PHYS ORG

Sandia's CANARY software protects water utilities from terrorist attacks and contaminants

July 25 2011

Americans are used to drinking from the kitchen tap without fear of harm, even though water utilities might be vulnerable to terrorist attacks or natural contaminants.

Now, thanks to CANARY Event Detection Software — an open-source software developed by Sandia National Laboratories in partnership with the Environmental Protection Agency (EPA) — public water systems can be protected through enhanced detection of such threats.

"People are excited about it because it's free and because we've shown that it works really well. We would love to have more utilities using it," said Regan Murray, acting associate division director of the EPA's Water Infrastructure Protection Division at the National Homeland Security Research Center.

The software tells utility operators within minutes whether something is wrong with their water, giving them time to warn and protect the public. And it's improving water quality by giving utility managers more comprehensive real-time data about changes in their water.

CANARY is being used in Cincinnati and Singapore, and Philadelphia is testing the software system. A number of other U.S. utilities also are evaluating CANARY for future use.

Sean McKenna, the Sandia researcher who led the team that developed CANARY, said people began to pay attention to the security of the nation's water systems after 9/11.

McKenna and Murray said CANARY could have lessened the impact of the nation's largest public water contamination. In 1993, a cryptosporidiosis outbreak in Milwaukee hastened the deaths of dozens of citizens, made more than 400,000 residents ill and cost more than $96 million in medical expenses and lost productivity, according to reports about the tragedy.

"If you don't have a detection system, the way you find out about these things is when people get sick," Murray said.

Sandia, a national security laboratory, had worked on water security before the 9/11 attacks. So when the EPA was looking for help early in the last decade to better monitor water utilities, they contacted Sandia.

A Sandia-developed, risk-assessment methodology for water focused on physical security of the utility infrastructure, but did not address detection and assessment of the impact of contamination within the water itself. CANARY was designed to meet that need for better assessment, McKenna said.

CANARY, which runs on a desktop computer, can be customized for individual water utilities, working with existing sensors and software, McKenna said.

While some utilities monitor their water using real-time sensors, many still send operators out once a week to take samples, said David Hart, the lead Sandia software developer for CANARY.

Compared to weekly samples, CANARY works at lightning speed.

"From the start of an event — when a contaminant reaches the first sensor — to an event alarm would be 20-40 minutes, depending on how the utility has CANARY configured," McKenna said.

The challenge for any contamination detection system is reducing the number of false alarms and making data meaningful amidst a "noisy" background of information caused by the environment and the utility infrastructure itself.

CANARY researchers used specially designed numerical algorithms to analyze data coming from multiple sensors and differentiate between natural variability and unusual patterns that indicate a problem. For example, the Multivariate-Nearest Neighbor algorithm groups data into clusters based on time and distance, explained Kate Klise, a numerical analyst at Sandia. When new data is received, CANARY decides whether it's close enough to a known cluster to be considered normal or whether it's far enough away to be deemed anomalous. In the latter case, CANARY alerts the utility operator, Klise said.

The computer program uses a moving 1.5- to two-day window of past data to detect abnormal events by comparing predicted water characteristics with current observations. But a single outlier won't trigger the alarm, which helps to avoid costly and inefficient false alarms. CANARY aggregates information over multiple 2- to 5-minute time steps to build evidence that water quality has undergone a significant change, McKenna said.

"We've taken techniques from different fields and put those together in a way they haven't been put together before; certainly the application of those techniques to water quality monitoring hasn't been done before," McKenna said.

CANARY also provides information about gradual changes in the water, McKenna said.

One unintended benefit of the software is that when utility operators better understood the data being sent by their sensors, they could make changes to the management of the water systems to improve its overall quality, McKenna said.

"What we found from utilities we work with is that a better managed system is more secure, and a more secure system is better managed," McKenna said.

Harry Seah, director of the Technology and Water Quality Office at the Public Utilities Board (PUB), Singapore's national water authority, wrote in a letter supporting CANARY that the software provided a "quantum leap" in the utility's practice.

In the past, Seah wrote, the utility depended on preset limits of three water characteristics to determine water quality.

"With the implementation of CANARY, relative changes in the patterns of these three parameters can be used to uncover water quality events, even if each individual parameter lies within the alarm limits," Seah wrote. "This dramatically improves PUB's ability to respond to water quality changes, and allows PUB to arrest poor quality water before [it reaches] the consumers."

As more versions of the software are installed at water utilities, researchers are working on new application areas for CANARY, such as computer network traffic logs and geophysical log analysis used by petroleum drillers to analyze rocks at different depths.

Provided by Sandia National Laboratories

Citation: Sandia's CANARY software protects water utilities from terrorist attacks and contaminants (2011, July 25) retrieved 19 April 2024 from https://phys.org/news/2011-07-sandia-canary-software-terrorist-contaminants.html