SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

iTrust
Centre for Research
in Cyber Security

CISS: Critical Infrastructure Security Showdown 2019

26 to 30 August 2019
Secure Water Treatment (SWaT) Testbed
Singapore University of Technology and Design

1.   Introduction

The CISS 2019 ("Event") is taking place at SUTD in August 2019, with the walkthrough phase on the morning of 26 August, and the attacking phase from 26 August (afternoon) to 30 August. In this event, Red Teams will have the chance to attack the water testbed, the Secure Water Treatment (SWaT) testbed, at SUTD. At the same time, Blue Teams will be able to showcase their detection capabilities against cyber attacks. For additional realism, Red Teams are encouraged to enter SWaT's network via the ZyCron Cyber City (ZCC), which simulates a plant operator's enterprise network and through which the Red Teams will attempt to gain access to reach the testbed.

2.   Schedule

The attack schedule will be determined by drawing lots and will be announced one week on the website before the actual event. Red Team leaders will also be notified via email.

Table 1: Summary of the activity and attack schedule

Date	Time	Activity & attack schedule	Involvement
26 Aug (Mon)	09:00 – 11:00	Session 1: Introduction to testbed + Q&A	Red Teams 1 to 4 (non-mandatory)
	11:00 – 13:00	Session 2: Introduction to testbed + Q&A	Red Teams 5 to 8 (non-mandatory)
	13:30 – 17:30	Attack by Red Team 1	Red Team 1 All Blue Teams
	17:30 – 18:30	System recovery	iTrust staff
27 Aug (Tues)	09:00 – 13:00	Attack by Red Team 2	Red Team 2 All Blue Teams
	13:00 – 14:00	System recovery	iTrust staff
	14:00 – 18:00	Attack by Red Team 3	Red Team 3 All Blue Teams
28 Aug	09:00 – 13:00	Attack by Red Team 4	Red Team 4

Date	Time	Activity & attack schedule	Involvement
(Wed)			All Blue Teams
	13:00 – 14:00	System recovery	iTrust staff
	14:00 – 18:00	Attack by Red Team 5	Red Team 5 All Blue Teams
29 Aug (Thurs)	09:00 – 13:00	Attack by Red Team 6	Red Team 6 All Blue Teams
	13:00 – 14:00	System recovery	iTrust staff
	14:00 – 18:00	Attack by Red Team 7	Red Team 7 All Blue Teams
30 Aug (Fri)	09:00 – 13:00	Attack by Red Team 8	Red Team 8 All Blue Teams
	13:00 – 14:00	System recovery	iTrust staff
	14:00 – 18:00	Judging & scoring	iTrust staff
	18:00 – 20:00	Reception and results announcement	All Red & Blue Teams

2.1   Familiarisation Phase: 26 August

2.1.1. All Red Teams are invited to come to the SWaT testbed to familiarise with SWaT and ZCC, and ask questions. No attacks or connections of any sort are allowed at this point. Attendance in this phase is non-mandatory and has no bearings on the team's final score. Please see Table 1 above for attendance schedule. Technical details of SWaT can be found here and here.

2.1.2. ZCC is a full-fledge organisation comprising of Information Technology (e.g., e-mail server, file server, printer server, CCTV, honeypot and intranet) and Operational Technology (water treatment processes in SWaT), that are meaningfully represented. To make these entities "alive," various types of network traffic are carefully crafted and included in Cyber City. A high-level architecture of ZCC is presented in Figure 1.
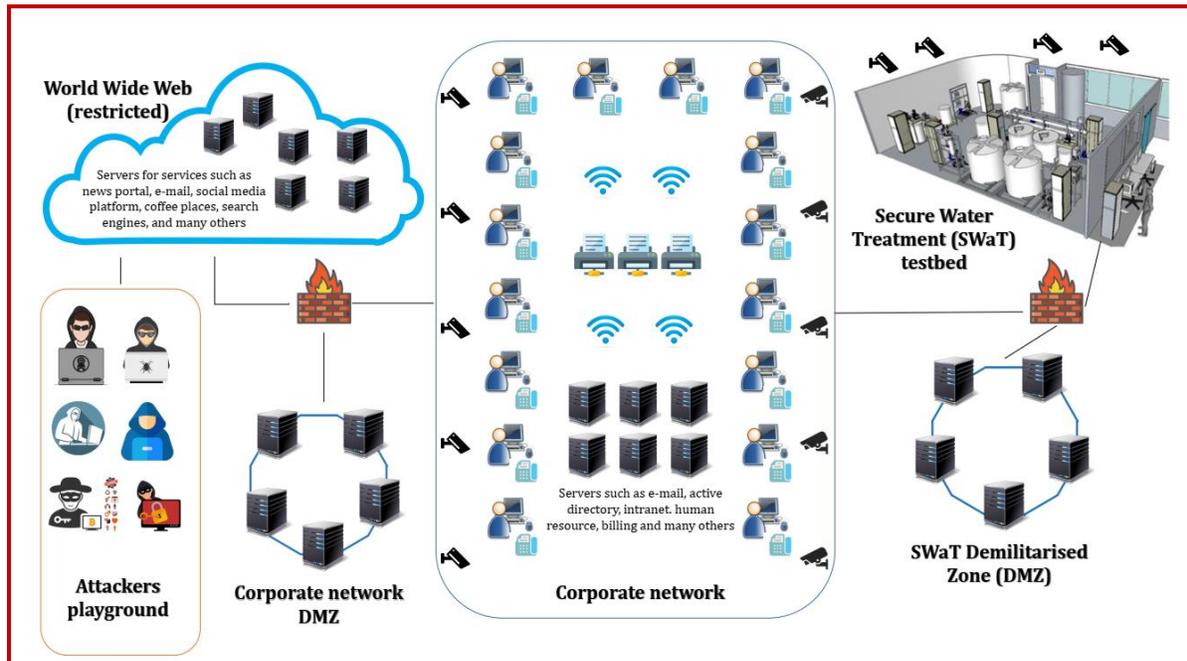
NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

iTrust
Centre for Research
in Cyber Security

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

Figure 2: High-level Architecture of Cyber City

2.2   Attack Phase: 26 – 30 August

2.2.1.   Each Red Team is given 4 hours to demonstrate its attacks and achieve the pre-determined goals (see para 4 for details on scoring). The 4 hours include, but are not limited to: setting up of equipment, reconnaissance, designing and launching attacks, interactions with judges and taking breaks[1].

2.2.2.   Red Teams will launch their attacks from the SWaT control room, which is nestled between the testbed and ZCC (see Figure 2). Only the active Red Team, accompanied by judges, iTrust staff and selected observers are allowed in the SWaT control room. Rooms will be available to other Red Teams to discuss and plan their attacks.

2.2.3.   Concurrently, an array of detection mechanisms is deployed in SWaT by the Blue Teams before the event, which will try to detect and report, but not prevent, the ongoing attacks. The Blue Teams will be housed in a separate room (EPIC Testbed) from the Red Teams to monitor and report the attacks to iTrust.

---

[1] Light refreshments will be provided

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

iTrust
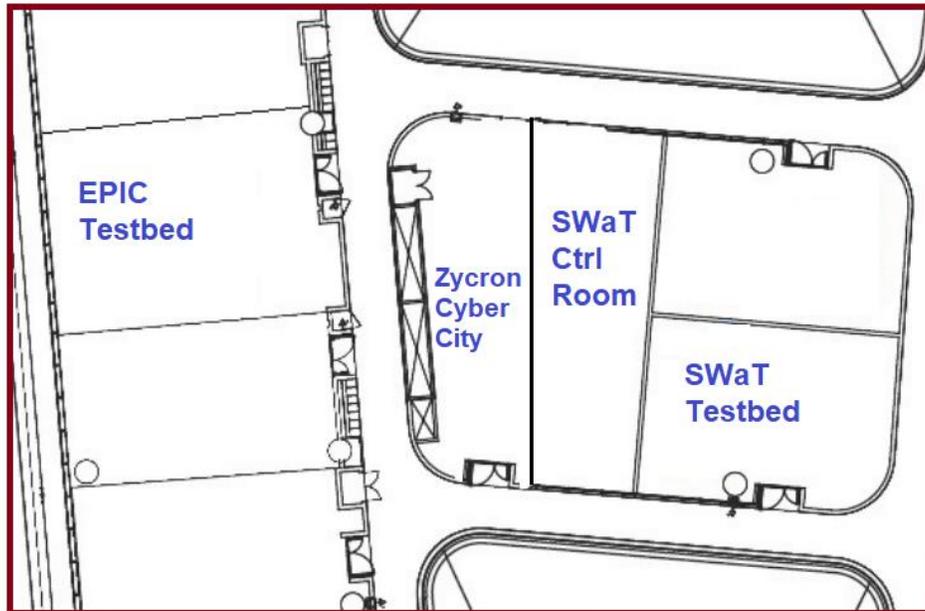Centre for Research
in Cyber Security

Figure 2: Venue for CISS 2019

3. Rules & Regulations

3.1 General

3.1.1. All participants in this event agree and accept the terms and conditions of participation and the use of personal data as well as photography and/or video recording during and after the event by the organisers for purposes of producing editorial content and research.

3.1.2. Red and Blue Teams must confirm and submit a list of their team members, along with a clear passport sized photo, to iTrust by 16 August 2019 in exchange for ID passes (non-transferrable). No changes to the team members will be entertained thereafter.

3.2 Red Team

3.2.1 Setup
- Up to 4 registered team members are allowed; ID passes issued by iTrust will be used for identification and access

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

iTrust
Centre for Research
in Cyber Security

- Electric power[2], tables and chairs for up to 4 persons and a separate network for internet uplink (do not attack that network) will be provided
- Can use your own laptops and hard/software tools; the laptops can be connected to the devices/network directly. iTrust will not provide any additional hard/software beyond what is already available in the control room
- Agree to provide a copy of their software tools and/or source codes to event organisers for research purposes

3.2.2 Attack

- There shall not be external communication with other persons, for example, to seek assistance in launching the attacks
- No physical access to SWaT and ZCC
- Must inform the judges on the attacks they wish to carry out, obtain a green light, before proceeding
- Activities or actions that would interfere, obstruct or disturb other teams, participants, event organisers and running of the event are strictly prohibited. In addition, the following will not be available for attack:
  a) Hypervisors
  b) 10.10.0.0/16
  c) 1.2.222.0/24

3.3 Blue Team

3.3.1 Setup

- Up to 4 registered team members are allowed, comprising solution provider and system integrator (no restriction on make up of team[3]); ID passes issued by iTrust will be used for identification and access
- Each Blue Team is given up to 3 working days to set up and test their defence mechanisms at SWaT. Booking for set up scheduling is on a first-come-first-served basis, and can be done through a booking form (to be announced.)
- iTrust will not provide any additional hard/software beyond what is already available in the control room
- iTrust will not be responsible for any loss or damage to the equipment before, during and after the event (installed CCTVs notwithstanding)

---

[2]Type G, British BS-1363 wall outlet, 220-240 volts AC @ 50 Hz
[3] E.g., the make up can be 2 from solution provider and 2 from SI, or 3 from solution provider and 1 from SI

SINGAPORE UNIVERSITY OF
TECHNOLOGY AND DESIGN

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

iTrust
Centre for Research
in Cyber Security

- Any system modification required for setting up the defence mechanism is subject to, and supervised by, the testbed engineer
- Electric power[2], tables and chairs for up to 4 persons and a separate network for internet uplink will be provided
- All system modifications must be removed and the testbed restored to its original and working condition within 2 weeks after the event

3.3.2 Detection

- Each Blue Team shall provide the logs of their detection mechanism, as well as a post-event report detailing the detection

4. Scoring System

A structure to classify different attacks, and define how such attacks are scored, is described below. In general, the scoring, *s*, for an attack is computed based on three factors *p, g* and *c:*

$$s = p * [(g_{p1}*c_{p1} +… g_{pn}*c_{pn}) + (g_{s1}*c_{s1} +… g_{sn}*c_{sn})]$$

Where:

- p = point of entry modifier
- g = points awarded based on whether specific physical process or sensor data goals can be manipulated; and
- c = control modifier that is awarded based on the extent of control the attacker has in manipulating the physical process or sensor data goals

4.1 Point of Entry Modifiers, p

- Factor = 1: Entering via ZCC to launch attack on SWaT
- Factor = 0.8: Launching attack directly from SWaT

4.2 Physical Process Goals, g_p: Control over physical process

- 100 points: Motorised Valves (open/close/transitioning/intermediate)
- 130 points: Water Pumps (on/off)
- 145 points: Pressure
- 160 points: Tank fill level (true water amount, not sensor reading)
- 180 points: Chemical dosing

4.3 Sensor Data Goals, g_s: Control over sensor readings

- 100 points: Historian values
- 130 points: HMI/SCADA values
- 160 points: PLC values
- 200 points: Remote I/O values

4.4 Control modifiers, *c*

- The control modifier determines the extent of control the attacker has over the goals
- The scoring is as follows:
  - 0.5, if the attacker can only randomly influence the process (value and time)
  - 1.0, if the attacker can precisely influence the process or sensor value to a *target value* chosen by the judges

5. Process for Launching Attacks

All attackers must adhere to the following process for carrying out their attacks:

5.1 Scope of attacks

We currently have the following blacklist for attacks:

- Server rack: The server rack should not be attacked through physical layer
- Historian: Do not directly try to compromise the historian. We use it to record data for later analysis. Feel free to manipulate data sent to the historian
- General electric supply, fire alarm systems etc.: Please do not manipulate the overall setup on a scale that affects more than the testbed setup (e.g., trigger university-wide fire alarm or similar).

5.2 Preparation phase

- Set up their attacks, but not carry them out
- Document the attack steps and provide them to the judges

5.3 Transition phase

Declare their attack goal(s) to the judges:

- Achieve which physical or sensor goal?
- Extend of control over the goals (judges will provide target value to achieve)
- How long is the attack expected to take?

5.4 Attack demonstration phase

- Attacks are conducted under monitoring of judges and lab engineer
- Judges declare when goal is met
- If there is more than one attack, another preparation and transition phase will follow

5.5 Resetting phase

- Once all attacks have been completed by a team or after 4 hours, whichever is earlier, the lab engineer resets the testbed to its original slate

6. Funding & Prizes

6.1 Partial funding is provided for shortlisted Red Teams as follows:

   a) Round-trip and most direct economy fare tickets for up to 2 registered members (booked by iTrust[4]); and

   b) Up to 7 nights' accommodation (one twin room with breakfast) at Park Avenue Changi Hotel, which is about 10 mins' walk to SUTD. **The applicable dates are between 24 Aug 2019 and 30 Aug 2019 only;** participants who wish to check in before 24 Aug 2019 or check out after 30 Aug 2019 will bear their own cost.

6.2 Local transport, visa and passport renewal fees and travel insurance are not covered. It is the participants' sole responsibilities that they have the proper documentation to travel and enter Singapore. Please refer to the Immigration Checkpoint Authority's website for the most up to date regulations. In the event that they are barred from entry, iTrust may seek compensation for the flight and/or hotel cancellation charges and penalties, whether in part of in full. Participants are also encouraged to purchase travel insurance coverage.

6.3 The top three Red Teams will receive cash prizes of S$500, $300 and $200 respectively. All Red Teams will receive a certificate of participation as well.

6.4 This event is supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme and administered by the National Cybersecurity R&D Directorate.

---

[4] We will request for a copy of your passport and contact details for flights booking; Personal data in Singapore is protected under the Personal Data Protection Act 2012 (PDPA)