THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

A Laboratory-Scale Spillway SCADA System Testbed for Cybersecurity Research

Presenter: Mohammad E. Alim

mohammad.alim@uah.edu

Authors: M. E. Alim, Shelton Wright, Tommy Morris

Introduction

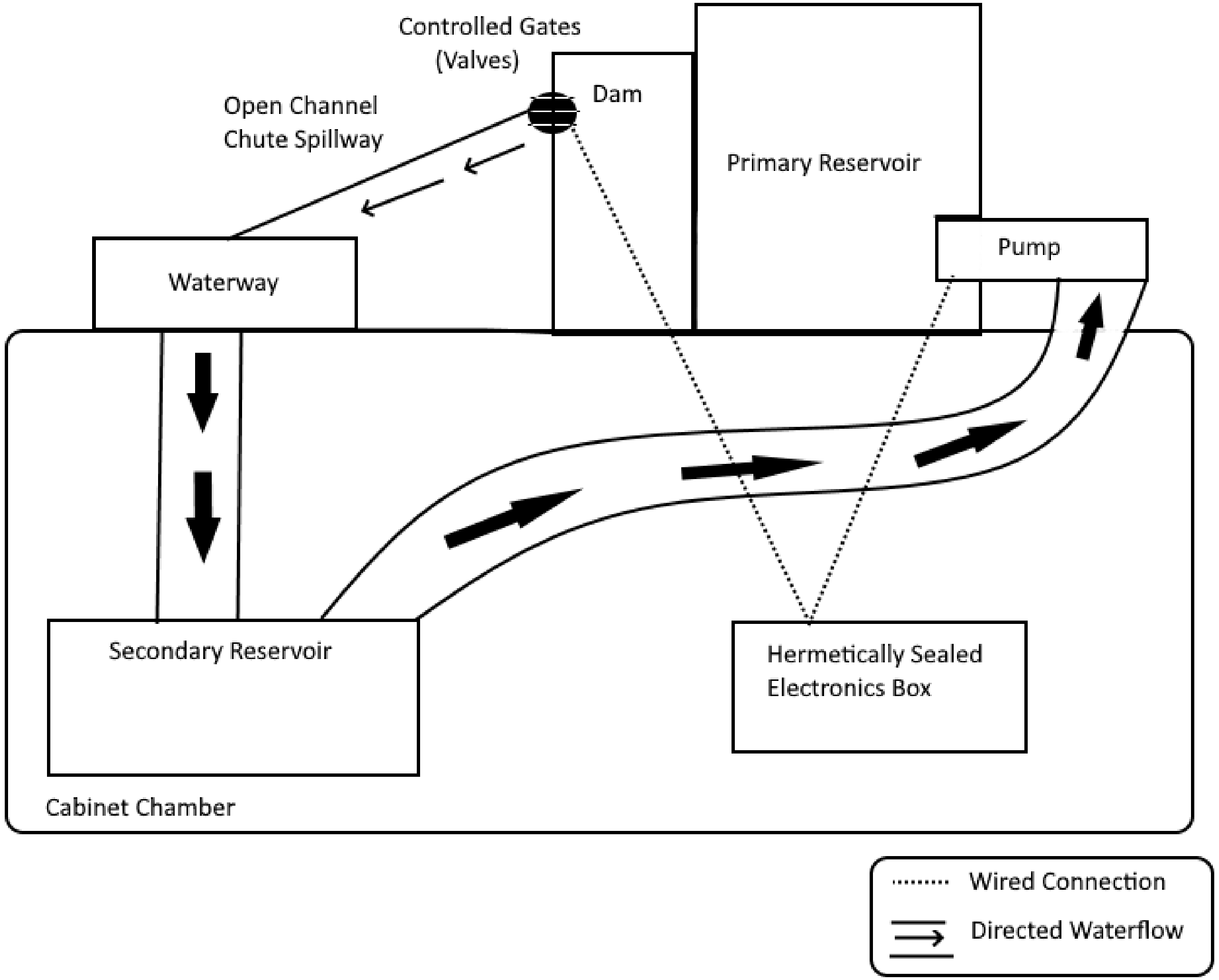
- Supervisory Control and Data Acquisition (SCADA) systems control and monitor critical infrastructures and similar legacy systems
- A malfunctioning SCADA system, caused by either equipment failure or by a malicious agent’s successful cyber attack, creates many disastrous consequences for the surrounding populace
- Cybersecurity professionals need tools to test developed mechanisms intended for securing critical SCADA systems

Motivation

- Testbeds simulate real-world models and provide insight aligned with the research interests in academia and industry
- Alternatively, testbeds may provide a potential source of dataset generation for intrusion detection/prevention systems and related cybersecurity development
- A reproducible physical testbed for a SCADA system found in critical infrastructure would benefit both students and researchers in SCADA-related fields

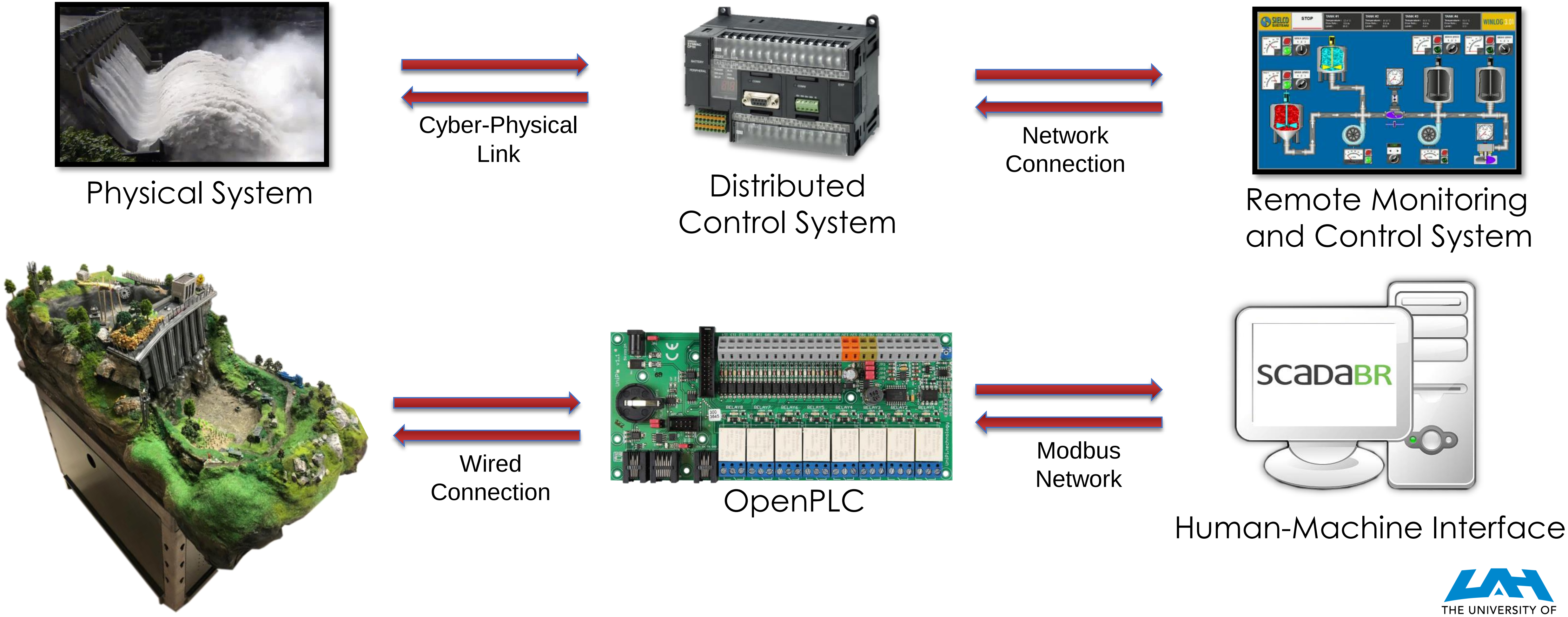
- **Objective**: to describe, design, and implement a reproducible physical testbed that features open-source software and functioning physical processes to model contemporary control systems found in a spillway system for a hydroelectric dam

Methodology – Spillway Modeling



- Generic dam model, typical chute spillways, conventional means to convey sequestered water
- Primary and secondary reservoirs in closed-loop pumped-storage hydropower scenario
- Pump mechanism to fill primary reservoir to a setpoint water level
- Controlled gates to control or stage waterflow

Methodology - 5 Components of SCADA



Physical System

Cyber-Physical Link

Distributed Control System

Network Connection

Remote Monitoring and Control System

Wired Connection

OpenPLC

Modbus Network

Human-Machine Interface

Physical Spillway Testbed

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Methodology

- 5 Components of a SCADA system

Component in a SCADA system	Component in Testbed System
Physical System	Sensors: Reservoir water level sensor, water flow sensors; Actuators: solenoid valves, piezoelectric buzzer alarm, RGB LEDs
Cyber-Physical Link	Electrical wires to transport voltage/current signals to PLC
Distributed Control System	Devices: Raspberry Pi running OpenPLC, UniPi with relays, Arduino Uno and Mega processing signals; Operation: Automatic and Manual modes to pump water and control gates implemented in ladder logic
SCADA Network Connection	Modbus TCP/IP protocol
Remote Monitoring and Control System	ScadaBR on Apache Tomcat webserver

Results

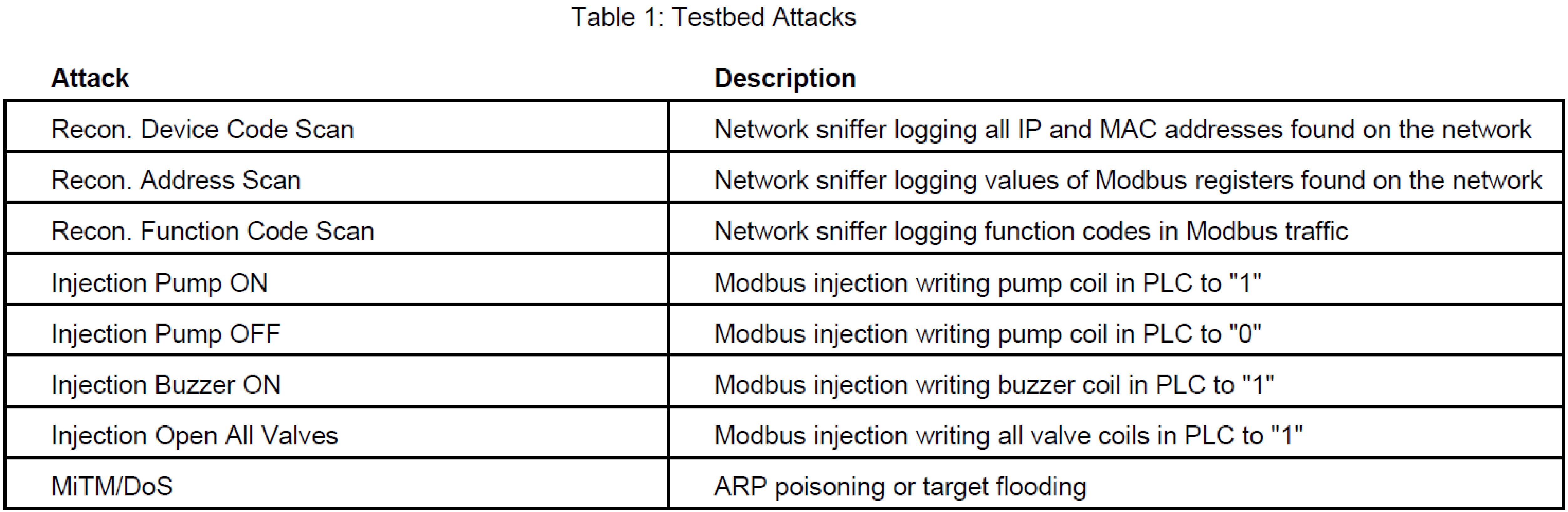
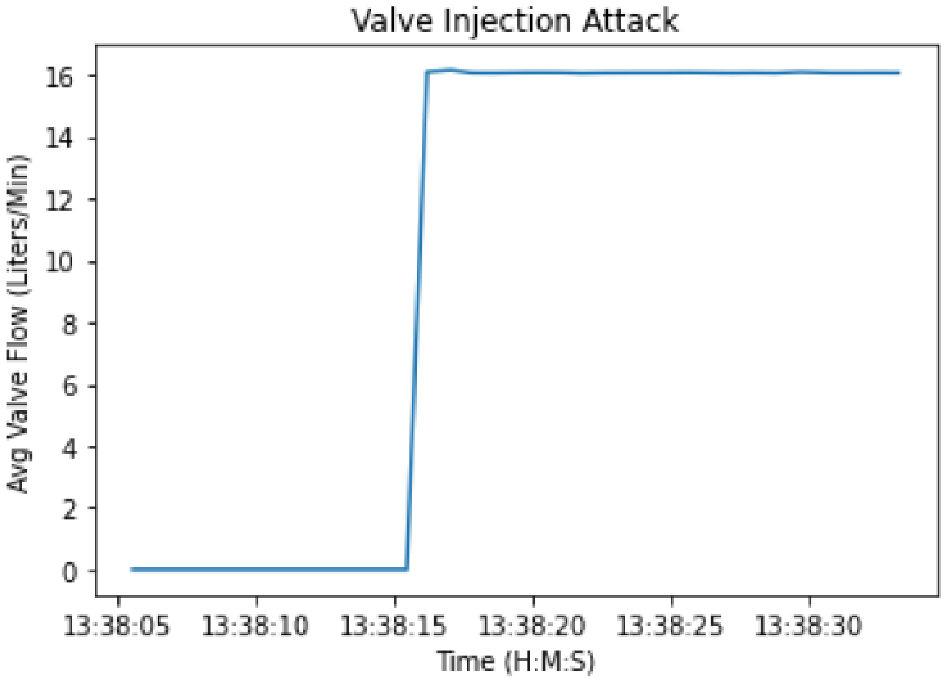


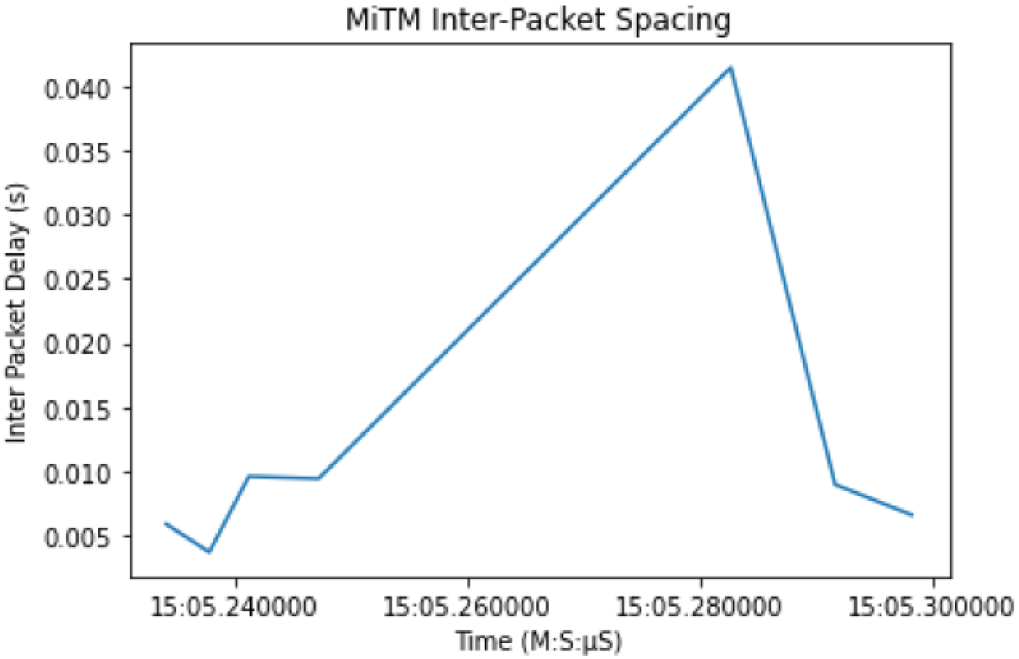
Table 1: Testbed Attacks

Attack	Description
Recon. Device Code Scan	Network sniffer logging all IP and MAC addresses found on the network
Recon. Address Scan	Network sniffer logging values of Modbus registers found on the network
Recon. Function Code Scan	Network sniffer logging function codes in Modbus traffic
Injection Pump ON	Modbus injection writing pump coil in PLC to "1"
Injection Pump OFF	Modbus injection writing pump coil in PLC to "0"
Injection Buzzer ON	Modbus injection writing buzzer coil in PLC to "1"
Injection Open All Valves	Modbus injection writing all valve coils in PLC to "1"
MiTM/DoS	ARP poisoning or target flooding

Results



(a) Injection Open All Valves: Valve Flow



(b) Man-in-the-Middle: Inter-Packet Spacing

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

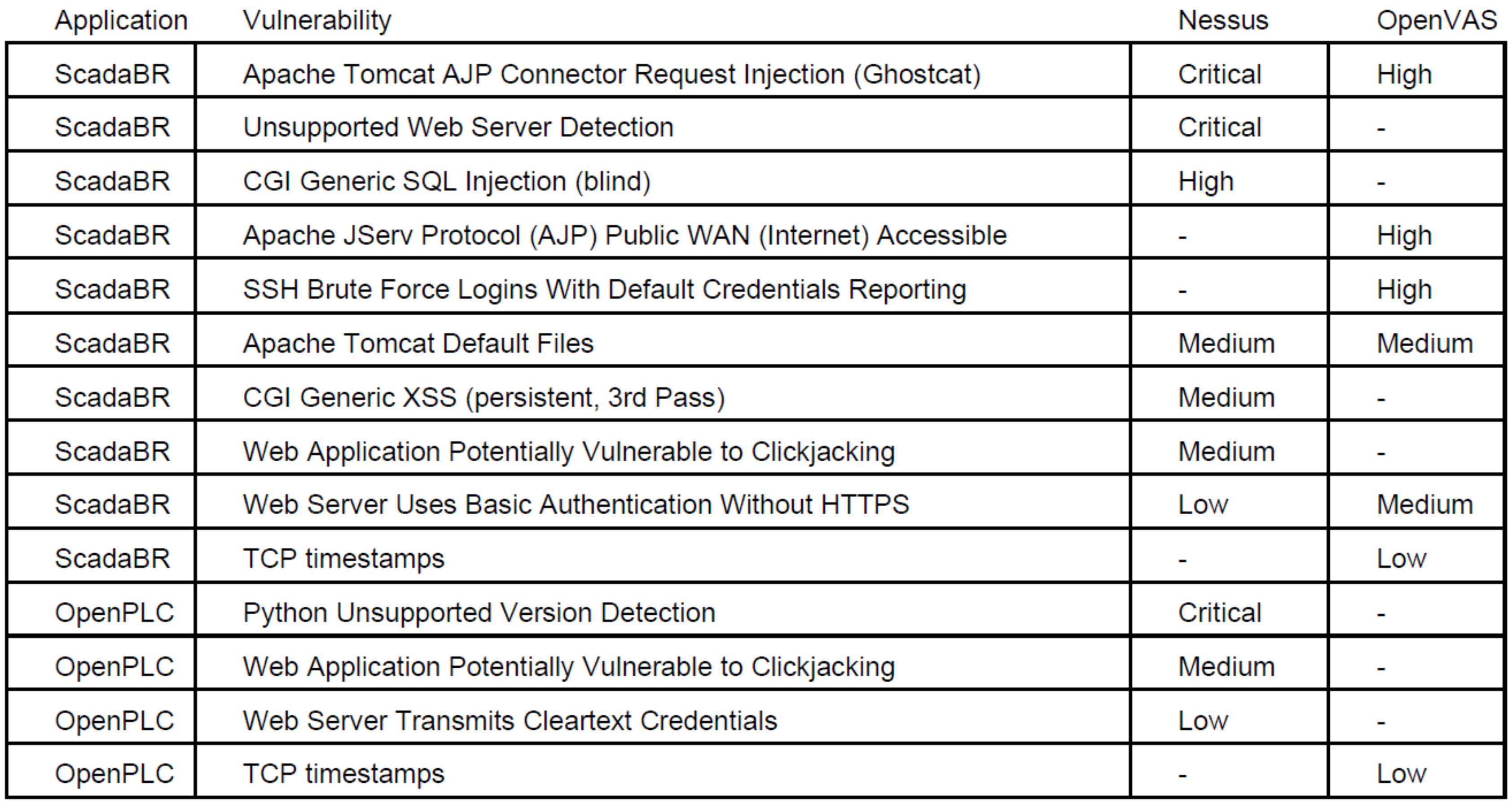
CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION

Results

- Data logs (Modbus Traffic + Network Traffic) record meaningful metrics and information for use in ML applications, e.g.
  - Packet size, timestamps of transmission, protocol overhead
  - Inter-packet arrival time, packet process time
  - Throughput, client network flow
- Dataset generation provides a tool to train/test IDS + IPS applications
- Next steps in a future work
  - Training profilers
  - Extendable datalogger intended for adding/removing meaningful parameters of interest

Results

Table 2: Vulnerability Scan Results



Application	Vulnerability	Nessus	OpenVAS
ScadaBR	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Critical	High
ScadaBR	Unsupported Web Server Detection	Critical	-
ScadaBR	CGI Generic SQL Injection (blind)	High	-
ScadaBR	Apache JServ Protocol (AJP) Public WAN (Internet) Accessible	-	High
ScadaBR	SSH Brute Force Logins With Default Credentials Reporting	-	High
ScadaBR	Apache Tomcat Default Files	Medium	Medium
ScadaBR	CGI Generic XSS (persistent, 3rd Pass)	Medium	-
ScadaBR	Web Application Potentially Vulnerable to Clickjacking	Medium	-
ScadaBR	Web Server Uses Basic Authentication Without HTTPS	Low	Medium
ScadaBR	TCP timestamps	-	Low
OpenPLC	Python Unsupported Version Detection	Critical	-
OpenPLC	Web Application Potentially Vulnerable to Clickjacking	Medium	-
OpenPLC	Web Server Transmits Cleartext Credentials	Low	-
OpenPLC	TCP timestamps	-	Low

Conclusion

- This paper contributes a **reproducible method of constructing a physical spillway testbed model** with accompanying detailed descriptions of the underlying DCS and remote monitoring and control system.
- The designed and implemented testbed aligns with the **research interests** in academia and industry.
- In constructing a testbed, students and researchers can learn from a testbed representative of real-world systems with cyber components to **emulate an authentic system that is <u>cheaper</u>** and **<u>easier</u>** to use than the corresponding existing counterparts.
- The testbed provides a potential source of **dataset generation** for research in IDS, IPS, and related cybersecurity development for applications in critical infrastructure.

Acknowledgments

- This work was supported by the U.S. Army Engineer Research and Development Center (ERDC) – W914HZ-16-BAA-02.
- The authors appreciate the insight provided by Dr. Rishabh Das, Raphael B. Oliveira, Jack Smalligan, and Christopher H. Nguyen.

Questions?

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

CENTER FOR CYBERSECURITY
RESEARCH & EDUCATION