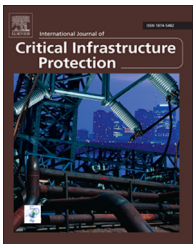
Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.elsevier.com/locate/ijcip



Securing wastewater facilities from accidental and intentional harm: A cost-benefit analysis

Stephen Papa[a,b], *William Casper*[a,b], *Tyler Moore*[a,*]

[a]*Computer Science and Engineering Department, Bobby Lyle School of Engineering, Southern Methodist University, P.O. Box 750122, Dallas, TX 75275, USA*

[b]*Lockheed Martin Aeronautics, 1 Lockheed Boulevard, Fort Worth, TX 76101, USA*

ARTICLE INFO

Article history:
Received 14 January 2013
Accepted 29 April 2013
Available online 4 May 2013

Keywords:
Industrial control system security
Wastewater facilities
Security economics
Cost-benefit analysis

ABSTRACT

It has been widely reported that industrial control systems underpinning critical infrastructures ranging from power plants to oil refineries are vulnerable to cyber attacks. A slew of countermeasures have been proposed to secure these systems, but their adoption has been disappointingly slow according to many experts. Operators have been reluctant to spend large sums of money to protect against threats that have only rarely materialized as attacks. But many security countermeasures are dual-use, in that they help protect against service failures caused by hackers and by accidents. In many critical infrastructure sectors, accidents caused by equipment failures and nature occur regularly, and investments for detecting and possibly preventing accidents and attacks could be more easily justified than investments for detecting and preventing attacks alone. This paper presents a cost-benefit analysis for adopting security countermeasures that reduce the incidence of sewer overflows in wastewater facilities. The paper estimates the expected annual losses at wastewater facilities due to large overflows exceeding 10,000 gallons using publicly-available data on overflows, cleanup costs, property damage and regulatory fines. Also, it estimates the costs of adopting security countermeasures in wastewater facilities in eight large U.S. cities. The results of the analysis indicate that, in many cases, even a modest 20% reduction in large overflows can render the adoption of countermeasures cost-effective.

1. Introduction

Supervisory control and data acquisition (SCADA) systems and industrial control systems (ICSs) are widely used to control systems such as water supply systems, wastewater collection and treatment facilities, refineries, oil and gas pipelines, factories, ships and subways. These systems have evolved from direct human control to computer-based control over the last several decades. Once computer-based control became common practice, a migration from proprietary to standards-based systems, protocols and interfaces occurred. Today, many systems have adopted standard wireline and RF physical interfaces, and the TCP/IP protocol is commonly used to move command and status messages within these systems. To ease management, the trend has been to connect these control networks to company intranets, which are normally connected to the Internet.

Unfortunately, SCADA systems and ICSs were not designed to defend against even the simplest network attacks. Operational commands, controller software updates, and operational status messages are not authenticated [32]. As a result, these systems are vulnerable to command

*Corresponding author.
E-mail address: tylerm@smu.edu (T. Moore).

1874-5482/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ijcip.2013.05.002

injection [9] and middle-person attacks [18]. A programmable logic controller (PLC) attack was at the heart of the Stuxnet virus that targeted Iranian uranium hexafluoride centrifuges [15]. Effectively, Stuxnet used a middle-person attack to change the PLC logic to report normal centrifuge operations to plant operators while issuing control commands that damaged the centrifuges.

Research efforts focused on control systems security typically take for granted that an attack will occur and instead focus on adopting security countermeasures to thwart attacks. However, attacks have been so rare in practice that asset owners and operators are reluctant to invest in adequate defenses. This paper studies one particular critical infrastructure sector – wastewater collection and treatment systems – and investigates whether the expense of security countermeasures can be justified, provided that they can also be used to prevent accidents as well as attacks. The wastewater sector is selected precisely because the intended effect of a cyber attack is the same as a relatively common failure mode – a sewer overflow. Furthermore, systems for detecting malicious overflows in wastewater systems can also detect accidental ones.

The next section, Section 2, outlines the threat model for wastewater facilities and explains how security countermeasures can be deployed in a representative system to detect and prevent sewer overflows. Section 3 presents a framework for calculating the expected costs of large sewer overflows. Detailed public data from the California Water Board is used to estimate the incidence of large sewer overflows. Reports of legal settlements are collated to estimate the cost of property damage, and EPA data on Clean Water Act violations are examined to estimate the cost of regulatory fines as well as the probability of drawing the ire of regulators. Also, an estimate for the cost of comprehensive security countermeasures is provided. Section 4 presents a cost-benefit analysis based on the findings discussed in Section 3. The net expected utility is assessed by comparing the costs with the benefits of experiencing fewer overflows. Because wastewater facilities vary greatly in complexity, a detailed analysis is provided for facilities in eight U.S. cities, with the results demonstrating that some cities are likely to view the costs as acceptable whereas other cities will not. Section 5 reviews related work in the field and Section 6 discusses key limitations of the analysis and outlines opportunities for future research.

2. System model

This section describes the threat model for wastewater facilities considered in this paper. It explains the countermeasures that have been proposed and how a representative wastewater facility may be secured using the available countermeasures.

2.1. *Threat model*

The threat model includes all sewage system overflow failures occurring at wastewater facilities, regardless of intent. The wide range of common failures includes electrical equipment failures (sensors, pumps and control electronics), blockages and structural failures. However, an overflow can also be triggered by an actor with malicious intent. The primary methods of attack on industrial control systems include command injection, service-denial and middle-person attacks [9,18,32]. Regardless of whether the attacker's motivation is wealth, fame, notoriety or terror, invariably the aim of an attack is to disrupt system operations. In this paper, we do not differentiate sanitary sewer overflows (SSOs) from combined sewer overflows (CSOs) that may be caused by accidents or attacks. A CSO involves a single collection system for both stormwater and sanitary wastewater, and an SSO involves only wastewater, but we refer to both as sewer overflows (SOs). Note that overflows typically cannot be prevented even if they detected, notably the overflows caused by excessive storm water inflow.

In the case of wastewater facilities, the most likely and disruptive method of attack is to trigger a sewer system overflow. A famous attack on a wastewater collection system is the Maroochy Water Service Breach [1]. In this attack, a SCADA system installer injected commands to a lift station, triggering millions of liters of SOs on at least 46 separate occasions. While the incidents persisted for nearly two months, we view it as a single, sustained attack rather than 46 separate attacks because it was carried out by the same perpetrator. The person responsible, Vitek Boten, was sentenced to two years in prison and was levied fines to help cover the cleanup costs; his motive was to obtain a consulting job with the utility to stop the SO incidents.

In general, the PLCs that control lift station pumps are the most logical targets for causing overflows. Attack methods include turning off one or more pumps, under pumping, or repeatedly cycling power to the pumps in order to cause motor damage and malfunctions. These attacks can be executed by modifying the PLC control logic, by injecting malicious control commands, or by modifying operator commands. PLCs are vulnerable to attack because they often have no mechanisms for authenticating commands.

2.2. *Countermeasures to prevent sewage overflows*

Two complementary types of countermeasures have been proposed to protect against attacks on control systems. The more proactive approach is to improve the integrity of control elements such as PLCs and RTUs in a SCADA system and the communications channels they rely on to transmit messages. For example, researchers have proposed retrofitting communications channels with devices to encrypt communications at the link level [14,25,33]. Alternatively, integrity can be achieved at the system level by deploying new sensors and PLCs that incorporate trusted hardware (e.g., trust anchors [17]). While the approach offers a high level of protection against attacks, adding systems such as trust anchors are expensive and do not, on their own, aid in detecting system failures or attacks.

A second class of countermeasures is much more reactive. Instead of preventing attacks by improving system and communications integrity, attacks and failures can be detected by monitoring systems for aberrant behavior. Several researchers have proposed intrusion detection