SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

CPS-SPC 17 @ Dallas, US

Gamifying ICS Security Training and Research: Design, Implementation, and Results of S3

DANIELE ANTONIOLI, H. R. GHAEINI, S. ADEPU, M. OCHOA, N. O. TIPPENHAUER

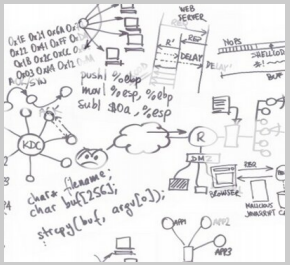
Singapore University of Technology and Design (SUTD)

Capture-The-Flag Security Competitions

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Jeopardy-style CTF
  - Teams compete online
  - Set of challenges divided by categories (RE, crypto)
  - Score points by finding (or computing) flags
- Attack-defense CTF
  - Each team gets a vulnerable (virtual) machine
  - Maintain the services uptime to score points
  - Compromise the services of other teams to score points
- Why are CTF events useful?
  - Instant feedback for the players
  - Playing as a team is key (orthogonal skills)

Selected CTF Events



iCTF by UCSB

Insomni'hack

OWASP CTF

Google CTF

Source: ctftime.org

- Diverse organizers: academia, industry, amateurs
  - *Almost no CTF targeted to Industrial Control System security*

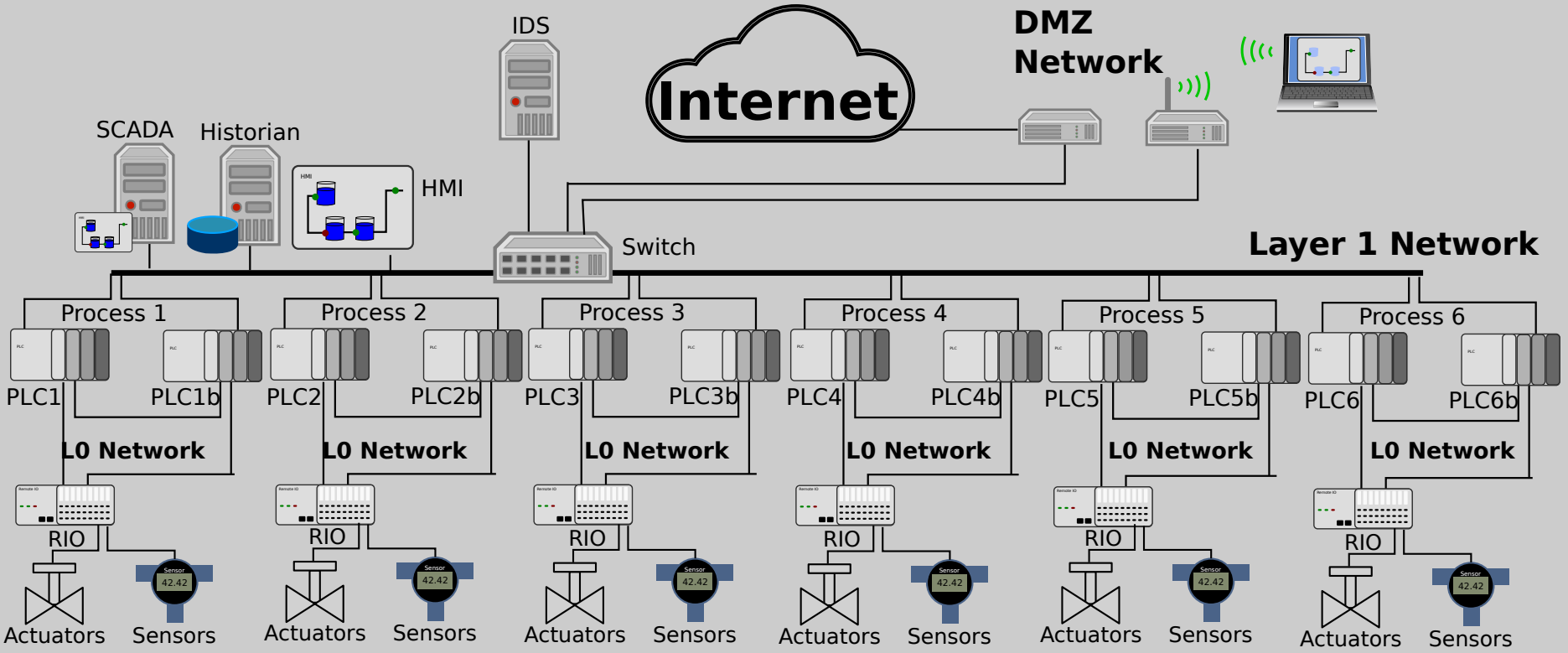
Our Approach: The S3 Contest

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- **SWaT Security Showdown (S3) contest**
  - ICS-centric, gamified security competition
  - Involves academia and industry
  - Develop (new) attacks and evaluate (new) defenses
  - Access to a real ICS (SWaT)
- **Online phase: Jeopardy-style CTF**
  - ICS-specific categories
  - Over the web
- **Live phase: attack-defense CTF**
  - Attack and defend SWaT
  - Hosted by SUTD

Secure Water Treatment (SWaT) Testbed

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN



Process 1: Supply and Storage
Process 2: Pre-treatment
Process 3: Ultrafiltration

Process 4: De-Chlorination
Process 5: Reverse Osmosis
Process 6: Permeate Managment

Layer 1 Network: control

L0 Networks: field

S3 Online Competition Setup (2016)

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

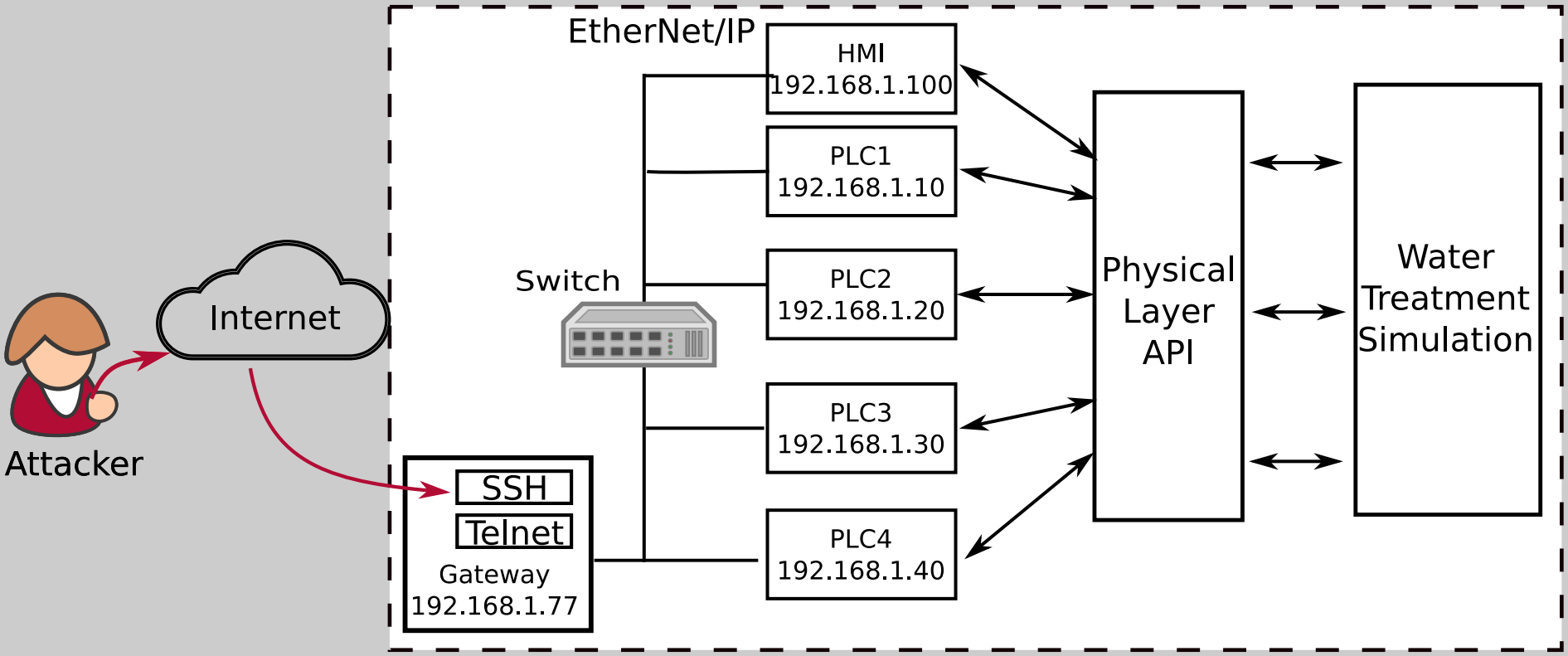
- 6 invited international attacking teams
  - 3 from industry
  - 3 from academia
  - Team names are anonymized
  - No defenders in this phase
- Jeopardy-style CTF logistics
  - Flask-based web application (over HTTPS)
  - 20 challenges (mostly SWaT-related)
  - 5 categories (worth 510 points)
  - Two 48-hours CTFs (3 team / CTF, identical CTFs)

S3 Online Phase: CTF Challenges

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Category	Chs	Points	ICS Security Domains
Forensics	4	105	Packet manipulation and cryptography
MiniCPS	5	210	Simulated tank overflows, industrial network mapping, MitM attacks
Misc	2	90	Web authentication, steganography
PLC	3	60	Remote access to real PLCs, Ladder logic programming
Trivia	6	45	SWaT's physical process, devices and attacks
Total	**20**	**510**	

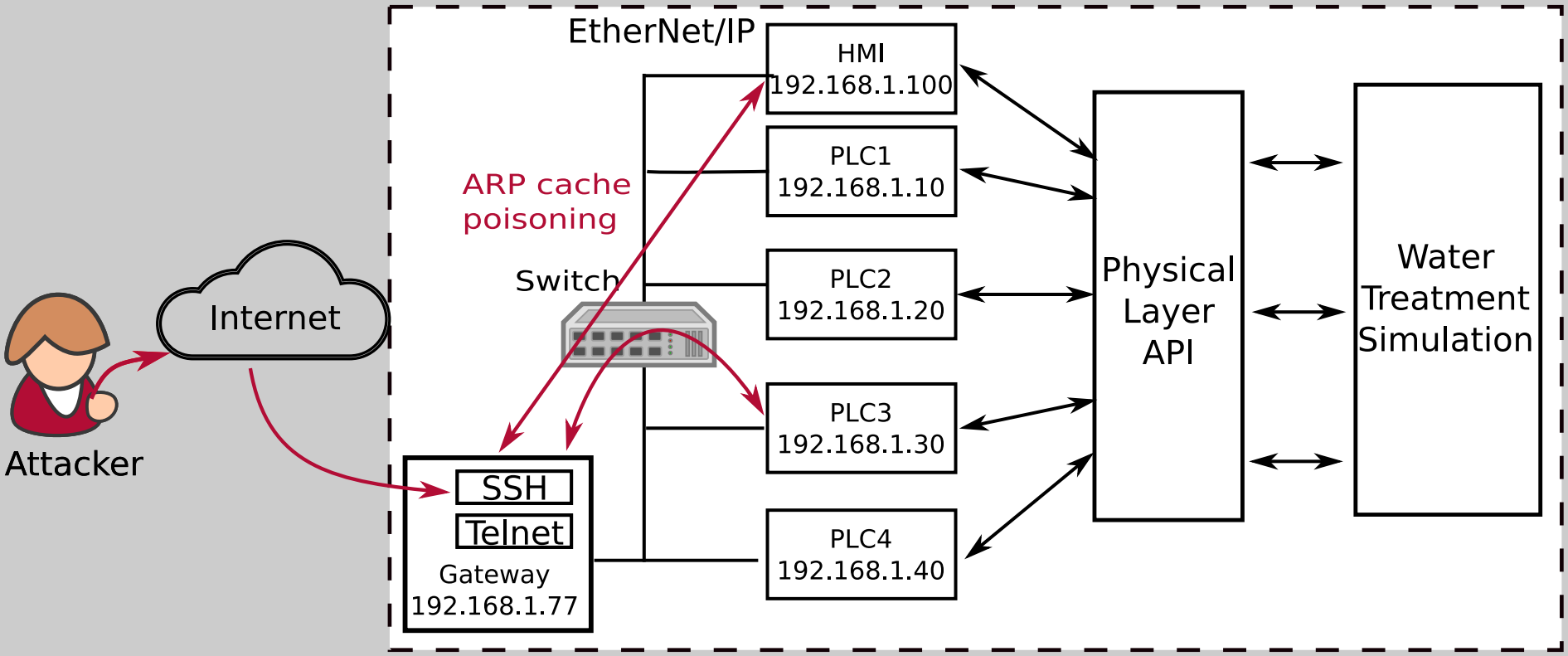
S3 Online Phase: MiniCPS



- MiniCPS:
  - Combines `mininet` network emulation with ICS devices and physical process simulation[1]
  - Mimics part of the SWaT control network[2]

[1] *MiniCPS: A toolkit for security research on CPS Networks* [CPS-SPC15]
[2] *Towards High-Interaction Virtual ICS Honeypots-in-a-Box* [CSP-SPC16]

S3 Online Phase: MiniCPS



- MiniCPS:
  - Combines `mininet` network emulation with ICS devices and physical process simulation[1]
  - Mimics part of the SWaT control network[2]

[1] *MiniCPS: A toolkit for security research on CPS Networks* [CPS-SPC15]
[2] *Towards High-Interaction Virtual ICS Honeypots-in-a-Box* [CSP-SPC16]

S3 Online Phase: PLC

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Attackers had access to a PLC programming IDE
  - VNC client to get a GUI on the SWaT workstation
  - Workstation runs Studio 5000 (Rockwell Automaton)
- Ladder logic programming for PLC
  - Sequential control logic represented as a diagram
  - Graphical programming
- Attacker had to audit and modify the PLC control logic
  - Jump to a specific subroutine
  - Fix bugs and reload the program in real-time
  - No access to the firmware
  - Recent related work[3]

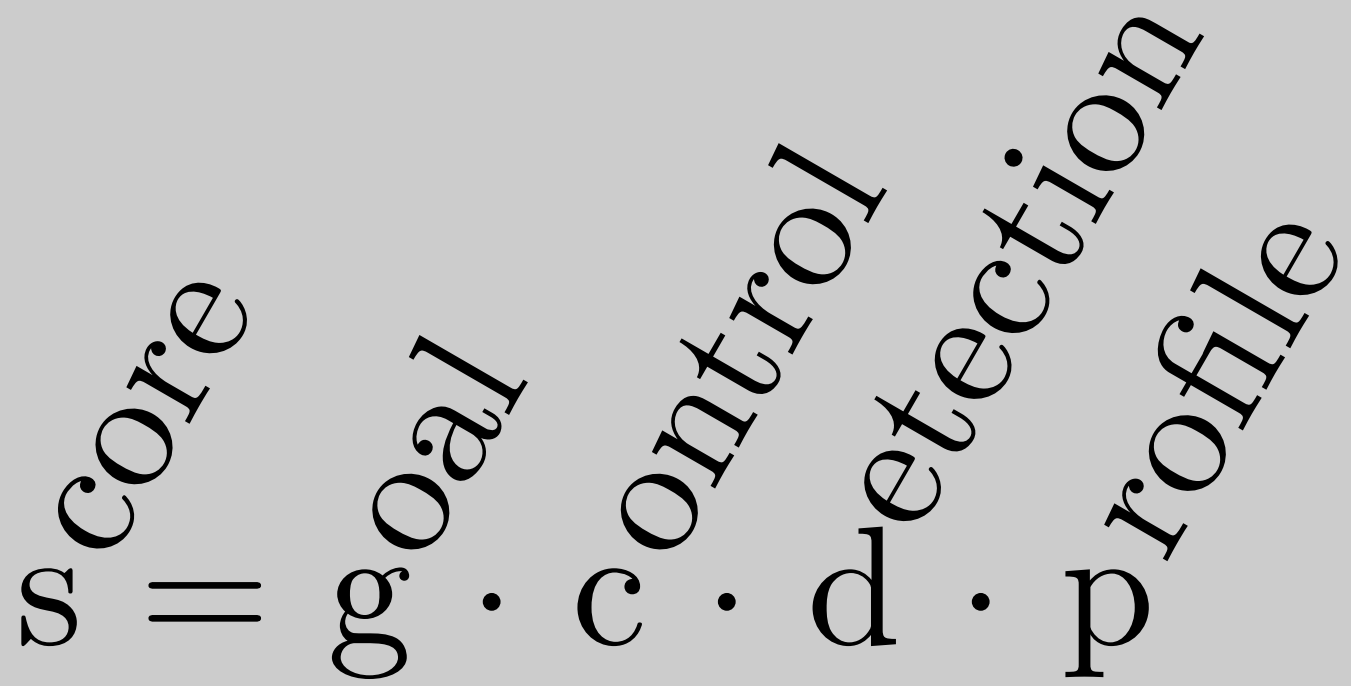
[3] *On Ladder Logic Bombs in Industrial Control Systems* [CyberICPS17]

S3 Live Competition Setup (2016)

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- 6 defending teams
  - 4 invited from industry
  - 2 from SUTD
- Same attacking teams of the online phase
- Attack-defense CTF logistics
  - 1 day access to the SWaT (prior to S3)
  - 3 hours per attacking team (3 teams per day)
  - 6 defenders played in all the sessions
  - We scored only the attackers

S3 Live Scoring System



- Scoring goals:
  - Incentivise sophisticated attacks to better evaluate the countermeasures
  - De-incentivise re-use of same attack techniques
  - Accomodate attackers with different expertises
  - Correlate the score to an adequate ICS attacker model[4]

[4] *On Attacker Models and Profiles for Cyber-Physical Systems* [ESORICS16]

S3 Live Scoring System

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

$$\text{PLC readings: } g = 160$$
$$\text{Randomly affected: } c = 0.2$$
$$\text{One detection: } d = 1.84$$
$$\text{Insider attacker: } p = 1.5$$
$$s = 88$$

- Scoring goals:
  - Incentivise sophisticated attacks to better evaluate the countermeasures
  - De-incentivise re-use of same attack techniques
  - Accomodate attackers with different expertises
  - Correlate the score to an adequate ICS attacker model[4]

[4] *On Attacker Models and Profiles for Cyber-Physical Systems* [ESORICS16]

S3 Our Detectors: ARGUS and HAMIDS

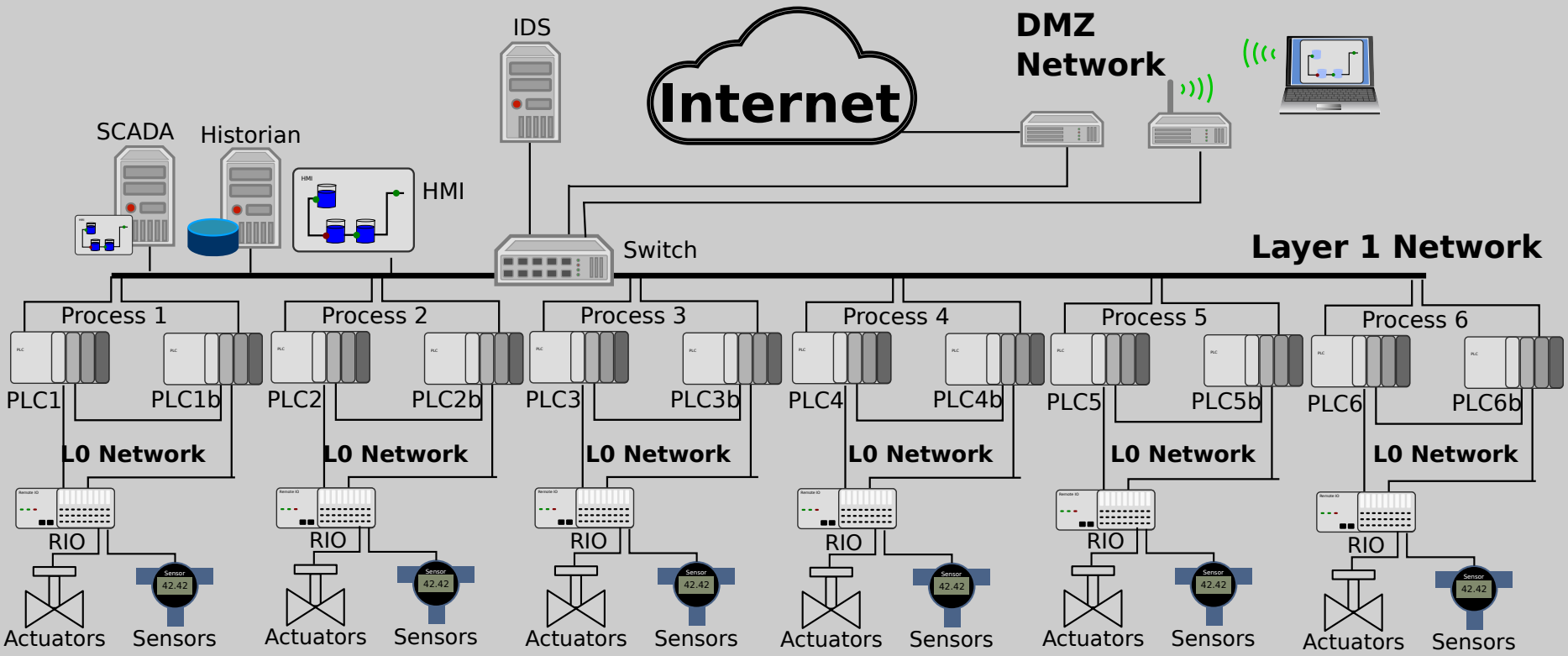
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- Disclaimer
  - I'm not the developer of these detection mechanisms
- ARGUS[5]
  - Based on physical invariants derived from the SWaT
  - Invariants translated to the PLC control logic
  - Extra PLC logic used for detection
- HAMIDS[6]
  - Distribute Bro detectors nodes in the ICS network
  - Centrally collect and process network data
  - Detect suspicious traffic

[5] *Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plant* [AsiaCCS16]

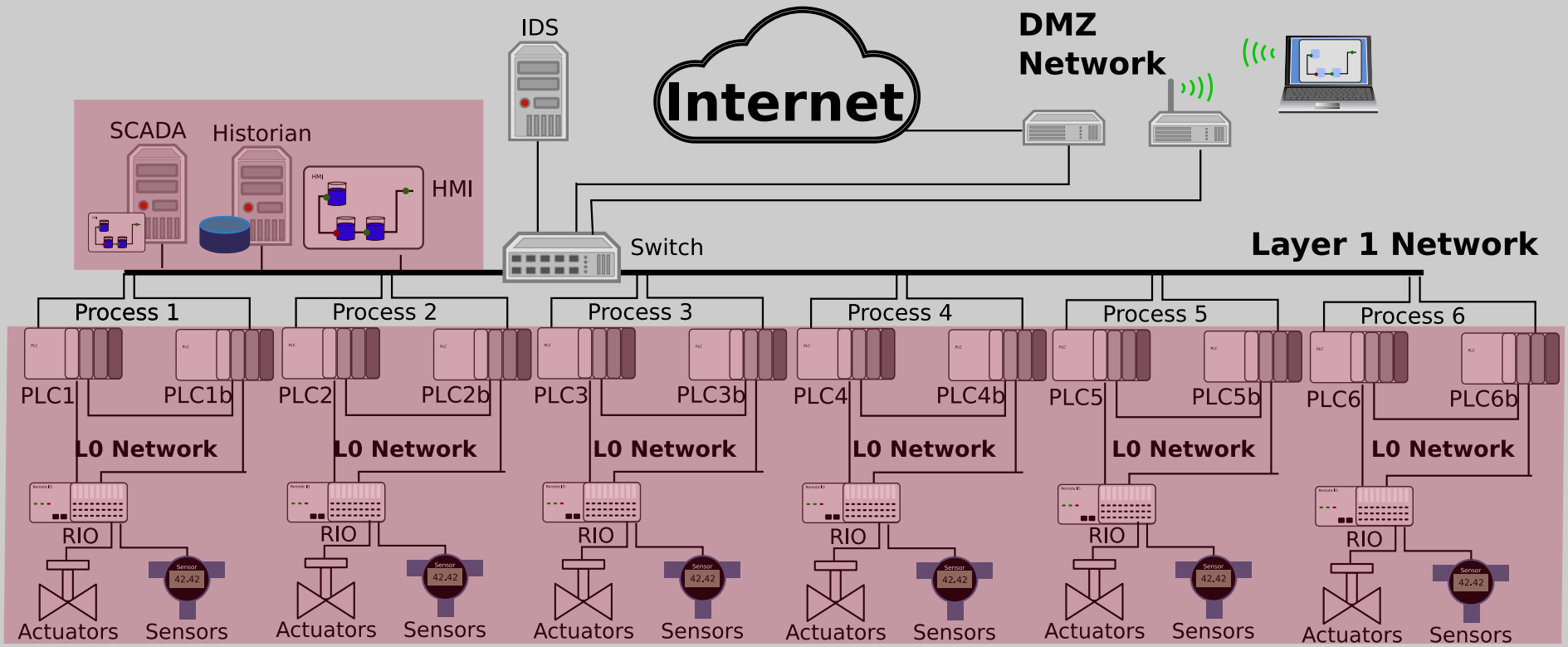
[6] *HAMIDS: Hierarchical Monitoring Intrusion Detection System for Industrial Control Systems* [CPS-SPC16]

S3 Live Phase: Attackers and Defenders



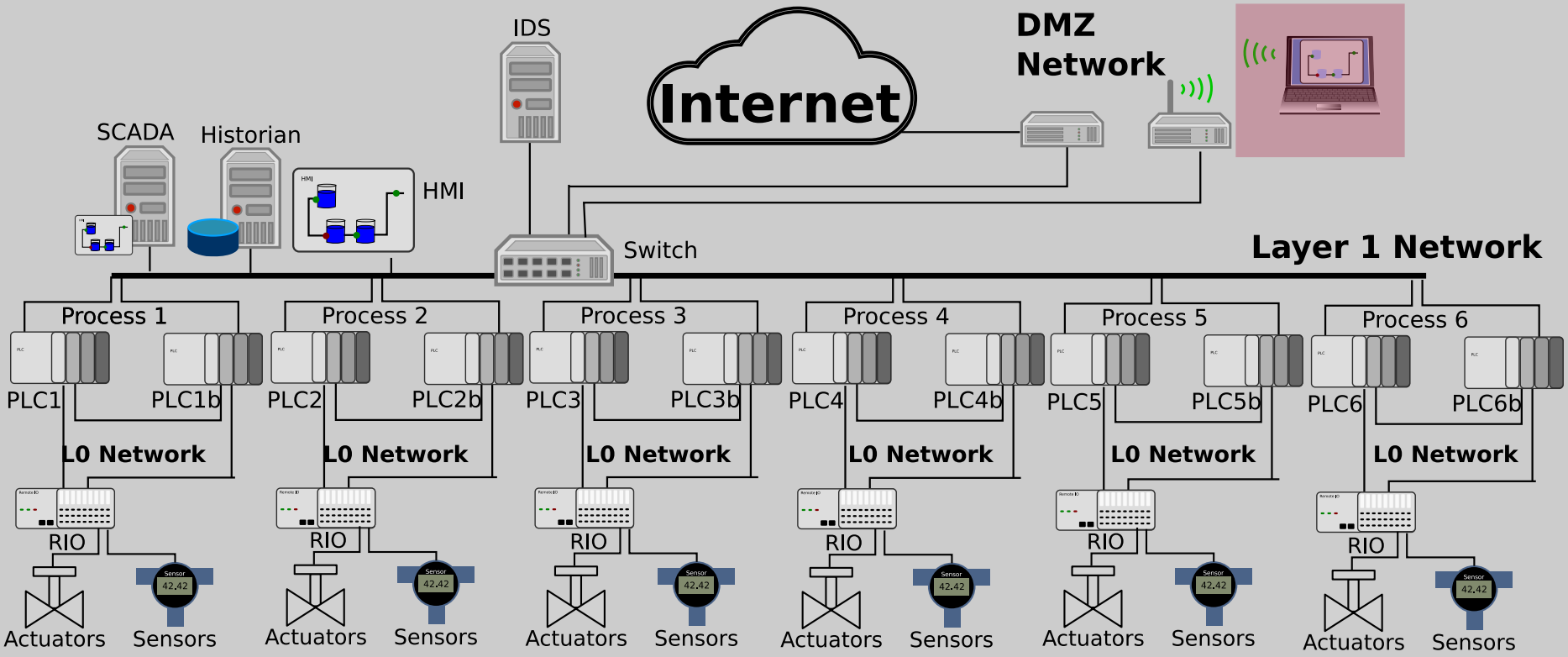
- SWaT testbed

S3 Live Phase: Attackers and Defenders



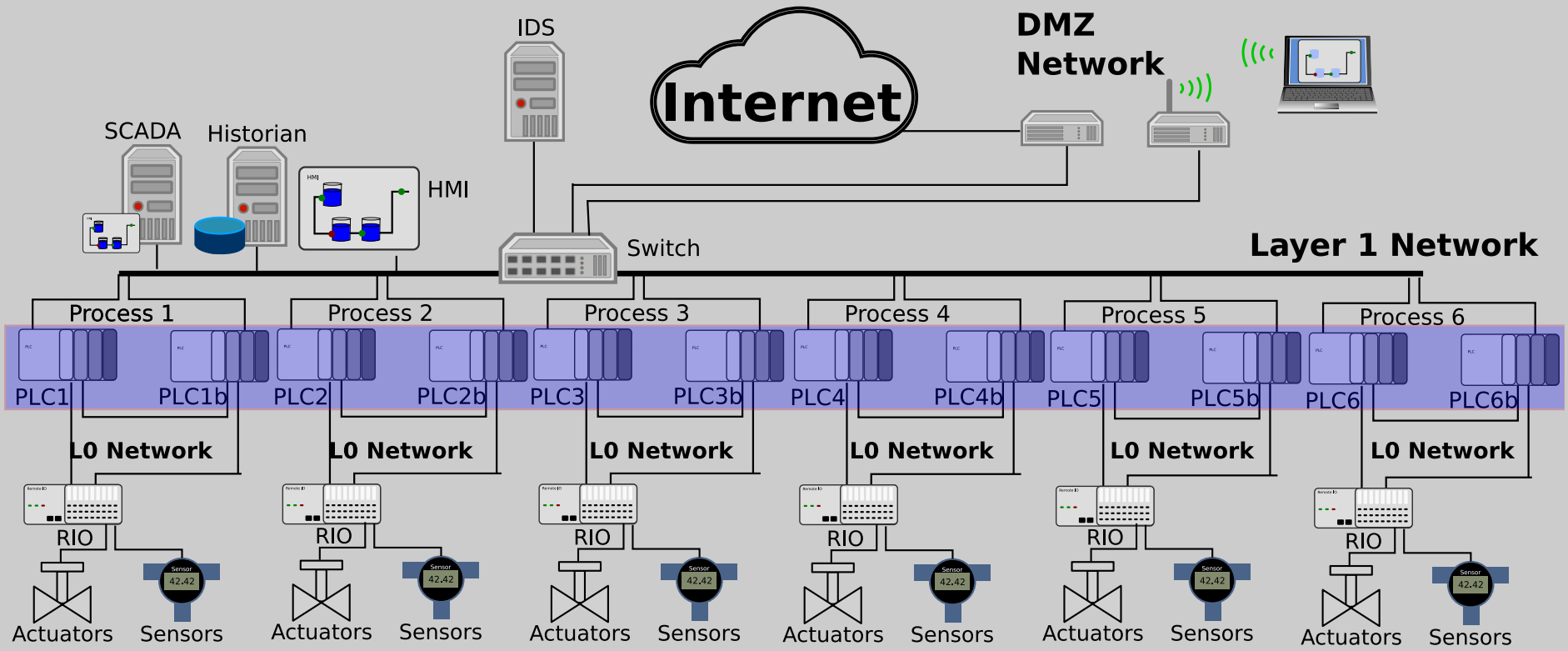
- Insider attacker

S3 Live Phase: Attackers and Defenders



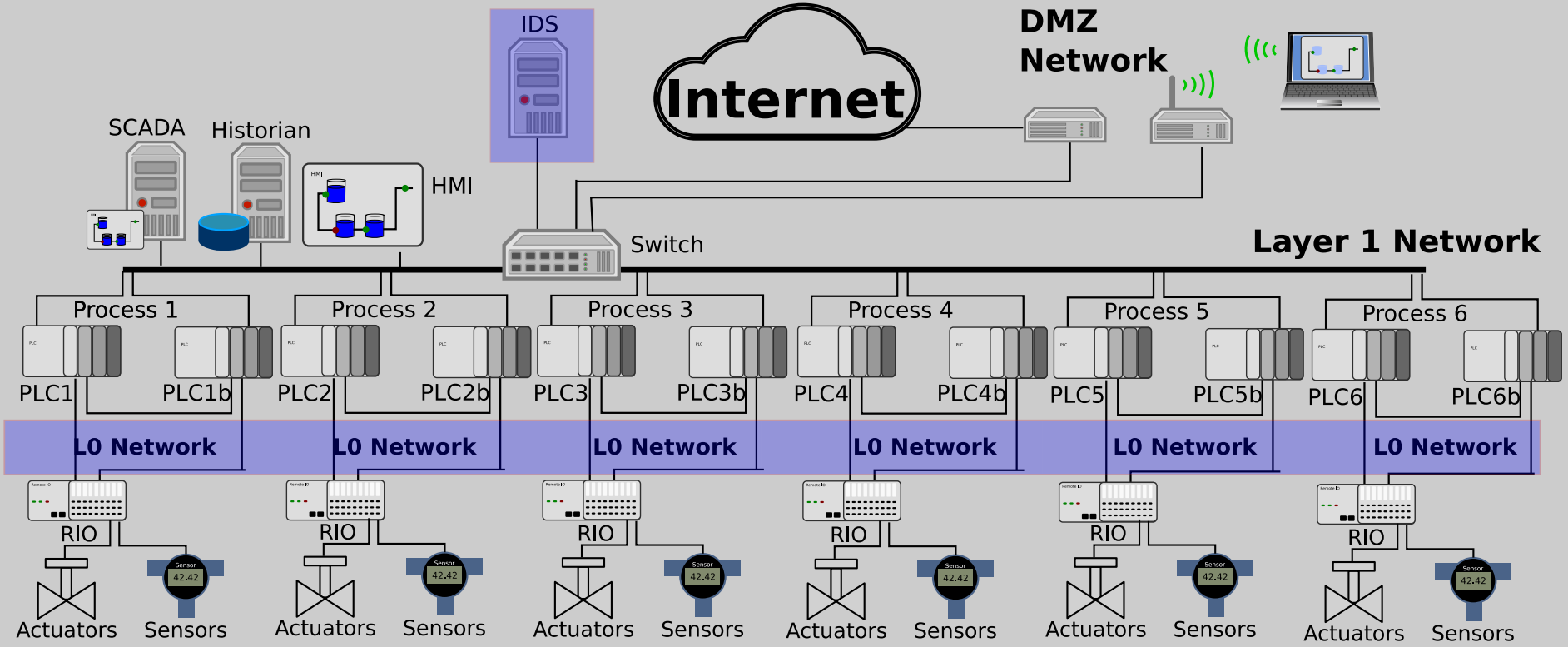
- Cybercriminal attacker

S3 Live Phase: Attackers and Defenders



- ARGUS detection

S3 Live Phase: Attackers and Defenders



- HAMIDS detection

S3 Selected Attacks

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Description	Type	ARGUS	HAMIDS	Score
DoS PLC1 by TCP SYN flooding	Cyber	○	●	396
Dosing pump manipulation	Physical	●	○	360
Spoofing over the field network	Physical	●	●	324
DDoS by distributed ARP spoofing	Cyber	○	●	104

- Legend: ○= Undetected, ●= Detected.

S3 Online Phase Results (2016)

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Jeopardy-style CTF

	Category-Flags						
Team	**C-5**	**T-6**	**F-4**	**P-3**	**M-2**	**Flags**	**Score**
T2	5	6	4	3	2	20	510
T6	5	6	4	3	2	20	510
T1	2	6	4	0	1	13	250
T4	4	4	2	0	0	10	161
T3	0	4	2	0	1	7	86
T5	0	4	2	0	1	7	66
Total	**16**	**30**	**18**	**6**	**7**	**77**	**1583**

- Legend: C=MiniCPS, T=Trivia, F=Forensics, P=PLC, M=Misc

S3 Live Phase Results (2016)

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Attack-defense CTF

Team	Attacks	Score
T5	5	688
T1	4	666
T3	3	642
T6	3	477
T2	2	458
T4	1	104
Total	**18**	**3035**

Post-S3 Survey by Attackers

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Question	Outcome
Overall grade for the S3 event?	Good +
Difficulty of the live phase?	Good
Difficulty of the online phase?	Good -
Scoring for the live phase?	Good -
Scoring for the online phase?	Good
Usefulness of pre-shared information?	Good -

SWaT Security Showdown (S3) Summary

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

- **S3: Jeopardy-style and attack-defense CTF events**
  - Gamified, ICS-security centric
  - Involves academia and industry
  - Remote and physical access to a real testbed (SWaT)
  - Development of new attacks
  - Evaluation of actual countermeasures
- **S3 in numbers:**
  - Six attacking teams: 3 from industry and 3 from academia
  - Six defending teams: 4 from industry and 2 from academia
  - Online phase: 77 captured flags worth 1583 points
  - Live phase: 18 attacks on a real testbed worth 3035 points

Thanks for your time! Questions?