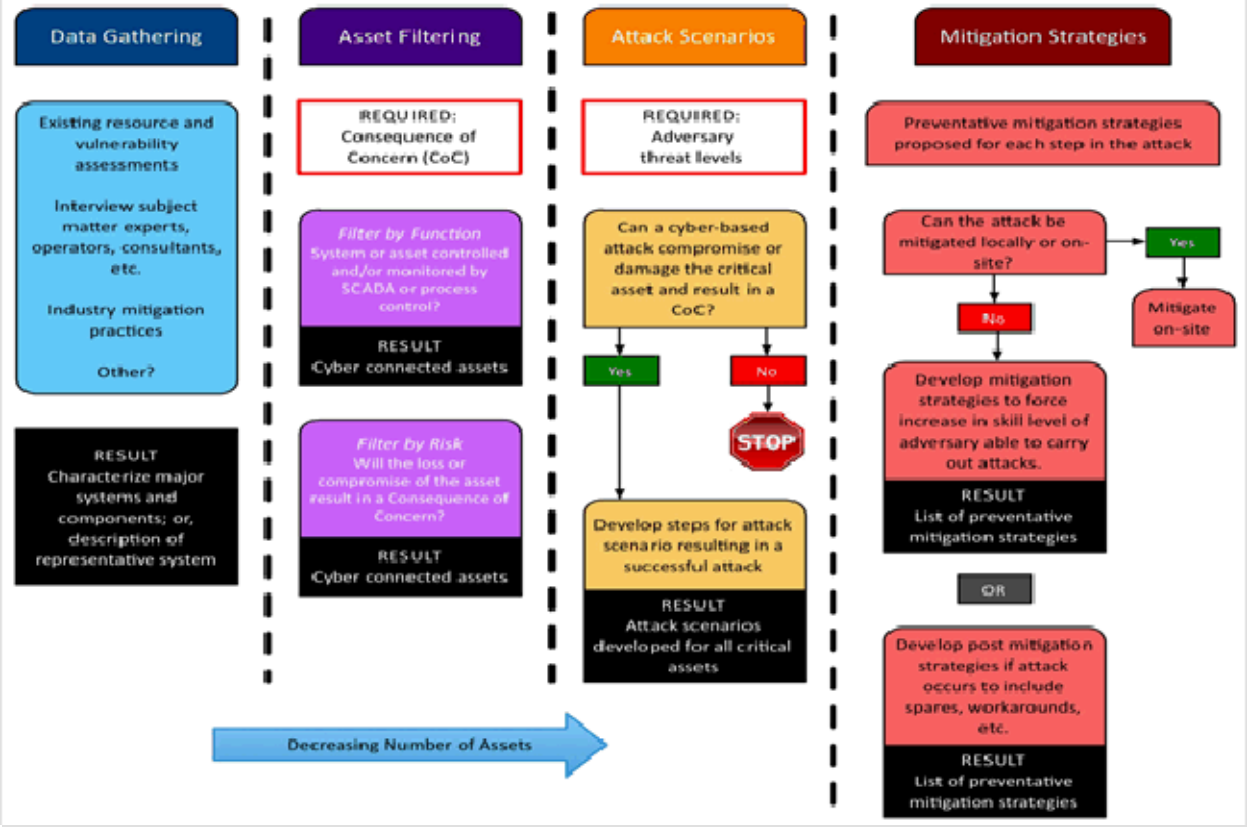

Figure 1 *Methodology Overview*

The process steps can be broadly categorized as follows:

- Team organization and data collection;
- Development of representative system description;
- System review and cyber-connected asset identification;
- Consequence of concern and critical asset determination;
- Threat-level determination and attack scenario development;
- Mitigation development—protective actions and post-consequence strategies;
- Industry verification and validation; and
- Final report delivery.

The Sandia methodology is systematic. The process steps enable the team to identify mitigations for protecting the most vulnerable components from the most likely attacks.

2.2 Phase II Goals and Activities

In Phase II of the project, Sandia was tasked with exercising the methodology at utilities in four CIKR sectors (Water, Electric, Oil and Gas Transportation, and Nuclear). The intent was to vet the methodology with real-world scenarios and stakeholders, to incorporate the lessons learned into the methodology, and to transfer a proven and improved methodology to DHS.

The breadth of the Phase II assessments was very large, ranging from utilities responsible for less than 100,000 customers to utilities responsible for more than two million customers. In each assessment, stakeholders were engaged to develop the consequences of concern (i.e., to answer the question, "What keeps you up at night?"). These conversations ultimately drove the assessment scope.

In the water sector, four utilities were assessed. One was a very small utility that was found to be lacking in cyber-security basics, so the assessment team delivered that utility a subset of cyber-security practices focused on stopping a common, unskilled hacker. The assessment team was able to develop actionable mitigations sharable with the larger community.

2.3 Organization of Present Report

The present report will describe the small water utility assessment. We present an overview, a description of the scope of the assessment, a list of the consequences of concern, and a summary of the associated vulnerabilities and mitigations. Lastly, we conclude with recommendations.

3 SMALL WATER UTILITY FINDINGS

Water and wastewater systems are fundamentally important for human health and for the proper functioning of modern communities. In 2007, the US water/wastewater sector included more than 50,000 community water systems. This number includes public, cooperative, and private systems. About 4,000 systems provide water in localities with more than 10,000 inhabitants, and the remaining 46,000 systems provide water to localities with less than 10,000 inhabitants. The utilities in the water sector rely on control systems that monitor operations, collect data, and provide feedback to human operators. In the larger utilities, many of these control systems are automated and some operations are conducted without direct action from a human operator. Because of this increased reliance on automated control systems, the need to understand the potential vulnerabilities of these systems to cyber attacks is essential. It is generally recognized that the various subsystems in the water sector include equipment and operations that, if compromised, could lead to disruption of important water services. Additionally, public utilities in the water sector possess personal information about customers that, if compromised, could lead to loss of confidence in the utility.

3.1 Small Utility Overview

The small water utility we assessed was a ground and surface water utility that is organized within a county district. The district has a service population of approximately 65,000. The district has developed a straightforward management structure consisting of a Board of Directors that is elected by its customers, a general manager, and staff members. The small water district has put together a professional team of experts to operate and maintain both water and modern sewer systems.

3.2 Scope

The assessment focused on categorizing the risk to components associated with SCADA systems that were related to production and treatment of water and to water distribution. During the initial data gathering, a general lack of cyber security was found, so the assessment team worked with utility personnel to develop a basic cyber-security posture and a set of mitigations for identified vulnerabilities. Collectively, these mitigations have the least effort/cost for implementation, represent common control system security practices, and target a low level adversary—a common hacker. As such, the results of this assessment and the associated mitigations represent what fairly unprotected, unsophisticated water utilities might want to consider to protect their systems from potential cyber attacks.

3.3 Consequences of Concern

Based on discussions with utility personnel, the following consequences of concern were identified:

1. Any fatalities or illnesses.
2. Long-term impacts of 7 or more days for recovery.
3. Economic loss to owner/operator or to the community of $3-$5M.
4. Public confidence and/or the utility reputation are negatively impacted.
5. Cyber attacks that cause interruptions and can be easily replicated. This consequence of concern was one in which the utility would be quick to resort to manual operation as a solution.
6. Unauthorized shut-off notices generated through the Customer Service IT system.

The assessment team found that a common hacker using openly available tools and well-known techniques could gain access and cause disruption, disclosure, and modification of components of the SCADA and IT systems because of the lack of a cyber-security culture, policy and procedures, and network segmentation. Such attacks could result in COCs 2, 3, 4, 5 and 6.

3.4 Vulnerabilities

Vulnerabilities for the small water utility are described in three broad categories: network segregation, disaster recovery, and secure practices. These categories help the utilities focus mitigation efforts into theme areas as opposed to a much longer list of seemingly disparate efforts. The grouping also allows for mitigation prioritization based on utility-specific security goals and budgets. It is likely that these general categories of vulnerabilities are common across much of the water/wastewater sector, particularly in the numerous small and unsophisticated systems, and that the lessons learned described here are broadly applicable across the entire sector.

3.4.1 Network Segregation

Network segregation refers to the segregation, or lack of segregation, between the various IP networks (accounting, IT, and SCADA) used by a utility to conduct its operations. The vulnerabilities identified were:

- No segmentation: the small utility's enterprise network allows unauthorized access to the customer service system, potentially leading to consequences such as disclosure of sensitive customer information or issuing shut-off orders to multiple customers.

- No segmentation: the lack of separation between the enterprise (IT) and SCADA network allows unauthorized internal access to SCADA control, potentially leading to consequences such as disabling alert settings.

3.4.2 Disaster Recovery

Disaster recovery refers to both the policy and the engineered controls that allow for recovery and operation in the event that automated systems are compromised. The vulnerabilities identified were as follows:

- SCADA system logic is not backed up within the small utility. Rather, backups of this vital operations data were held by a contractor to the utility.
- No SCADA master or recovery plan exists at the small utility.
- Little instrumentation exists for local control of facilities that allows "graceful failure" of system control.
- The staff is reliant on the automatic operations of the water system. There is a lack of confidence that the system can be effectively operated manually.
- Poor physical security and environmental protection exposes servers, workstations, and local controllers.
- Common security awareness and training is lacking.

3.4.3 Secure Practices

Secure practices refer to the policies and procedures that are necessary for secure cyber operations. The team identified the following vulnerabilities:

- A common, shared password is used for the VPN between the Internet and enterprise (IT) network.
- Unencrypted or weakly encrypted wireless communication is in use.
- Secure HTTP (HTTPS) is not utilized for connections made to the SCADA host nor is the access protected with strong passwords.
- Control over administrative accounts is poor, e.g., privilege control is inconsistent.
- Unsupported operating systems are in use (operating systems no longer supported by their manufacturers).
- Security policy and procedures are inadequate.

3.5 Mitigations

To address the various vulnerabilities identified at the small utility, the assessment team recommended the mitigations listed in the following subsections.

3.5.1 Network Segregation

- Segment the SCADA network from outside access; improve access controls. Apply intrusion detection/prevention around network assets.
- Provide segregation and access controls for both IT and SCADA network. Apply intrusion detection/prevention around network assets.

3.5.2 Disaster Recovery

- Train SCADA operators to download remote terminal unit (RTU) configurations. Secure backups of these configurations in an access-controlled fireproof safe.
- Develop policies and training for loss of SCADA that allow for seamless and prolonged manual operation.
- Develop manual operation training and provide facilities to allow for local control of key systems, subsystems, and components.
- Institute semi-annual training on manual operations and disaster recovery. Operate the system semi-annually in manual mode for one work shift, followed by a debrief meeting to generate "lessons learned."
- Consider a dedicated control room that is secure from environmental effects.
- Assign at least one person at the utility to be responsible for SCADA network security and, as part of that responsibility, ensure that the responsible person is familiar with the SCADA network infrastructure and data warehouse components.

3.5.3 Secure Practices

- Allow only authorized individuals remote access to enterprise (IT) network via the VPN. Enforce strong passwords per user. A strong password is sufficiently complex enough to resist guessing attempts by both humans and computer programs.
- Require strong encryption (AES-CCMP) and authentication using Wi-Fi Protected Access II (WPA2, IEEE 802.11i) for all 802.11 (Wi-Fi) networks. Disable 802.11 networks in locations that do not require it or when it is not in use.
- Require secure HTTP (HTTPS) connectivity and strong individual passwords when accessing the SCADA host.
- Implement role-based security and the principle of least privilege. Role-based security limits access to a system by assigning roles to users. The roles allow access only to specified operations. The "principle of least privilege" means giving users only those privileges that are essential to doing their job.
- Download software updates directly from the Microsoft website.
- Implement a backup communication system or ensure local control is not impacted by loss of SCADA connectivity.
- Implement a scheme (including date/time, cost, action/change) to document all SCADA and IT network architectures, changes, and operations.
- Limit or disable the ability to implement RTU logic revisions or downloads remotely.
- Implement a policy to require escort for SCADA contractors.
- Develop and document cyber-security policy and procedures.

3.6 Summary and Recommendations

The mitigations described above are a small subset of common cyber-security practices. They represent first steps in a process that will achieve a large increase in security for the least investment. They are an effective start to improving the assessed organization's security culture.

Based on the results presented in this high-level report and in discussions with utility personnel and the American Water Works Association (AWWA) water sector user group, we believe there is an urgent need in the water/wastewater sector for improved cyber security practices. The work described in this report represents the logical extension of efforts by DHS and AWWA to define requirements for sector-specific cyber security. What was not expected, however, was the clear lack of implementation of roadmap recommendations on the part of some utilities in the water sector. It is our belief that the methodology and actions described herein can be duplicated across broad segments of the water sector with little added investment. Such action would serve to strengthen both the understanding and posture for the entire sector and would benefit all participants—DHS, the AWWA, and the utilities.

4 CONCLUSION

The systems in our nation's CIKR sectors are particularly crucial, and they are highly reliant on industry-specific automation technology and physical components that often have long production lead-times and a small number of associated suppliers. Such supply chain limitations mean that CIKR systems could be forced offline for months or years by a successful cyber attack or by a catastrophic cyber failure that damages essential components. DHS has taken a lead role in proactively identifying methods to measure the risk to critical systems and components and to develop strategies to mitigate that risk. The methodology for this process has been developed and vetted in this project. For a given attack scenario, the process will yield defensible mitigations.

Improving our nation's infrastructure is a complex undertaking and will certainly not be addressed by a simple solution. Rather, many solutions must be collectively implemented to achieve a resilient infrastructure that is defended in depth. Although the methodology is available and successfully proven, perhaps a more daunting challenge remains—to influence change across many organizations and entities. The next steps involve a disciplined focus on which events are more likely and, thus, which mitigations must be prioritized.

Acknowledgements

The report summarizes portions of an ongoing effort by the US Department of Homeland Security, National Cyber Security Division (NCSD), Critical Infrastructure Cyber Protection Awareness (CICPA) to protect Critical Infrastructure and Key Resources.

Special thanks to the American Water Works Association (AWWA), Kevin Morley for his support and direction