Universities Council on Water Resources
Journal of Contemporary Water Research and Education
Issue 129, Pages 8-12, October 2004

Assessing the Vulnerabilities of U.S. Drinking Water Systems

Jeffrey J. Danneels and Ray E. Finley

Sandia National Laboratories

During the Clinton administration, the importance of our critical infrastructure was highlighted by the National Security Council in Presidential Decision Directive 63 (PDD 63). PDD 63 was superseded recently when President Bush signed Homeland Security Presidential Directive 7 (HSPD-7). HSPD 7, like its predecessor PDD 63, establishes a national policy under which federal departments and agencies are required to identify and prioritize United States critical infrastructure and the key resources needed to protect them from terrorist attacks. PDD 63 and HSPD 7 also encourage Federal departments and agencies to form public and private partnerships to pursue the goal of lowering risks to our national assets due to malevolent events. The Environmental Protection Agency (EPA) is assigned responsibility for the water infrastructure, which includes both drinking water and wastewater systems.

Subscribers (mainly water utilities) of the American Water Works Association Research Foundation (AwwaRF) were also becoming concerned about security at drinking water utilities and encouraged AwwaRF to assist them in understanding potential malevolent threats. In response to PDD 63, and with input from public water utilities, both EPA and AwwaRF initiated programs to understand and mitigate the security vulnerabilities of drinking water utilities. The events of 9/11 accelerated the development of these programs.

This paper describes efforts to assess and mitigate the vulnerabilities of drinking water utilities. (See O'Neill and Hais, this volume, for a discussion of wastewater security issues.) This paper covers several key areas, including threat assessment, water contamination, and response effectiveness.

Law Requires Vulnerability Assessments

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 into law (PL 107-188). This Act requires community water systems that serve populations of greater than 3,300 persons to conduct vulnerability assessments. According to EPA statistics, approximately 4,800 water utilities fit into this category. When combined, these water utilities serve over 256 million people.

Large drinking water utilities, defined as those serving more than 100,000 people, were required to conduct their vulnerability assessments and submit a report to the EPA by March 31, 2003. Drinking water utilities serving 50,000 to 100,000 people were to conduct their vulnerability assessments and submit a report by December 31, 2003. Drinking water utilities serving 3,300 to 50,000 people were to conduct their vulnerability assessments and submit a report by June 30, 2004.

Vulnerability Assessment Process

In cooperation with the EPA and AwwaRF, Sandia National Laboratories (Sandia) created the Risk Assessment Methodology for Water Utilities known as RAM-W™. RAM-W™ is the most widely

used methodology to assess security risks at large water utilities. Several thousand water utility owners/operators, regulators, and water industry consultants have been trained in the use of RAM-W™. Other tools have been developed by other entities and were used at several large water utilities, but were applied more prevalently to medium and small water utilities.

Figure 1 illustrates the process followed in RAM-W™ and demonstrates the iterative nature of the methodology. This methodology was developed through decades of security research and development at Sandia, initially focused on safety of nuclear facilities. Ideally, the entire analysis is driven by the threats one wants to protect against. In many high-security applications, this threat level is determined by a federal entity (e.g., the Department of Energy or the Nuclear Regulatory Commission) and a designated security analyst then evaluates the effectiveness of the security system. Most high-security applications also employ an on-site guard force, usually armed and well trained, to respond to malevolent incidents. Managers of the majority of civilian infrastructures do not employ a dedicated response force and operate geographically distributed assets, the majority of which reside in the public realm.

Each major block of the methodology has multiple steps and/or requirements. For a complete description of RAM-W™, please contact the American Water Works Association for a copy (the requestor must demonstrate a need-to-know and must sign a nondisclosure agreement). AwwaRF subscribers may contact them directly.

Results

Sandia conducted several vulnerability assessments during the development and validation of RAM-W ™ and water utility owners/operators and consultants applied the methodology at several hundred additional locations. As a result, the water community gained a good understanding of the state of security at water utilities and identified challenges that may lie ahead. In a recent project, AwwaRF and Sandia teamed to collect information on the vulnerability assessments conducted by the large water utilities to better understand (1) how well the process worked, (2) remaining areas of concern, and (3) what further developmental efforts to pursue (AwwaRF 2004).

Defining the Threat to Water Utilities

Although encouraged to contact local law enforcement and other authorities, most water utilities found it difficult to obtain relevant threat data.

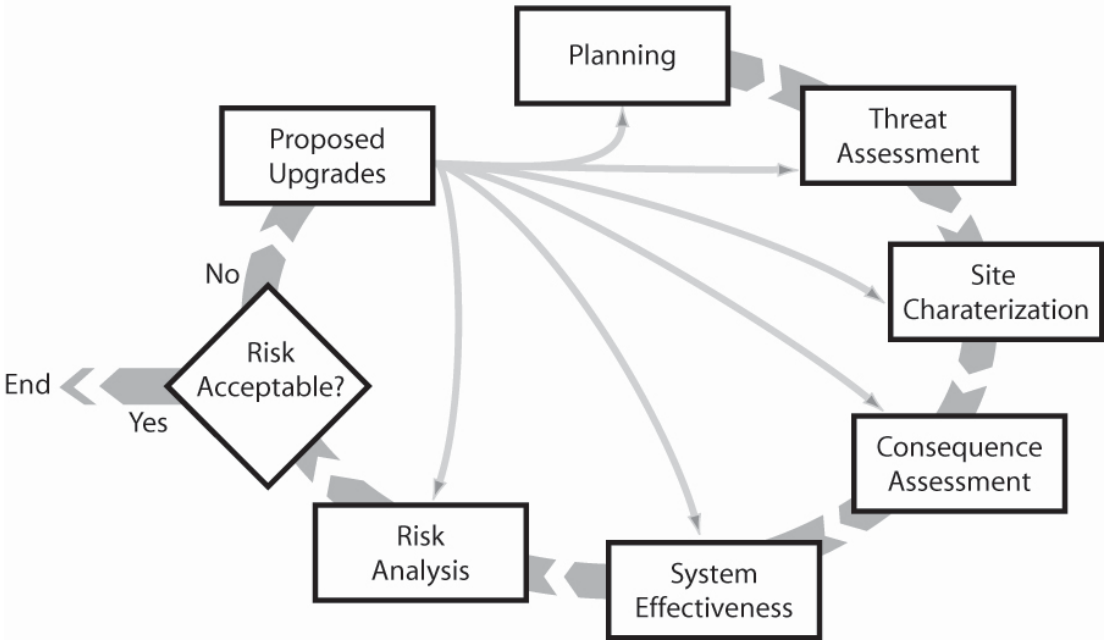

Figure 1. RAM-W™ Process

As stated earlier, the specified threat drives the risk analysis. Therefore, water utilities are faced with a high degree of ambiguity about what the actual threats are while having to undertake risk reduction programs that may cost millions of dollars. Even with the billions of dollars already being spent to improve the security of our nation's water utilities, it is questionable whether or not the utilities will be able to withstand a high-level threat. Much of the utilities' infrastructure resides in the public realm, is broadly distributed, and is very difficult to protect.

The Federal government has not defined a threat that can be used as the basis of a security design for the water infrastructure, nor is there agreement in the water community about what threats to consider. Therefore, the water utilities analyzed a multitude of threats and threat levels. Neighboring water utilities often used significantly different threat levels during their risk assessment. The number of adversaries and their projected capabilities will dramatically affect the outcome of the security risk analysis.

Contamination of Water Supplies

One of the least understood threats to the drinking water industry is contamination, particularly in the water distribution system. At the beginning of the program to assess the vulnerabilities of water utilities, very little was known about malevolent water contamination and even fewer analytical tools were available to help understand and analyze the problem. Since 9/11, several groups, including the AwwaRF, the EPA, and the Center for Disease Control, have collaborated to collect and characterize information on contaminants that may pose a significant health threat in drinking water systems. Prioritizing contaminants, developing methods to rapidly detect them, developing a full understanding of contaminant fate and transport, developing estimates for contamination risks to water distribution systems, creating programs for isolating and treating contaminants, and final restoration of clean water supplies are all in their early stages of development.

Sandia has launched an internal research program, with collaborators at EPA, to provide tools for answering many of these important contamination-related questions. This research program will develop numerical tools to probabilistically predict the fate and transport of a variety of potential contaminants and thus facilitate the development of contamination risk maps for water distribution systems. The research program will also help determine optimal sensor locations for detection of contaminants (assuming the appropriate sensors are developed) and develop analytical tools to quickly locate where contaminants were introduced.

Response to Threats

High-security environments often have an on-site response force to deal with malevolent threats. The vast majority of water utilities do not employ such a strategy. Instead, they rely on cooperation from local law enforcement, public health authorities, and other providers of emergency services. This is not an unusual situation within the community of critical infrastructures, but this approach leads to long response times, raising a concern about the level of security provided.

Immediately after 9/11, many metropolitan areas assigned police officers at water utility assets to deter adversaries. Due to budget constraints and a belief that the threat is not as imminent as previously believed, this practice has been largely discontinued.

Recommendations

Based on the experience of applying RAM-W™ to hundreds of water utilities, several improvements could enhance future risk assessments. These improvements include: a refined threat description, complete integration of the water distribution system contamination analysis with the risk assessment, and improved response protocols. Naturally, these recommendations will require resources and time to accomplish.

Because the threat level drives the risk assessment analysis and ultimately, the risk reduction recommendations, the area of threat assessment could be improved. A variety of approaches may be taken, such as the following:

1. Issue a mandatory threat level for all water utilities (minimum standard) to use as the basis for determining which risk reduction upgrades are appropriate
2. Use a graded approach to implementing upgrades based on population served or some other statistic, such as volume of water shipped

3. Water-community-developed threat scenarios that are graded by population
4. Threat levels based on regional or target attractiveness

Whatever threat definition system is chosen, consistency and minimally acceptable threat levels should be created to provide a balanced approach to countering the threat.

The water distribution system has long been known to represent one of the greatest security vulnerabilities. Current challenges include a lack of clear understanding of the fate and transport and consequences of potential contaminants within a water distribution system coupled with generally easy access into the system. To minimize the potential risks from a malevolent contamination attack, it is first necessary to develop computational tools that can predict the fate and transport of contaminants within distribution systems, or more generally, how contaminants might move in a hydraulically complex pipe network. This computational tool must be integrated within a systematic framework (as embodied in RAM-W™), so that a more comprehensive risk assessment can be accomplished. Such a tool (or set of tools) (1) would be capable of determining (in a probabilistic sense) the spread of contaminants within a distribution system, (2) could be used to estimate consequences from such an attack, (3) would be able to identify optimum locations for early-warning sensors, and (4) would be able to identify the source location (point of introduction) in near-real time. Determining the extent of contamination in a water distribution system in real time is essential so that proper actions can be taken to minimize the further spread of the contaminants.

Methodologies for conducting vulnerability assessments should include a framework for cleanup and recovery. The tools to estimate the fate and transport of contaminants within a water distribution system could also play a significant role in developing a methodology for recovery after such an event and could serve as the instrument to integrate both components for the protection of drinking water systems.

Better response protocols are needed in several areas. Response to water contamination events is entirely different than response to an armed attack where the intent is to damage the utility's physical assets. The current research underway to understand the fate and transport of contaminants will help decision makers understand the risk and to develop new response protocols that address that attack before the contamination event. Those protocols must include clean-up processes and placing the system back in service.

Responding to threats may require new approaches that greatly enhance the time an adversary needs to complete a malevolent act. Threats can be countered by storing high-consequence assets underground, limiting the paths an adversary might exploit and thereby creating long task times. For example, pumping stations could be protected better by installing them below grade in protected shelters.

In testimony to the United States House of Representatives Committee on Science entitled "H.R. 3178 and the Development of Anti-Terrorism Tools for Water Infrastructure," Jeffrey J. Danneels of Sandia suggested several alternatives that might provide the improved security desired at a much lower cost than the physical security approaches currently in use. Research dollars should be made available to study alternatives that put final treatment of the water supply closer to the consumer, consider much of the present potable water system as non-potable to decentralize the impact of a potential event, and evaluate the efficacy of creating municipal bottling facilities and other novel approaches that provide the level of security demanded by the water consumer and which may not be achievable through any other means.

Conclusions

Understanding and analyzing the vulnerabilities within the water infrastructure is a very important undertaking. Our government needs to protect one of the most basic assets America has—a clean water supply. Understanding and analyzing the vulnerabilities within the nation's water infrastructure will help us protect the health and safety of our citizens. The efforts completed to date have highlighted several vulnerabilities that will require significant amounts of effort to correct. Within the list of 14 U.S. critical infrastructures listed in HSPD-7, the water infrastructure is probably the most taken for granted. A large investment will be required to provide even minimal levels of security for this

important resource. "When is enough, enough?" will be a difficult question to answer and will be debated for years to come.

Acknowledgements

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy under Contract DE-AC04-94AL85000.

Author Bio and Contact Information

Jeffrey J. Danneels is a Department Manager within the Security Systems and Technology Center at Sandia National Laboratories. He manages critical infrastructure security programs and is responsible for the Risk Assessment Methodology for Water Utilities, RAM-W™. Shortly after the events of 9/11 he testified to Congress on two occasions. His first testimony concerned the security of the water infrastructure and in the second he outlined security research needs to better protect the water infrastructure. Mr. Danneels has provided security training to hundreds of students and led the development of a security course for water utility employees that has been attended by thousands. Mr. Danneels was the Program Director for the international *Innovative Technologies for Disaster Mitigation* conference held in Washington, DC in October of 1999. This three-day Architectural Surety® conference provided a forum for experts from around the world to exchange information on mitigating the consequences of natural and man-made disasters. He holds a BSCE from Michigan State University, a MSCE from Louisiana State University, and a Masters in Management from the University of New Mexico. Jeff has been with Sandia since 1985. Jeffrey J. Danneels, Sandia National Laboratories, PO Box 5800, Albuquerque, NM 87185, Phone: 505-284.3897, FAX: 505-284-8677, jsdanneels@sandia.gov

Ray Finley is the Manager of the Geohydrology Department at Sandia National Laboratories in Albuquerque, New Mexico. He has evaluated security aspects related to Sandia's critical infrastructure program since the mid-1990's. He participated in the development of methodology for evaluating the vulnerabilities of large federal dams, electrical transmission systems, and drinking water systems. In this role he has led and participated in numerous vulnerability assessments, training programs, applications of the methodologies, and vulnerability assessment reports. He continues to be actively engaged in assessing vulnerabilities of critical infrastructures, including physical disruption and contamination of water distribution systems.

References

Awwa Research Foundation. 2002. *Risk Assessment Methodology for Water Utilities (RAM-W™).* 2nd ed. Denver, Colorado: Awwa Research Foundation and Sandia National Laboratories.

Awwa Research Foundation. 2004. *Results from the Water Utility Vulnerability Assessment Lessons Learned Study.* Denver, Colorado: Awwa Research Foundation and Sandia National Laboratories.

Environmental Protection Agency. n.d. *FACTOIDS: Drinking Water and Ground Water Statistics for 2001*. Available at http://www.ngwa.org/pdf/01factoids.pdf.