WADI: A Water Distribution Testbed for Research in the Design of Secure Cyber Physical Systems

Chuadhary Mujeeb, Palleti Venkata Reddy, and Aditya Mathur

iTrust
Center for Research in Cyber Security
Singapore University of Technology and Design
Singapore

CYSWATER 2017: Pittsburgh

April 21, 2017
Testbeds

Water Treatment

Water Distribution

Electric power generation, transmission, distribution, AMI
WDN Security

- Distributed Systems Controlled via PLCs
- Automation - blessing or a curse
- Maroochy Shire Australia (2000) *
  - Hacked by a disgruntled employee
  - 1 Million litres of waste water spillage
- ICS-CERT reported attacks on water utilities in USA**


Contributions

(a) Description of an operational WAter Distribution (WADI) testbed.

(b) Attack scenarios and an attacker model is proposed.

(c) Results from experiments conducted using WADI.
Pictorial view of WADI

Primary Grid

Elevated Reservoir

Six Consumer Tanks

Return Water Tank (out of photo)
Figure 2: Three stages in WADI are shown. Solid arrows indicate flow of water and sequence of processes. S and A represent, respectively, sets of sensors and actuators. 1-LT-001: level sensor in stage 1 and tank 1; 1-FS-001: flow meter 1 in stage 1; 1-T-001: Tank 1 in stage 1; 2-MV-001: motorized valve 1 in stage 2; 2-MCV-101: motorized consumer valve 1 in stage 2; and 3-P-004: water pump 4 at stage 3.
Leak Detection

- Simulated by transparent double containment piping section with a modulating valve that opens into the outer pipe to simulate a leak.

- The leakage valve will be slowly opened and detected by downstream and upstream pressure transmitters downstream using pressure difference.

- A modulating drain valve can be completely open to simulate a broken/burst pipe. The difference in downstream and upstream pressures will be feed backed via the respective pressure transmitters.
Pipe Leakage Simulation

Normal Operation:
1. 2-MCV-009 is closed
2. 2-PIT-002 == 0.1 bar
3. 2-MV-008 is closed

Leakage Simulation:
1. 2-MV-008 is opened
2. 2-MCV-007 is opened
3. 2-PIT-002 < 0.1 bar
Pipe Leakage Simulation

Normal condition:
(i) 2-MCV-009 is closed. Water flow via gravity to inline booster station or direct to primary grid.
(ii) 2-DPIT-001 will show a reading of 0.1 bar (Line pressure vs pressure in outer containment pipe)
(iii) 2-MV-008 is closed

Pipe leakage condition:
(i) 2-MV-008 is opened
(ii) 2-MCV-007 is opened (Gradually percentage increase in opening).
Water is diverted to double containment pipe.
(iii) 2-DPIT-002 will feedback a decreased in reading to less than 0.1 bar (Line upstream pressure vs Line downstream pressure)
(iv) Alarm Triggered

(v) To restore back to normal condition (To be done manually)
a. Close 2-MCV-007
b. Close 2-MV-008
Contamination Dosing

WADI caters for the possibility of dosing an organic or inorganic contaminant.

1) Each dosing system is made up of a tank and a dosing pump

2) The dosing points are located after the water quality analysers at the outlet of the service reservoir.

3) A set of water quality analysers (pH, ORP, Conductivity and turbidity) are installed downstream of the dosing points to detect the differences in water quality parameters.

4) Simulation will require to be on manual mode and the contaminated water might have to divert to a chemical disposal tank if necessary (not fit for direct discharge to Sewers)
Contamination Dosing

GRAVITY FEED & CONTAMINANT DETECTION SKID

COND TURB pH ORP
2A AE 001/002/003/004

Organic/Inorganic Contamination

2" Static Mixer

2-MV-005

To Gravity Flow Drawing P2B
Communication Infrastructure

Layer 2

SCADA, HMI, Engineering Workstation, Historian, etc.

NIP/SP  GPRS modem

Layer 1

P1
PLC: Water Supply Control Logic
Sensors Actuators

P2A
RTU: Sampling Station
Sensors

P2
PLC: Primary Grid, Consumers Control Logic
Sensors Actuators

P2B
RTU: Sampling Station
Sensors

P3
PLC: Return Water Control Logic
Sensors Actuators

Modbus RS485
Figure 1: Network Architecture
Attacker and Attack Models

- Attacker model includes attacker intentions and the targeted components.*

- Example: Intent: “cut off water supply to the consumer tanks.”

- The attacker has access to the SCADA system

Level (LIT 001) sensor attack
Conductivity meter (AIT 001) attack

![Diagram showing the conductivity of water over time with a sharp drop at the launch of attack.](image-url)
Future Work

Attack design: Multi point and multi stage

Implementation and assessment of WaterDefense

Leak detection under multi point deception attacks

Contaminant detection under multi point deception attacks

EPANET model to be tuned to WADI.