Security hands on and current issues in industrial systems

Duration: 15 hours

Material: All slides and additional material will be available at: https://gitlab.com/wild_boar/phd_sec_course

Location: Sala Riunioni DISI, Viale del Risorgimento, 2
https://www.google.it/maps/place/DISI+-+Dept.+of+Computer+Science+and+Engineering/@44.4878745,11.3305258,19z/data=!4m5!3m4!1s0x477fd4eddbbc43eb:0xe66cdb8a7e8f5eb5!8m2!3d44.487854!4d11.3308128

Overview

Cybersecurity is one of the main trends of recent years. While being extensively addressed in "consumers" scenarios, the security of industrial systems is not very advanced and it poses other problems such as legacy devices, time constraints, usable security for installation of devices, devices not connected to the internet, physical security, safety constraints, etc.

This field has never been deeply analyzed, since these kinds of devices were thought and built in “closed” networks, where the only possible attacks were physical ones. With the advent of the fourth industrial revolution (Industry 4.0), these systems have been exposed to the public domain and the attack surface, as a consequence, it exploded.

There is indeed the need of a strong security paradigm for these systems to contrast attacks which are more frequent every day.

The goal of this course is to give a clear view on the implementation and research questions of cybersecurity on industrial systems. We will expose which are the current research directions and what research can do to meet with industry security standards from our industrial experience and research points of view.

Day 1: 04/07/2022 09.00-13.00
Sala Riunioni DISI Viale del Risorgimento, 2
Introduction

2h: Main concepts about Security
- Kill Chain
- Red vs Blue team
- Security areas (critto, pwn, network, web, hardware, …)
- State-of-the-art
- Future Challenges
- Safety vs Security (Introduction)

2h: Industrial Security
- Safety vs Security (SIL Level)
- Industrial System Scenarios (PLC, Automotive)
- I4.0 / I5.0 / Japanese Society 5.0
- Security Challenges IT
- Security Challenges OT (Famous Use Cases)
- State-of-the art defensive mechanism

Day 2: 14/07/2022 09.00-13.00
Sala Riunioni DISI Viale del Risorgimento, 2
Network (Blue Team/Defensive Security)

2h: Network Requirements
- Switch e router
- Spoofing
- Sniffing
- Crypto (HTTPS)
- Future: SDN / NFV / PDP / Microservices

2h: Industrial Protocols
- Ethernet (+ Ethernet / IP)
- Modbus
- DNP3
- TSN (PTP)
- CANBus (Automotive)
- OPC-UA
- VLAN + Hopping

Day 3: 18/07/2022 09.00-13.00
Sala Riunioni DISI Viale del Risorgimento, 2
Systems (Red Team/Offensive Security)

2h: Attacks over Infrastracture and HMI

- Client-Side
- Sever-Side
- Exploitation
- Defense

2h: Attacks and Software

- PWN
- Debug
- Reverse
- Challenges

Day 4: 25/07/2022 14.00-17.00
Sala Riunioni DISI Viale del Risorgimento, 2
Demo + assignment:

Goal of this last lecture will be to start discussion on how student's current research may fit, or apply over modern security research activites.

Student will have to present an assessment (see next Section), for the remaining time this lecture will include:

Recents Attacks, Demos and PoC

- CTF TEE
- Ranflood
- Shodan

Modern attack using ML techniques such as:

- Model Poisoning
- Adversial Beahvior Attack

Learning and assessment

The final assessment will consist of a report on practical security aspects, ideally on industrial applications. It can consist of one of:

- a description or implementation of an interesting (well-known) attack;
- an implementation of a test for a well-known attack;
- a report or implementation of a defence or analysis mechanisms;
- an academic (conference or workshop or journal) paper;
- an hacker (e.g. phrack, pagedout!, PoC||GTFO, hackinbo, defcon, blackhat, ...) article or presentation at the conference;
- a discovery (or the description of the research process) of a novel attack on industrial devices, with or without a CVE.

This assessment must be discussed with the instructors before producing it.