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

Singapore University of Technology and Design

Contents

Version 7 (23 Jul 19)

1. Introduction

The Critical Infrastructure Security Showdown (CISS) 2019 ("Exercise") is the third run of iTrust's technology assessment exercise, dubbed the SWaT Security Showdown (S3) in 2016 and S317 in 2017[1]. This year's Exercise is sponsored by the National Research Foundation. Organised by iTrust, the CISS 2019 is held at SUTD, with the setup phase from 1 to 25 August, walkthrough phase on the morning of 26 August, and the attacking phase from 26 August (afternoon) to 30 August. Red and Blue Teams from academia and industry are invited to participate in this Exercise.

2. Objectives of Exercise

2.1 iTrust is a Centre for Research in Cyber Security. The Exercise allows our security researchers to: (1) empirically test defence mechanisms developed in-house against skilled attackers (2) be exposed to and discover new attack vectors to defend against; and (3) strengthen existing defence mechanisms.

2.2 Red Teams will have a unique chance to attack the Secure Water Treatment (SWaT), a 5 US gallon/min industrial water treatment testbed. 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. Additional points are given if this route is taken (see para. 6.)

2.3 Concurrently, Blue Teams will be able to showcase their detection capabilities against cyber attacks. For the avoidance of doubt, the only objectives of this Exercise are mentioned in 2.1. It is not our aim of iTrust to assist the Blue Teams to uncover their inability to detect cyber attacks (nor why), if applicable.

3. Registration

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

4. Schedule

The attack schedule will be announced on the website two weeks before the Exercise. Red Team

leaders will also be notified via email. Table 1 summaries the activities and attack schedule.

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 – 2 Aug (Thurs – Fri)	15:00 – 18:00	Briefing for Blue Teams on SWaT and CloneHistorian (select one of two days)	All Blue Teams
5 Aug – 25 Aug	09:00 – 18:00	Setting up defence mechanisms in SWaT + learning plant behaviour (if applicable)	All Blue Teams (3 working days each)
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

[1] Anonymised reports from S3 and S317 can be downloaded here and here.

Date	Time	Activity & attack schedule	Involvement
	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

4.1 Set Up Phase: 1 – 25 August

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

4.1.2. 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.

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

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

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

4.2 Walkthrough Phase: 26 August

4.2.1. 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.

4.2.2. 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 ZCC. As an IT environment ZCC is not set up with best practices i.e. it is

intentionally built with minimum security features and contains vulnerabilities for Red Teams to explore and exploit. A high-level architecture of ZCC is presented in Figure 1.

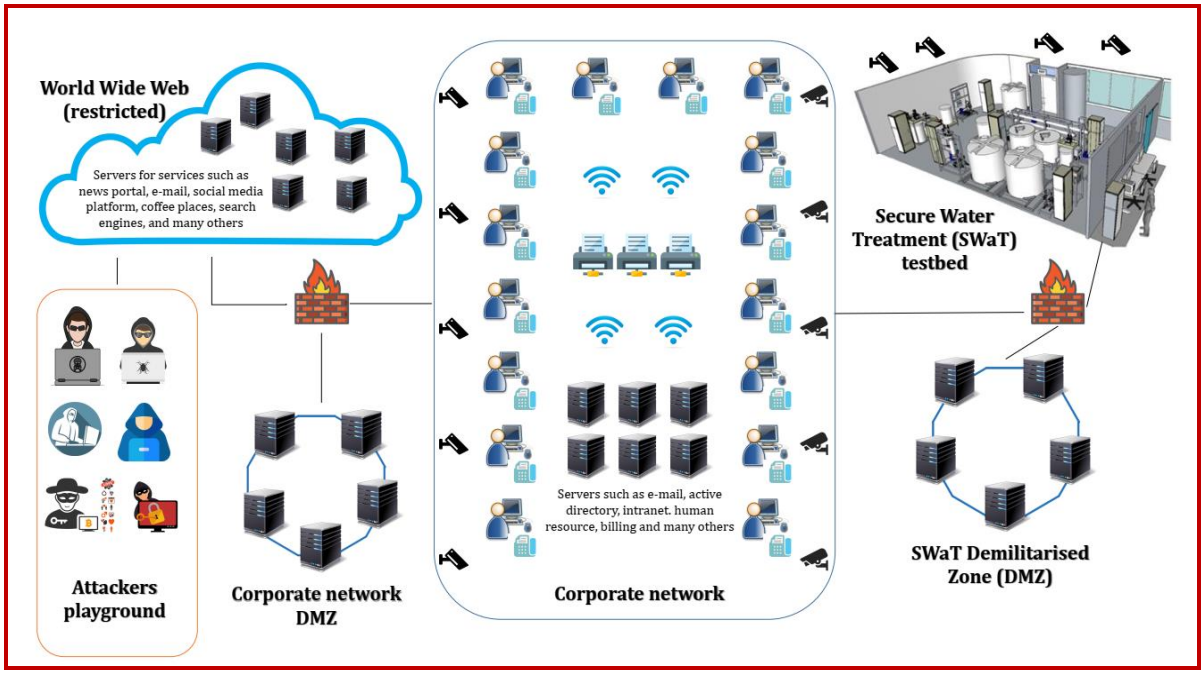

Figure 1: High-level Architecture of ZyCron Cyber City

4.3 Attack Phase: 26 – 30 August

4.3.1. 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[2].

4.3.2. 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.

4.3.3. 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

[2] Light refreshments will be provided

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.

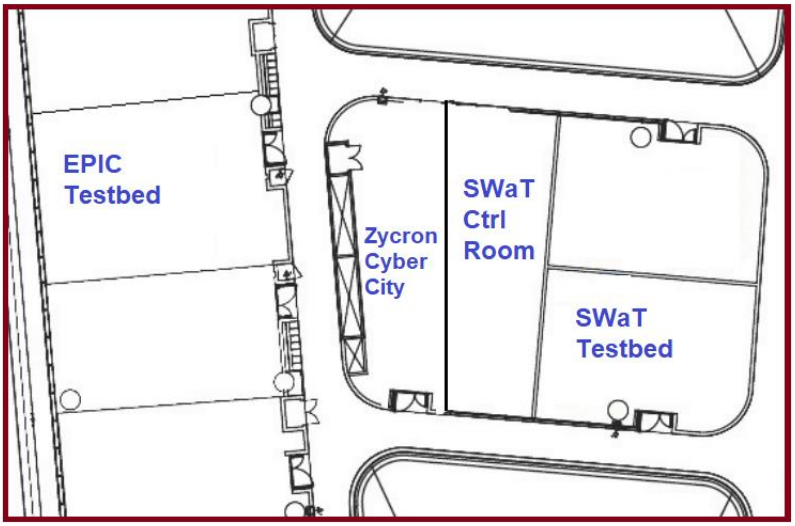

Figure 2: Venue for CISS 2019

5. Rules & Regulations

5.1 General

5.1.1. All Red and Blue Teams (collectively "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 iTrust for purposes of research and producing editorial content for publicity.

5.1.2. 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.

5.2 Red Team

5.2.1. Setup

- Up to 4 registered team members are allowed; ID passes issued by iTrust will be used for identification and access
- Electric power[3], tables and chairs for up to 4 persons and a separate network for

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

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

5.2.2. 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 Participants, iTrust 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

5.3 Blue Team

5.3.1. Setup

- **For teams whose defence mechanisms require querying data from the Historian, they must to do so via Virtual Machines (VMs) developed by iTrust, dubbed CloneHistorian.** This ensures that the detection efficiency and speed are not affected as a result of multiple defence mechanisms querying data from SWaT's Historian. More information on CloneHistorian is given in Annex A. A briefing has also been arranged on 1 and 2 Aug for Blue Teams to better understand CloneHistorian.
- Up to 4 registered team members are allowed, comprising solution provider and system integrator (no restriction on make up of team[4]); 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

[4] E.g., the make up can be 2 from solution provider and 2 from SI, or 3 from solution provider and 1 from SI

- All system modifications must be removed and the testbed restored to its original and working condition within 2 weeks after the Exercise

5.3.2. 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 a post-Exercise report detailing their detections

5.4 Observers & Technical Reporters

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

5.3.4. 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 interactions between judges and Participants. These observations will then be distilled into an anonymised report at the end of the Exercise for public sharing.

6. Scoring System for Red Teams

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

6.1 Point of Entry Modifiers, *p*

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

6.2 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

6.3 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

6.4 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

7. Process for Launching Attacks

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

7.1 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).

7.2 Preparation phase

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

7.3 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?

7.4 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

7.5 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

8. Funding & Prizes

8.1 Fundable Items

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[5]); and
b) Up to 6 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 25 Aug 2019 and 30 Aug 2019 inclusive ("block out dates")**. Participants 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.

8.2 Non-fundable Items

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. If Participants are barred from travelling or entry, iTrust may seek compensation for the flight and/or hotel cancellation charges and penalties, whether in full or in part. Participants are also encouraged to obtain travel insurance.

8.3 Prizes

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.

8.4 Sponsor

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.

9. Intellectual Property

iTrust agrees that no transfer of the Participant's intellectual property rights is granted or implied by its participation in this Exercise.

[5] 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)

10. Acceptance of Terms & Conditions

Participants who register for this Exercise are deemed to have read and accepted all the terms and conditions set out in this document. iTrust reserves the right to change these terms and conditions at any time up until the Exercise, without prior notice.

Annex A: Information on CloneHistorian

To ensure a smooth Blue Team experience, iTrust has installed an in-house load balancer – CloneHistorian – to get access to the Historian data in real-time. Blue Teams which need to query data from SWaT's Historian must do so via CloneHistorian.

The CloneHistorian acts as a Client for the primary Historian and a Server for the Defenders. Blue Teams will be clients of this CloneHistorian. All the requests from the BlueTeam will be cached in advance on the CloneHistorian, hence the responses/replies are served in the fastest way possible. In this way, CloneHistorian acts as a Content Delivery Network. There are several Virtual Machine instances of CloneHistorian running simultaneously, which make the whole system act as a load balancer as well. Figure 3 explains the architecture of CloneHistorian.

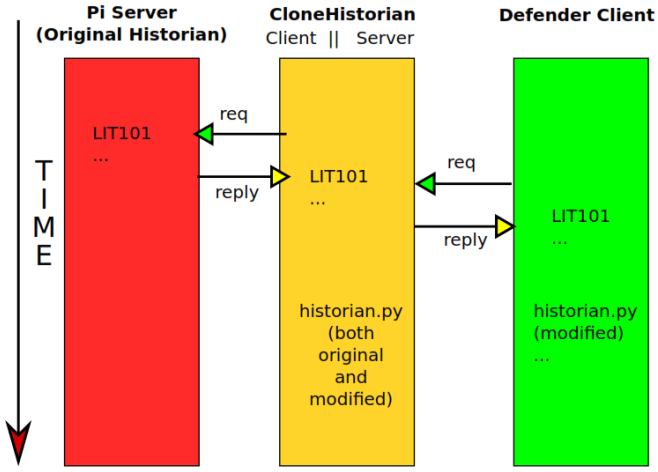

Figure 3: CloneHistorian architecture

Connecting to CloneHistorian is no different from connecting directly to the Historian. Its advantage is that it enables iTrust to decongest the network and prevent Blue Teams from slowing one another down during the Exercise. CloneHistorian can scale up to smoothly servicing as many concurrent Blue Teams as required. It has gone through rigorous stress-testing and fine-tuning using different scenarios to meet the expected load during the Exercise, and is already being used by iTrust.

iTrust will provide programming examples to get values of all the sensors, actuators, and other-related information in real-time (the application programming interface will be in Python).