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 ("Exercise") 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 Exercise, Red Teams will have a chance to attack the Secure Water Treatment (SWaT) testbed, at SUTD. Concurrently, 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 attempt to gain access to reach the testbed. Additional points are given if this route is taken (see para. 4.1.)

2. Registration

Red and Blue Teams' participation is by invitation only. Please register your participation using the given link that was provided in the invitation email. The deadline to confirm your registration is **31 Jul 2019 (Wed), 1800 hrs.**

3. Schedule

The attack schedule will be determined by drawing lots and will be announced on the website two weeks before the Exercise. Red Team leaders will also be notified via email.

Table 1: Summary of the activities and attack schedule

Date	Time	Activity & attack schedule	Involvement
31 Jul (Wed)	18:00	Registration for Red & Blue Teams closes	All Red & Blue Teams
1 Aug – 25 Aug	09:00 – 18:00	Setting up defence mechanisms in SWaT + learning plant behaviour (if applicable)	All Blue Teams
26 Aug (Mon)	09:00 – 11:00	Session 1: Introduction to SWaT & ZCC + Q&A	Red Teams 1 to 4 (non-mandatory)
	11:00 – 13:00	Session 2: Introduction to SWaT & ZCC + 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 (Wed)	09:00 – 13:00	Attack by Red Team 4	Red Team 4 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

3.1. Set Up Phase: 1 – 25 August

3.1.1. Each Blue Team is given up to 3 working days to set up its defence mechanism in SWaT, assisted by the lab engineer. Booking for set up scheduling is on a first-come-first-served basis, and can be done through a booking form on the website (to be announced.)

3.1.2. Once all defence mechanisms have been set up, iTrust will run the testbed under "normal plant operating condition" for 3 days. This gives defence mechanisms time to learn the plant behaviour, where necessary/applicable.

3.1.3. iTrust will not provide any additional hard/software for installation/setting up

3.1.4. iTrust will not be responsible for any loss or damage to the equipment before, during and after the Exercise (installed CCTVs notwithstanding)

3.1.5. Any system modification required for setting up the defence mechanism is subject to, and supervised by, the testbed engineer

3.2. Walkthrough Phase: 26 August

3.2.1. All Red Teams are invited to visit the SWaT testbed to familiarise with SWaT and ZCC setup, 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.

3.2.2. ZCC is a full-fledge virtual 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.

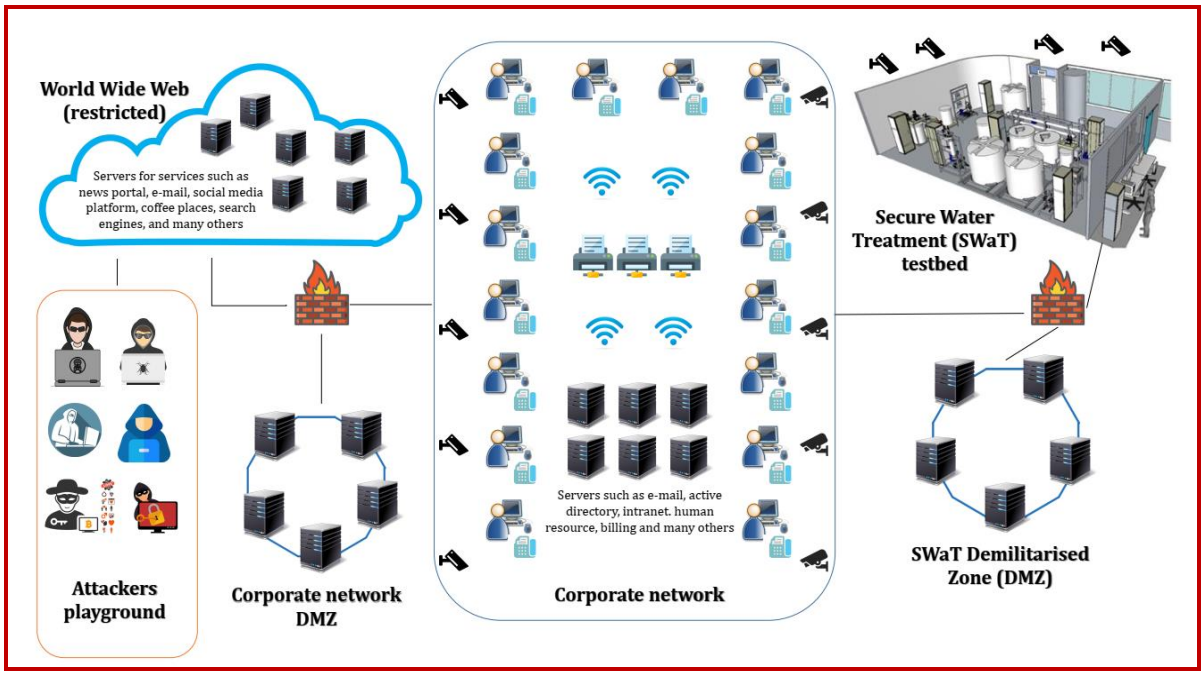

Figure 1: High-level Architecture of ZyCron Cyber City

3.3. Attack Phase: 26 – 30 August

3.3.1. 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].

3.3.2. 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.

3.3.3. Concurrently, an array of detection mechanisms is deployed in SWaT by the Blue Teams before the Exercise. These mechanisms will monitor and 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. Blue Teams may also use this opportunity to demonstrate their defence capabilities to observers.

[1] Light refreshments will be provided

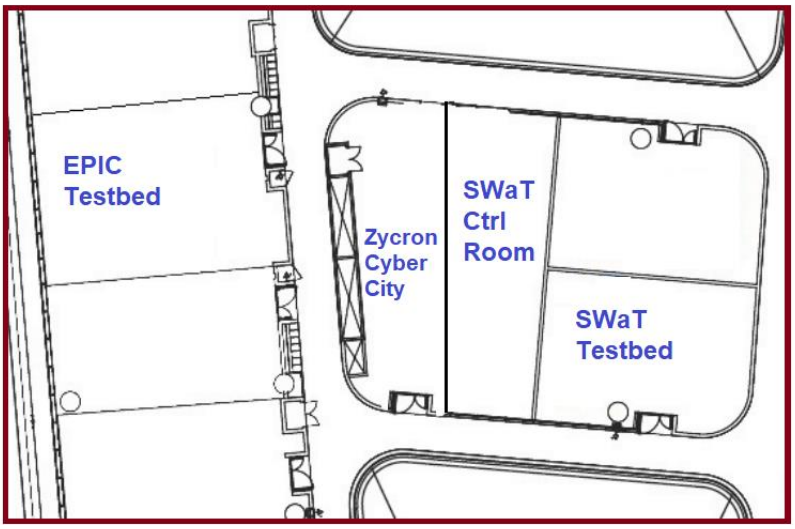

Figure 2: Venue for CISS 2019

4. Rules & Regulations

4.1. General

4.1.1. All participants in this Exercise 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 Exercise by the organisers for purposes of research and producing editorial content for publicity.

4.1.2. 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 permitted thereafter.

4.2. Red Team

4.2.1. Setup

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

[2] Type G, British BS-1363 wall outlet, 220-240 volts AC @ 50 Hz

- 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
- Provide a copy of their software tools and/or source codes (used during the attack) to Exercise's organisers for research purposes

4.2.2. 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, Exercise's organisers and running of the Exercise 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

4.3. Blue Team

4.3.1. 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
- 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 Exercise

4.3.2. Detection

- **There shall be no efforts made to prevent, halt or thwart any attacks launched by the Red Team**
- Each Blue Team shall provide the logs of their detection mechanism, as well as

[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

a post-Exercise report detailing their detections

4.4. Observers & Technical Reporters

4.4.1. Observers from government agencies may be present to witness the attack and defence capabilities of the teams. To ensure fairness and minimise disruptions, interactions between observers and the active Red Team will be kept to a minimum. However, observers can freely interact with Blue Teams to better understand their detection capabilities.

4.4.2. Technical reporters comprising iTrust staff and researchers will be attached to the active Red and Blue Teams to record and report the ongoing activities. These include, but are not limited to, photo taking and video recording, taking notes of how/when the attacks are launched and the interactions between judges and the active Red Team. These observations will then be distilled into an anonymised report at the end of the exercise for public sharing.

5. Scoring System

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

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

Where:

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

Example:
A Red Team launches an attack from SWaT directly (p = 0.8), and manages to exert control over the motorised valve (g_p = 100) and pressure (g_p = 145) to values determined by the judge (c_p = 1), but can only randomly control (c_s = 0.5) the PLC values (g_s = 160). The total score is thus:

s = 0.8 * [(100 * 1 + 145 * 1) + (160 * 0.5)]
= 260

5.1. Point of Entry Modifiers, p

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

5.2. 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

5.3. 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

5.4. Control modifiers, *c*

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

6. Process for Launching Attacks

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

6.1. 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).

6.2. Preparation phase

- Set up attacks, but not launch them
- Document the attack steps and inform the judges

6.3. Transition phase

Declare attack goal(s) to the judges:

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

6.4. Attack demonstration phase

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

6.5. Reset 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 state

7. Funding & Prizes

7.1. 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 ("block out dates")**. Participants

[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)

who wish to check in before or check out after the block out dates, including early check in/out on the block out dates, will have to bear their own cost.

7.2. Local transport (e.g., between airport to hotel and hotel to SUTD), passport renewal and visa fees and travel insurance are not funded. It is the participants' sole responsibilities that they have the proper documentation to travel to (including transit stops) and enter into Singapore. This includes permits/licenses/certificates to bring in any controlled/restricted equipment/device into Singapore, if any. Please refer to the Immigration Checkpoint Authority's and Singapore Custom's website for the most up to date regulations. In the event that participants are barred from travelling or entry, iTrust may seek compensation for the flight and/or hotel cancellation charges and penalties, whether in part of or in full. Participants are also encouraged to purchase travel insurance.

7.3. 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.

7.4. This Exercise 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.

8. Acceptance of Terms & Conditions

Participants who register for this Exercise is deemed to have read and accepted all the terms and conditions set out in this document.