MEng Innovation by Design
2019/2020 Ideate-Prototype-Realize


SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

G R Saravanan | Student
Jian Ying Zhou | Advisor

Background

Industrial work environment is changing. Technology is ever-present in virtually every kind of industry today, dramatic changes of all are taking place in our factories and other industrial environments. Industrial IoT (IIoT): they are used across multiple industries including but not limited to Electricity, Nuclear, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, Smart cities, Smart houses, Pharmaceutical Industries, and discrete manufacturing.

Attacks on Industrial IoT (IIoT) devices, exploiting inherent vulnerabilities, have intensified over the last few years. Recent large-scale attacks, validate concerns about the security of IIoT devices. To find and avoid this kind of attacks, we suggested to create a Honeypot architecture. Honeypots are designed to purposely engage and deceive hackers and identify malicious activities performed over the Internet.

Aim

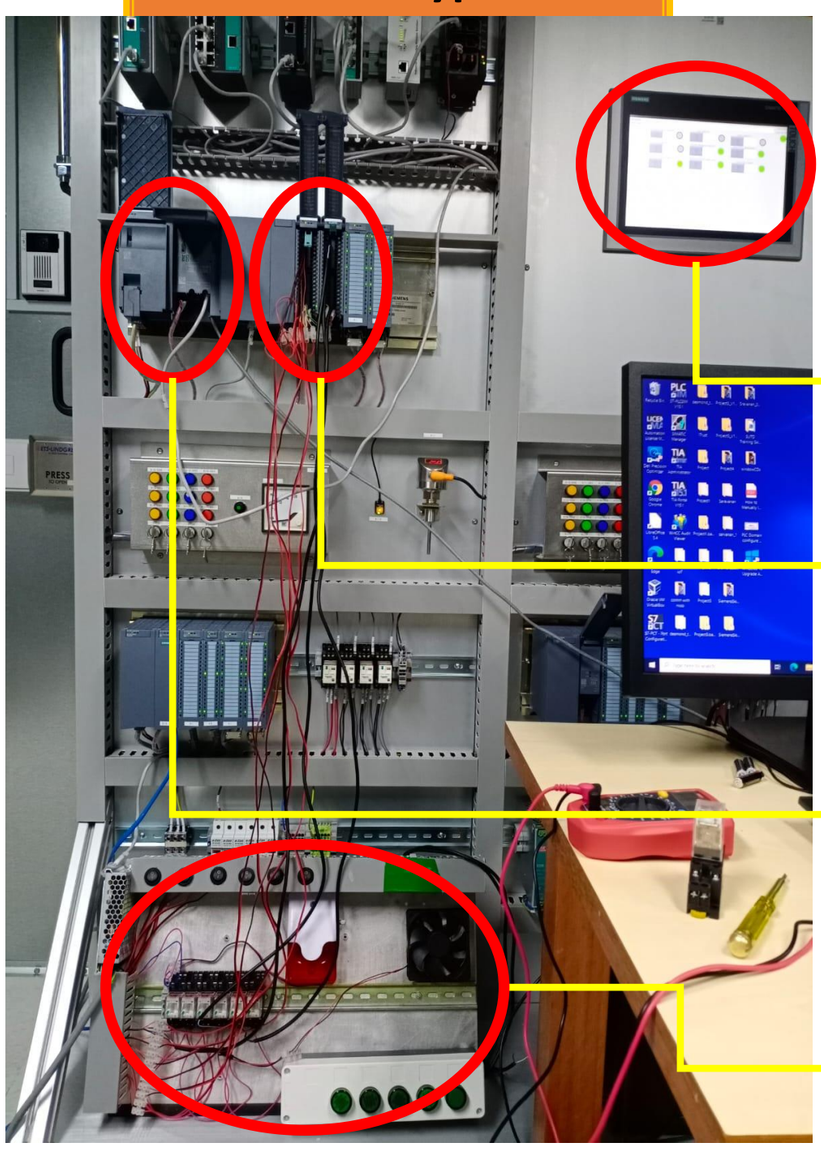
The goal is for those Industrial Automation devices, such as PLC to be discovered and exploited by attacks on the Internet, thereby revealing unknown vulnerabilities. For detection and examination of potentially malicious traffic, we devise two analysis strategies:

- given an outbound connection from honeypot, backtrack into network traffic to detect the corresponding attack command that caused the malicious connection and use it to download malware,
- perform live detection of unseen URLs from HTTP requests using adaptive clustering. We show that our implementation and analysis strategies can detect recent large-scale attacks targeting Industrial Internet of Things (IIoT) devices with overall low cost and maintenance effort.

Focus

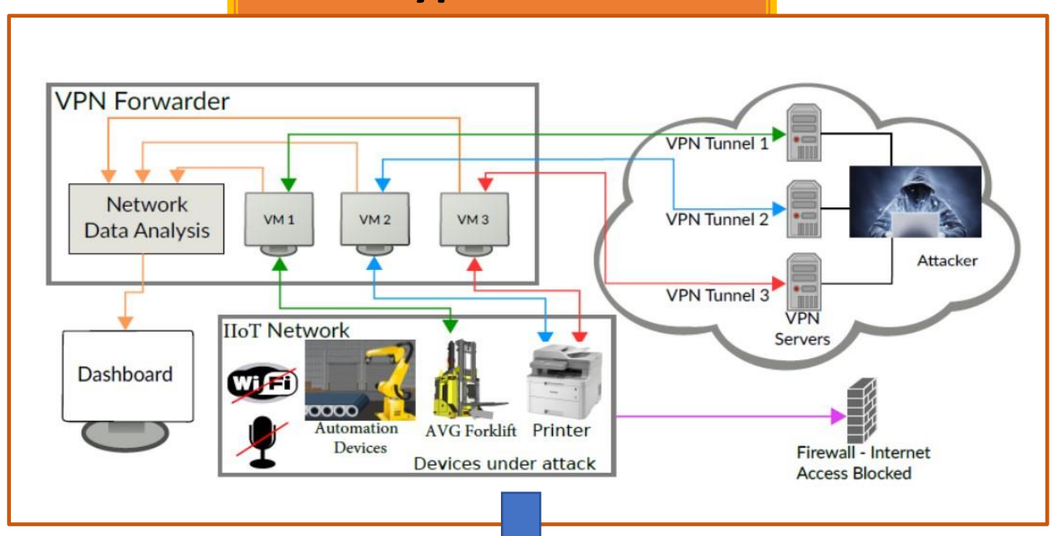
- Find a most vulnerable Industrial Automation devices such as PLC and design an industrial Automation architecture (Physical or Stimulated) and connect with this Honeypot architecture to detect the Industrial attacks.
- Design of a honeypot framework that incorporates Industrial Internet of Things (IIoT) devices for high interaction, utilizing low-cost commercial VPN providers
- An implementation of the proposed framework, demonstrating an automated, scalable, and economical approach to integrate IIoT devices
- Two live traffic analysis methods to detect large-scale attacks and subsequently 0-day vulnerabilities in IIoT devices using our honeypot infrastructure

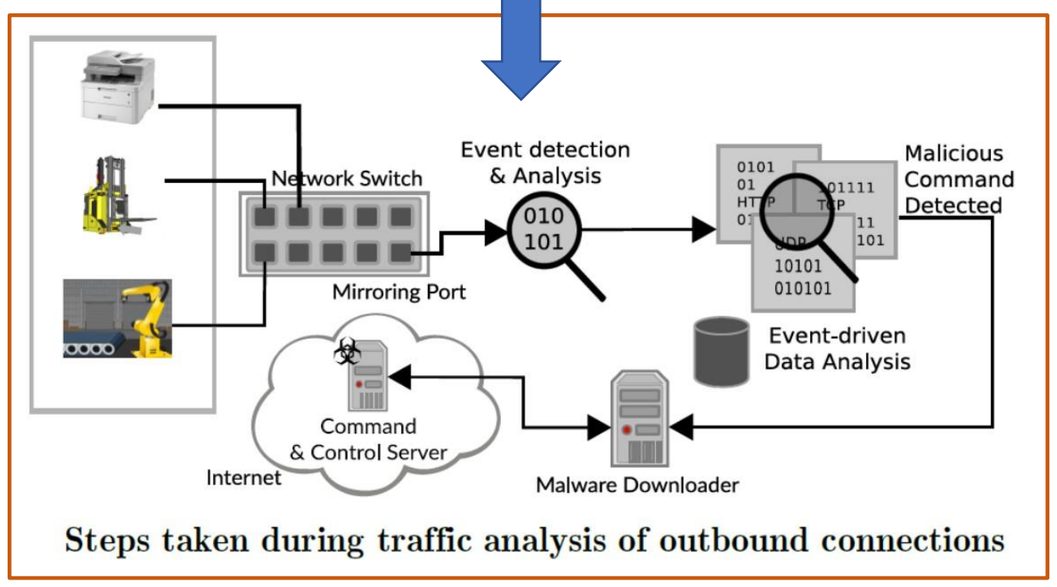
Prototype



- Smart Home Prototype is completed and controlled by PLC through HMI. Finally the Prototype is connected with Honeypot through PLC port.
- HMI Programming Completed, Necessary buttons are created to ON/OFF the devices.
- Input & Output Module Connected with Prototype through Switches & Relays.
- PLC & HMI Programming synchronized with workstation TIA portal.
- PLC Port connected with Honeypot and exposed for attackers.
- Prototype devices are synchronized with the PLC Input & Output module.

Honeypot Network





Steps taken during traffic analysis of outbound connections

IPR Conclusion

<u>Ideate</u> - Discovered the topic and proposed potentially innovative ideas about Industrial Automation device to connect with Honeypot for Intrusion detection, through literature reviews, benchmarking, ideation techniques, design of the architecture, on how to integrate the Automation device to the IoT honeypot framework.

<u>Prototype</u> - Developed Smart Home Prototype using Highly Vulnerable Automation Device (such as Siemens PLC) and connected with Honeypot Network.

<u>Realize</u> - Concluded the study about "Detect the attacks to Industrial Automation device" with some proof-of-concept of the ideas developed and prototyped. Helps uncovering vulnerabilities and driving innovation in developing defensive tools and frameworks. All this study and experiment will be used to prepare my thesis.

SUTD-MIT INTERNATIONAL DESIGN CENTRE (IDC) | jtc Breaking New Ground | LEE KUAN YEW CENTRE FOR INNOVATIVE CITIES | SUTD SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN Temasek Laboratories | iTrust Center for Research in Cyber Security