

A REMOTELY ACCESSIBLE, CONFIGURABLE, INSTRUMENTED ICS LAB FOR ATTACK, DEFEND, AND FORENSICS RESEARCH AND EDUCATION

Jim Jones, PhD

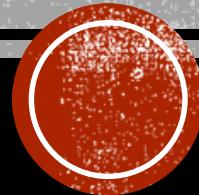
Associate Professor, ECE

George Mason University

Peggy Brouse, PhD

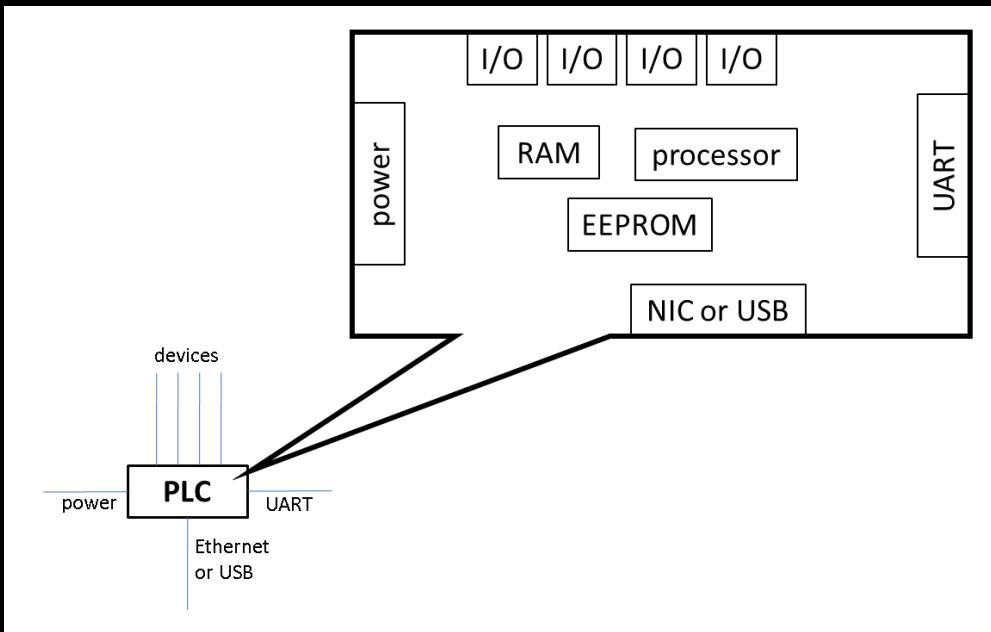
Professor, SEOR

George Mason University



BACKGROUND

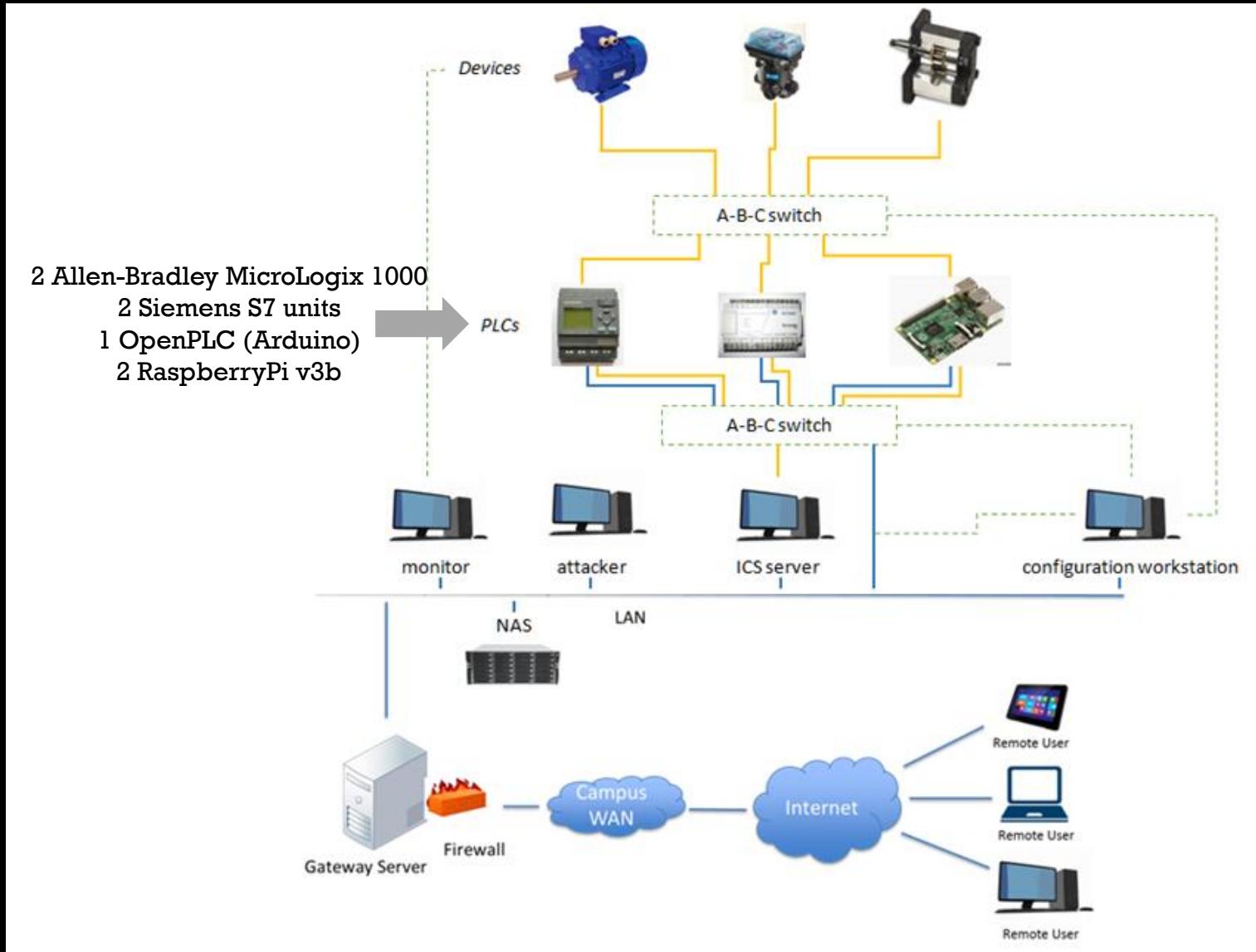
- ICS: Industrial Control System
- PLC: Programmable Logic Controller



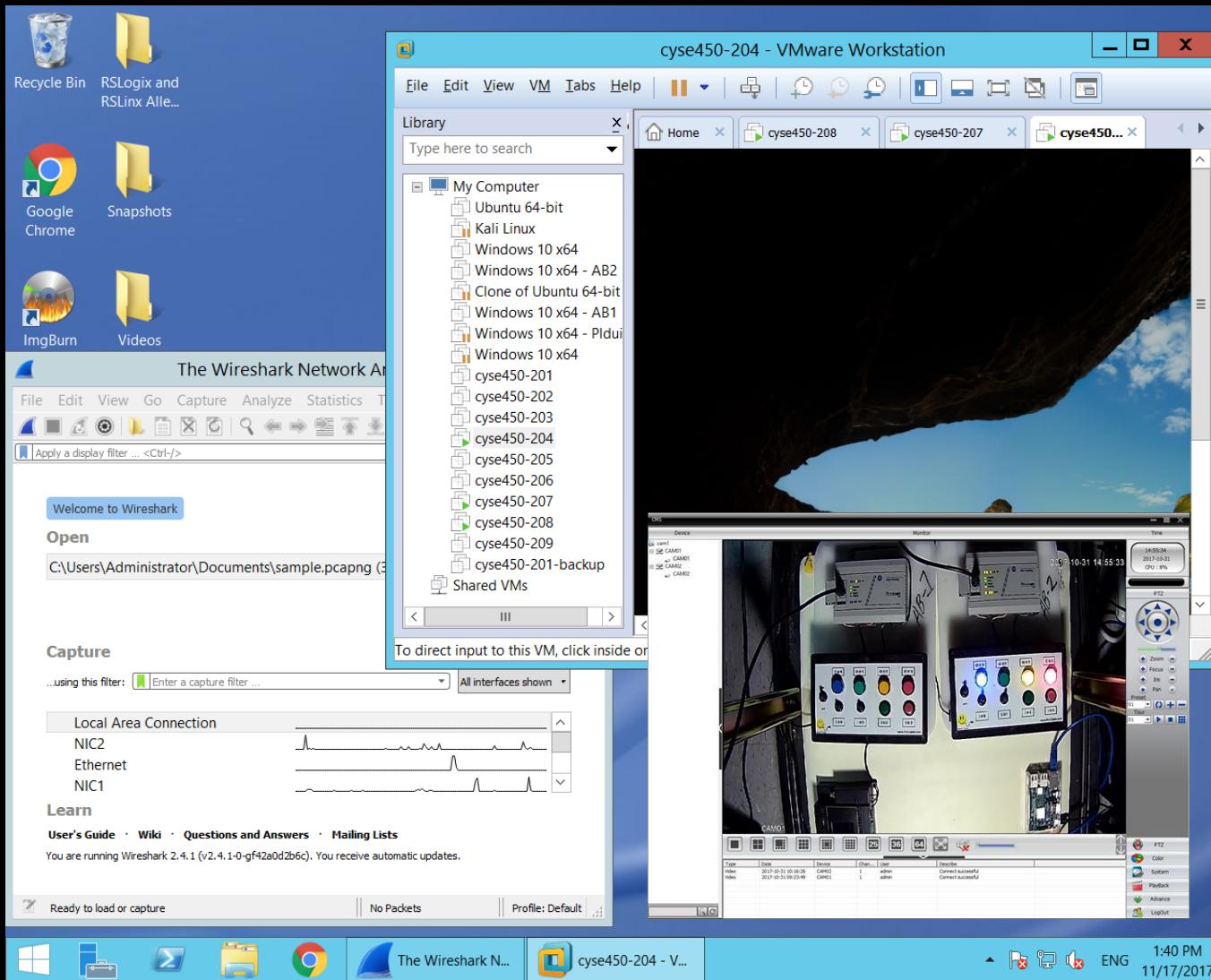
WHY? WHAT'S THE NEED, GAP, PROBLEM?

- **Academic programs:**
 - BS Cybersecurity Engineering
 - BS/MS/PhD Computer Engineering
 - PhD Information Technology with concentration in Digital Forensics
- **Research:**
 - Attack and compromise residual digital artifacts
 - persistent storage, volatile memory, and network
- **Need:**
 - Hands-on with realistic devices and environments
- **Problem:** virtual is useful for many cases, but with PLCs...
 - fidelity for deep forensics (e.g., storage behavior)
 - physical effects (e.g., power and other faults, inputs)
- **Goal:**
 - Real, remote environment for testing attack, defense, response, and forensics on ICS components (especially PLCs vs. control workstations)
- **Funding:**
 - NSA/US Army Reserve P3i grant

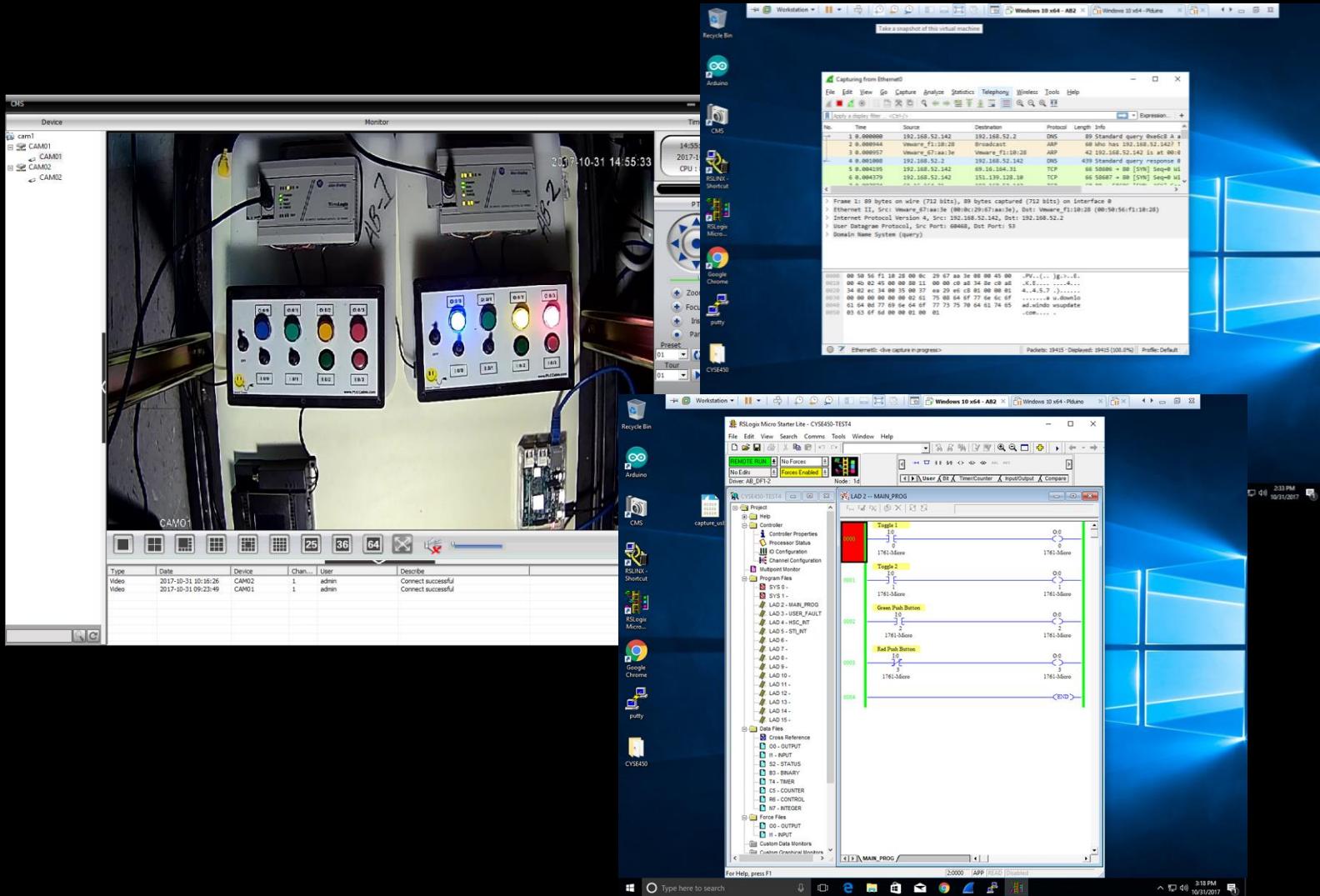
WHAT WE BUILT...



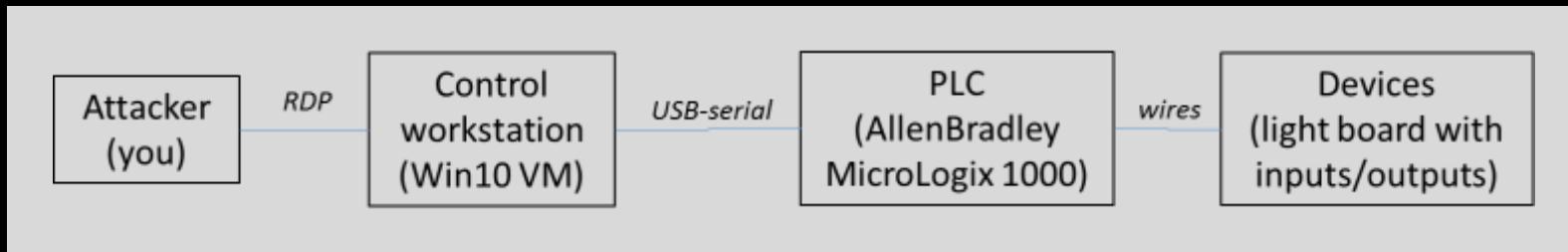
THE ADMINISTRATOR SEES...



THE STUDENT SEES...



STUDENT EXERCISE (CYSE 450)



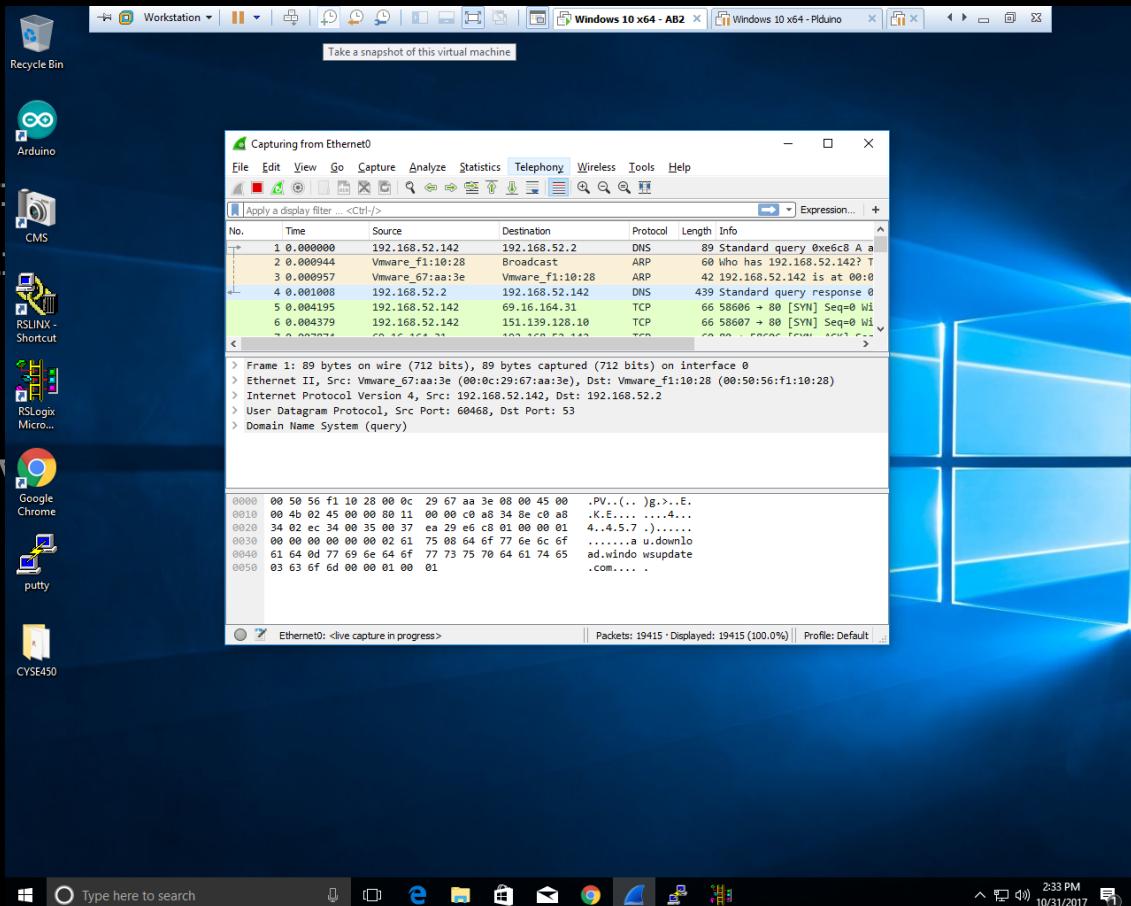
Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- Analyze firmware
- Analyze memory
- Offensive and defensive considerations

STUDENT EXERCISE (CYSE 450)

Exercise Activities:

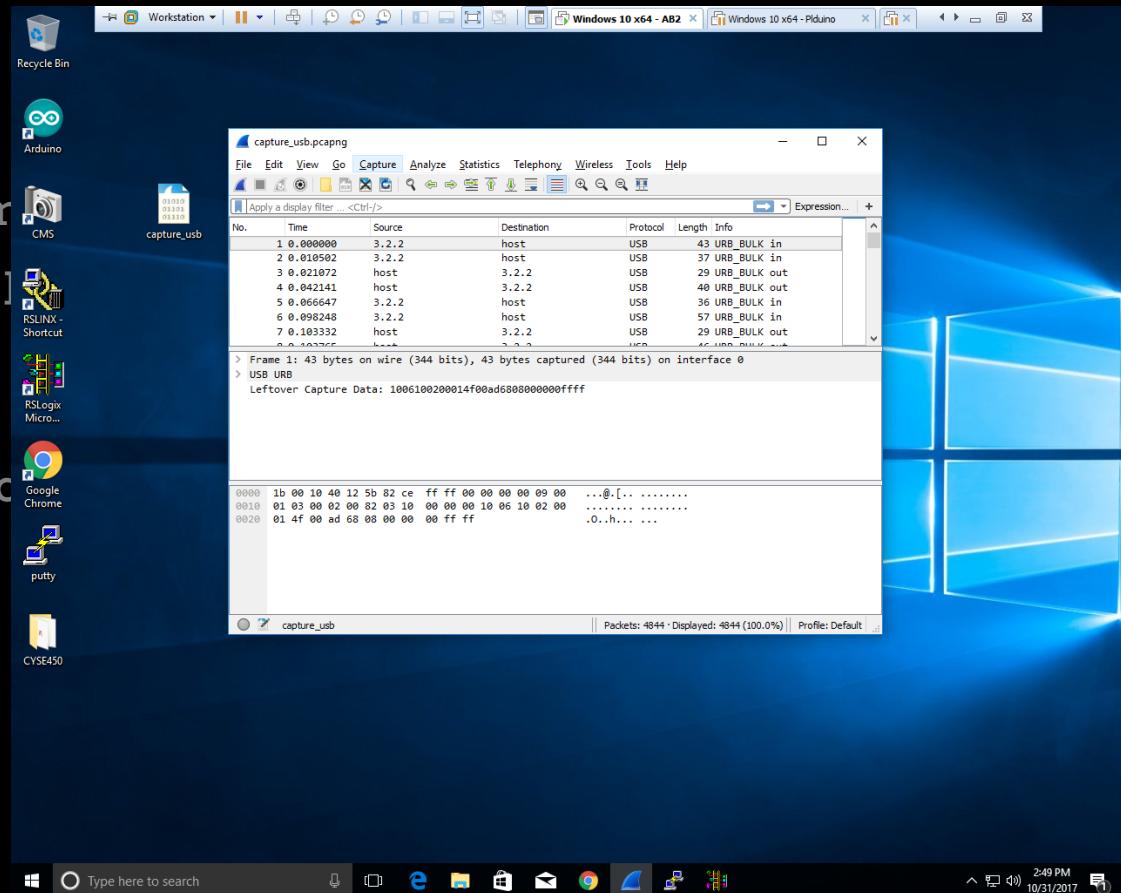
- **Access VM (control workstation)**
- **Sniff Ethernet side**
- Sniff USB/serial side
- Alter PLC states
- Capture running programs
- Modify and load running programs
- Analyze firmware
- Analyze memory
- Offensive and defensive exercises



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

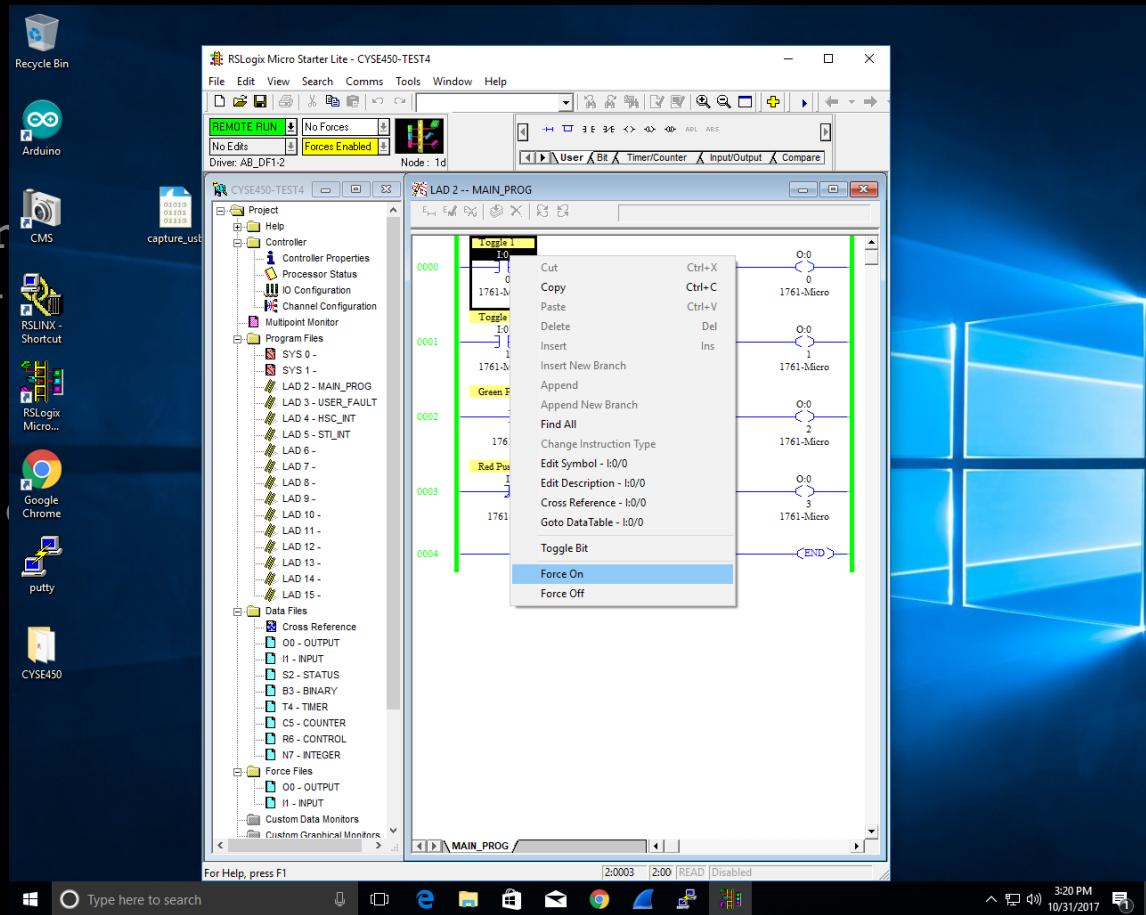
- Access VM (control workstation)
- Sniff Ethernet side
- **Sniff USB/serial side**
- Alter PLC states
- Capture running programs
- Modify and load running programs
- Analyze firmware
- Analyze memory
- Offensive and defensive controls



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

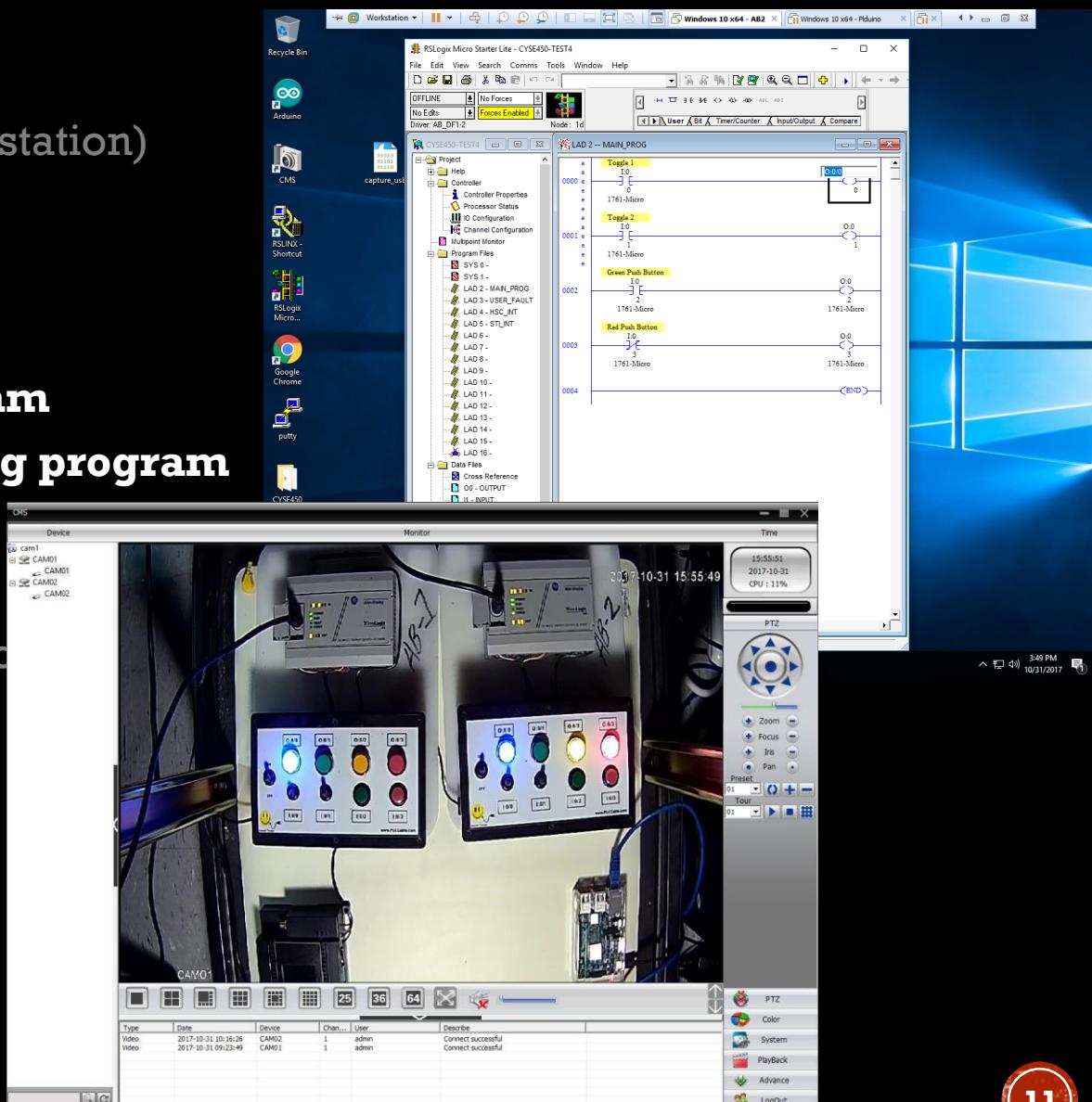
- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- **Alter PLC states**
- Capture running programs
- Modify and load running programs
- Analyze firmware
- Analyze memory
- Offensive and defensive exercises



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- **Capture running program**
- **Modify and load running program**
- Analyze firmware
- Analyze memory
- Offensive and defensive c



STUDENT EXERCISE (CYSE 450)

Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- **Analyze firmware**
- Analyze memory
- Offensive and defensive consider

HxD - [C:\Users\jones\Desktop\CYSE\CYSE450\1761-firmware.bin]

File Edit Search View Analysis Extras Window ?

1761-firmware.bin

Offset(h)	Hex	ASCII	Preview
00000000	4E F9 00 00 81 50 FF FF 46 57 52 4C 10 00 6E 2F	N...PyyFWRL/n	
00000010	61 00 00 00 FA 10 4D 4C 2D 31 31 30 30 20 4F 70	a...ú.ML-1100 Op	
00000020	65 72 20 53 79 73 74 65 6D 20 20 20 04 4C 00 01	er System .L..	
00000030	00 10 80 03 00 30 00 00 00 07 68 7C 00 00 F6 B3	..€.0....h ..ö³	
00000040	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000050	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000060	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000070	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000080	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000090	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000000A0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000000B0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000000C0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000000D0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000000E0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
000000F0	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	
00000100	00 00 00 00 A8 FFvvvvvvvvvvvvv	
00000110	FF	vvvvvvvvvvvvvvvvv	
00000120	FF	vvvvvvvvvvvvvvvvv	
00000130	FF	vvvvvvvvvvvvvvvvv	
00000140	FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00	vvvv.....	
00000150	46 FC 27 00 20 3C B0 00 00 00 4E 7B 08 01 20 7C	Fü'. <...N(..	
00000160	40 00 00 98 30 BC B0 00 20 7C 40 00 00 9C 20 BC	0...“0¤. @..¤.	
00000170	00 0F 00 01 20 7C 40 00 00 A2 30 BC OD E0 70 01 @..¤.ä.p.	
00000180	4E 7B 0C 04 20 3C 20 00 00 21 4E 7B 0C 05 20 7C	N(.. < ..!N(..	
00000190	40 10 00 50 10 BC 00 80 20 7C 40 14 00 00 30 BC	0..P.4.€ @...0¤	
000001A0	00 00 20 7C 40 00 00 80 30 BC FF E0 20 7C 40 00	.. @..€0¤yà @.	
000001B0	00 84 20 BC 00 1F 00 01 20 7C 40 00 00 8A 30 BC	.. ¤.... @..\$0¤	
000001C0	19 80 9D CE 72 14 41 FA 00 12 70 00 44 FC 00 01	.€.Ír.Aú..p.Dù..	
000001D0	22 7C 00 07 66 60 4E FB 98 F8 41 FA 00 4C 64 18	" ..f NÚ"¤Aú.Ld.	
000001E0	4F F9 B0 02 B1 38 4B F9 B0 01 00 00 42 A7 42 A7	Öù°.‡§Kù°...BSBS	
000001F0	42 A7 59 8F 41 FA 00 34 43 FA 00 36 2E 89 DB FC	BSY.Aú.4Cú.6.%Ü	
00000200	00 00 80 00 24 3C 00 00 00 26 3C 00 00 00 00 00	..€.\$<....&<....	
00000210	28 3C 00 00 00 00 2A 3C 00 00 00 00 2F 08 20 7C	(<....*<..../.	

Offset: 0 Overwrite

STUDENT EXERCISE (CYSE 450)

Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- Analyze firmware
- **Analyze memory**
- Offensive and defensive considerations

```
Data File S2 (hex) -- STATUS

Main
First Pass S:1/15 = No
Index Register S:2/4 = 0
Free Running Clock S:4 = 1001-1001-1011-1001

Scan Times
Maximum (x10 ms) S:2/2 = 1
Current (x10 ms) S:3 (low byte) = 0
Watchdog (x10 ms) S:3 (high byte) = 50

Math
Match Overflow Selected S:2/14 = 0
Overflow Trap S:5/0 = 0
Carry S:0/0 = 0
Overflow S:0/1 = 0
Zero Bit S:0/2 = 0
Sign Bit S:0/3 = 0
Math Register (lo word) S:12 = 0
Math Register (high word) S:14-S:13 = 0
Math Register (32 Bit) S:14-S:10 = 0

Debug
Suspend Code S:7 = 0

Errors
Extend I/O Configuration S:0/8 = 0
Fault Override At Power Up S:1/8 = 0
Startup Protection Fault S:1/9 = 0
Major Error Halt S:1/13 = 0
Major Error S:6 = 0h
Overflow Trap S:5/0 = 0
Control Register Error S:5/2 = 0
Major Error Executing User Fault Rtn. S:5/3 = 0
Retentive Data Lost S:5/8 = 0
Input Filter Selection Modified S:5/12 = 0
Error Description:

STI
Pending Bit S:2/0 = 0
Enable Bit S:2/1 = 1
Executing Bit S:2/2 = 0
Overflow Bit S:5/10 = 0
Setpoint (x10ms) S:30 = 0

Protection
RUN Aways S:1/12 = No
Deny Future Access S:1/14 = No

Forces
Forces Enabled S:1/5 = Yes
Forces Installed S:1/6 = No
```

Data File I1 (bin) -- INPUT																
Offset	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
I:0.0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1
I:0.1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Bul.1761

MicroLogix 1000 DH-485/HDSLave

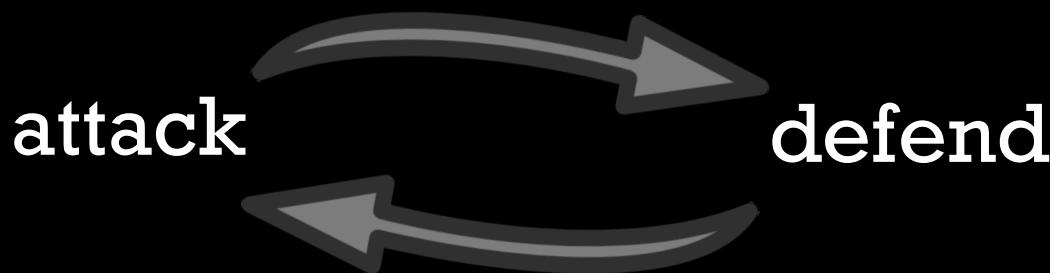
Data File O0 (bin) -- OUTPUT																
Offset	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
O:0.0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	Bul.1761

MicroLogix 1000 DH-485/HDSLave

STUDENT EXERCISE (CYSE 450)

Exercise Activities:

- Access VM (control workstation)
- Sniff Ethernet side
- Sniff USB/serial side
- Alter PLC states
- Capture running program
- Modify and load running program
- Analyze firmware
- Analyze memory
- **Offensive and defensive considerations**



RESULTS AND NEXT STEPS

RESULTS:

- Minimal problems walking through guided portion of lab
 - Exposure to PLCs, ladder logic
- Applied existing skills analyzing network, code, firmware, memory
- Offense and defense:
 - ideas from lab and open sources
 - applied iterative security assessment model

NEXT STEPS:

- Additional hardware (more PLCs)
- Additional exercises (attack and manipulation; forensics)
- More instrumentation
- Sequential memory snapshot analysis under adversarial activity

QUESTIONS?

Jim Jones, PhD

Associate Professor, ECE

Digital Forensics and Cyber Analysis

Nguyen Engineering Bldg., Room 3241

George Mason University, MS 2B5

Fairfax, VA 22030

(o) 703-993-5599

(c) 703-955-1033

(e) jjonesu@gmu.edu

(w) <http://ece.gmu.edu/>

(w) <http://cfrs.gmu.edu/>

(w) <http://dfdarg.wordpress.com>