Industrial Cybersecurity: Opportunities and challenges in Digital Transformation

KASPERSKY
RICCARDO TAORMINA
SUTD
Singapore

- Postdoc at the iTrust, SUTD
- Contributed in epanetCPA, a cyber-physical attack simulator on water distribution networks
- Organized the BATADAL, an international data-science competition for attack detection algorithms

linkedin.com/in/richtao
Characterization, Simulation and Detection of Cyber-Physical Attacks on Water Distribution Systems

Riccardo Taormina and Stefano Galelli
Contents

• Part I: Urban Water Infrastructures

• Part II: Cyber-Physical Security of Water Distribution Systems

• Part III: Testbeds @ iTrust

• Part IV: Conclusions
Part I: Urban Water Infrastructures
Urban Water Infrastructures

- Modern water infrastructures are cyber-physical systems.

- Cyber-layer depends on the type of underlying processes.

- Digital, interconnected ICS/SCADA replacing analog systems, air-gapped from corporate networks and internet.

- Higher efficiency, better service, cost-savings, real-time capabilities, …

- Vast attack surface: 3rd most targeted sector after manufacturing and energy*.

Review of attacks on Water Utilities

- 2000: Maroochy Water Services (AUS) Wastewater Treatment Facility
- 2006: Pennsylvania Water Company (PA) Water Filtering Plant
- 2007: Bowman Avenue Dam (NY) Reservoir Dam
- 2012: Key Largo Water (FL) Wastewater Treatment Facility
- 2013: ‘Kemuri’ Water Company (SJ) Water Distribution System
- 2015: Undisclosed (US) Water Distribution System
- 2016: Multiple utilities (Eastern US) Water Distribution System
- 2017: Undisclosed (US) Regional Water Supplier
- 2018: Undisclosed (US) Regional Water Supplier

Source: ASCE/EWRI Cyber-physical Security of WDS Task Committee
Review of attacks on Water Utilities

- At least 10 reported and confirmed attacks since 2000
- Targeted and untargeted attacks on very different infrastructures.
- Adversaries: outsiders, hacktivists, insiders, or third-party’s insiders.
- Other suspicious incidents reported:
  - 2005, Taum Sauk Dam, St. Louis, MO
  - 2011, Pump Station, IL
  - 2011, Water Treatment Plant, Houston, TX
- Many unreported attacks: over 90% of attacks reported in the US, lack of data elsewhere.

Source: ASCE/EWRI Cyber-physical Security of WDS Task Committee
Review of attacks on Water Utilities

**Goals**
- Cause damage
- Seize resources for other purposes
- Terrorism
- Ransom
- Revenge
- Steal money
- Data breach
- Practice
- Others, unknown

**Means**
- Unauthorized access
- Exploitation of software vulnerabilities
- Malware, Viruses, Trojans, Worms, ...
- Ransomware
- Social engineering
- Insider information

**Vulnerabilities**
- Poor separation of ICS/SCADA and corporate networks
- Lack of awareness
- Lack of IT/OT security teams
- Outdated software, hardware, firmware
- Poor attention to security guidelines

Source: ASCE/EWRI Cyber-physical Security of WDS Task Committee
Part II: CPS of Water Distribution Systems
Water Distribution Systems (WDS)
WDS are cyber-physical systems
Attacker model for WDS

ATK: PHYSICAL LAYER
ATK: LINK PHYSICAL/PLC
ATK: LINK PLC/SCADA
ATK: DIRECT ATTACK PLC
ATK: DIRECT ATTACK SCADA

Estimating the impacts of attacks on WDS

- Utilities are not keen to share data on attacks.
- It is hard to estimate the risk associated to attacks on WDS.
- Computer simulations can help estimate the impacts.

Based on EPANET
Implemented in MATLAB
Open source (MIT)
https://github.com/rttaormina/epanetCPA

---
epanetCPA: results

- Used to study attacks causing:
  - tank overflows,
  - low pressure conditions,
  - unmet demands,
  - total cutoffs of supply.
- Entity of impact depends on initial conditions.
- The tool can be used to assess district vulnerability.
- Existence of “windows of opportunity” for attack response.
- Usefulness of synthetic data generation.

ABOUT BATADAL

© 9 September 2016

The BATtle of the Attack Detection ALgorithms (BATADAL) will objectively compare the performance of algorithms for the detection of cyber attacks in water distribution systems. Participants will contribute an attack detection algorithm for a given water network following a set of rules that determine the exact goal of the algorithms.

MOTIVATION

Modern Water Distribution Systems rely on computers, sensors and actuators for both monitoring and operational purposes. This combination of physical processes and embedded systems (cyber-physical systems, in short) improves the level of service of water distribution networks but exposes them to the potential threats of cyber attacks. During the past decade, several water supply and distribution systems have been attacked, with the consequent creation of cybersecurity agencies and international partnerships to defend water networks. Yet, little is known about the potential effect of these attacks as well as the design and implementation of attack detection algorithms which identify anomalous behaviors of sensors, pumps and other components of water networks.
## BATADAL: results

<table>
<thead>
<tr>
<th>PLACE</th>
<th>TEAM</th>
<th>ATTACKS DETECTED</th>
<th>SCORE</th>
<th>ALGORITHM DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Housh and Ohar</td>
<td>7 out of 7</td>
<td>0.970</td>
<td>Process-based approach</td>
</tr>
<tr>
<td>2</td>
<td>Abokifa et al.</td>
<td>7 out of 7</td>
<td>0.949</td>
<td>PCA + ANNs</td>
</tr>
<tr>
<td>3</td>
<td>Giacomoni et al.</td>
<td>7 out of 7</td>
<td>0.927</td>
<td>PCA + Classifier</td>
</tr>
<tr>
<td>4</td>
<td>Brentan et al.</td>
<td>6 out of 7</td>
<td>0.894</td>
<td>Recurrent neural networks</td>
</tr>
<tr>
<td>5</td>
<td>Chandy et al.</td>
<td>7 out of 7</td>
<td>0.802</td>
<td>Variational Autoencoders</td>
</tr>
<tr>
<td>6</td>
<td>Pasha et al.</td>
<td>7 out of 7</td>
<td>0.773</td>
<td>Multiple approaches</td>
</tr>
<tr>
<td>7</td>
<td>Aghashahi et al.</td>
<td>3 out of 7</td>
<td>0.534</td>
<td>Feature extraction + classifier</td>
</tr>
</tbody>
</table>

Attack detection with Autoencoders (AE)

- Symmetric hourglass-shaped architecture made of an encoder and a decoder.
- The network is trained with the aim of replicating the inputs.
- AE learn a compressed representation of the input data.
- OUTPUTS = INPUTS → AE are self-supervised learning models (no labels).
- Reconstruction error ~ difference between input and its reconstruction.
Attack detection with Autoencoders (AE)

Normal operations data (SCADA historian)

Training

Validation

Real-time data from SCADA

PDF of reconstruction errors
Results on BATADAL dataset

- AE: 5 hidden layers, cf = 2.0, Q99.6
- Observed status
- Detected status

UNDER ATTACK

NORMAL STATUS

04-01  12-01  21-01  30-01  07-02  16-02  25-02  05-03  14-03  23-03  01-04

XGBoost

lightGBM
Attack localization
Part III: Testbeds
WATER DISTRIBUTION (WADI) TESTBED

SCADA
3 PLCs
HMI
5 Storage Tanks
6 Demand Nodes
Pumps, Valves
Chemical dosing systems
Analysers
Leak Simulator, ...
Secure Water Treatment (SWaT) Testbed
Testbeds at iTTrust

Four testbeds at iTTrust, SUTD
- WADI, water distribution
- SWaT, water treatment
- EPIC, power grid
- IoT, internet of things

Datasets with and without attacks available for download.

Used to carry out workshops and hacking competitions (attack and defense) for academia and industry.

Testbeds soon available for paid usage by external parties.
Part IV: Conclusions
Conclusions

- Modern water infrastructures are cyber-physical systems.
- Cyber-layer offers many benefits but lends an attack surface.
- Water sector is the third most targeted critical infrastructure.
- Major vulnerabilities include poor separation of ICS/SCADA from corporate network, lack of awareness and training.
- Guidelines are available but implementation is voluntary.
- We need to better report, study and characterize these attacks.
Conclusions

- Water Distribution Systems are heavily targeted infrastructures.
- Ongoing research to characterize and detect attacks on WDS.
- Simulations can be used to compensate for lack of real data.
- Testbed experiments can provide further insights, generate datasets, and improve the realism of simulations.
- Major advancements will require collaboration with utilities.
Thanks!

Riccardo Taormina
riccardo_taormina@sutd.edu.sg

iTrust@SUTD
https://itrust.sutd.edu.sg/
Related publications


