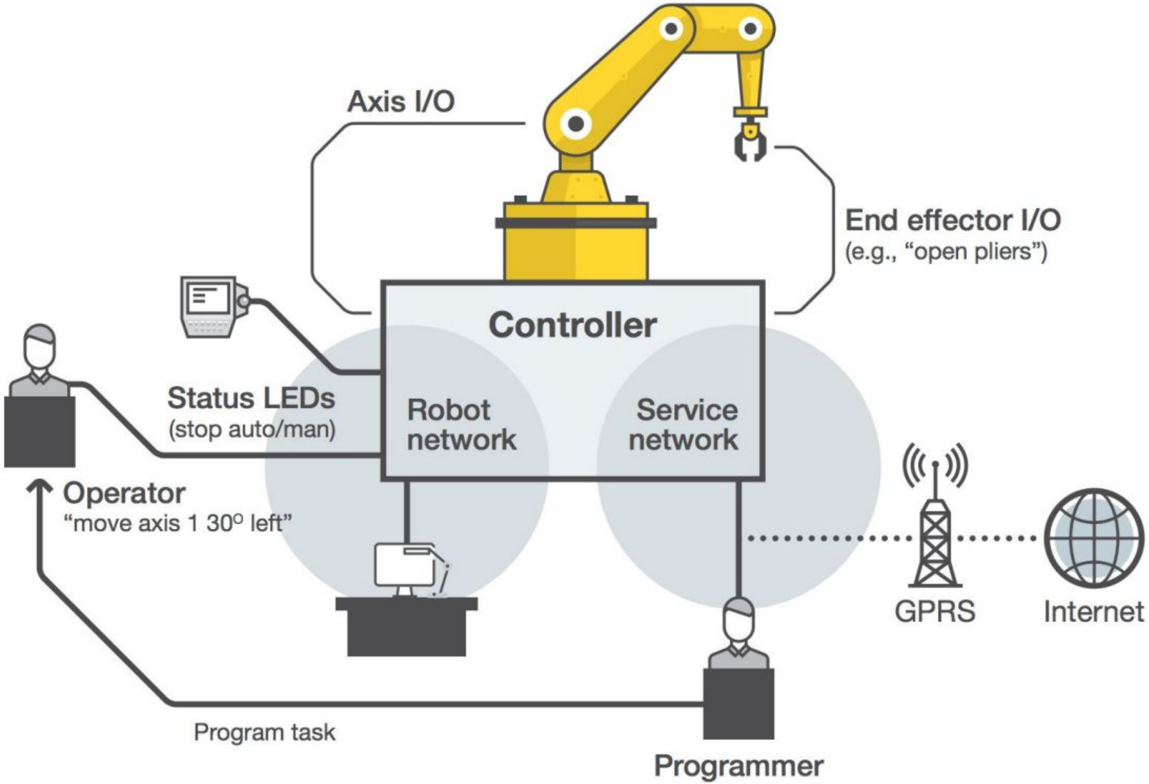
An experimental security analysis of an Industrial Robot Controller

Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, Stefano Zanero

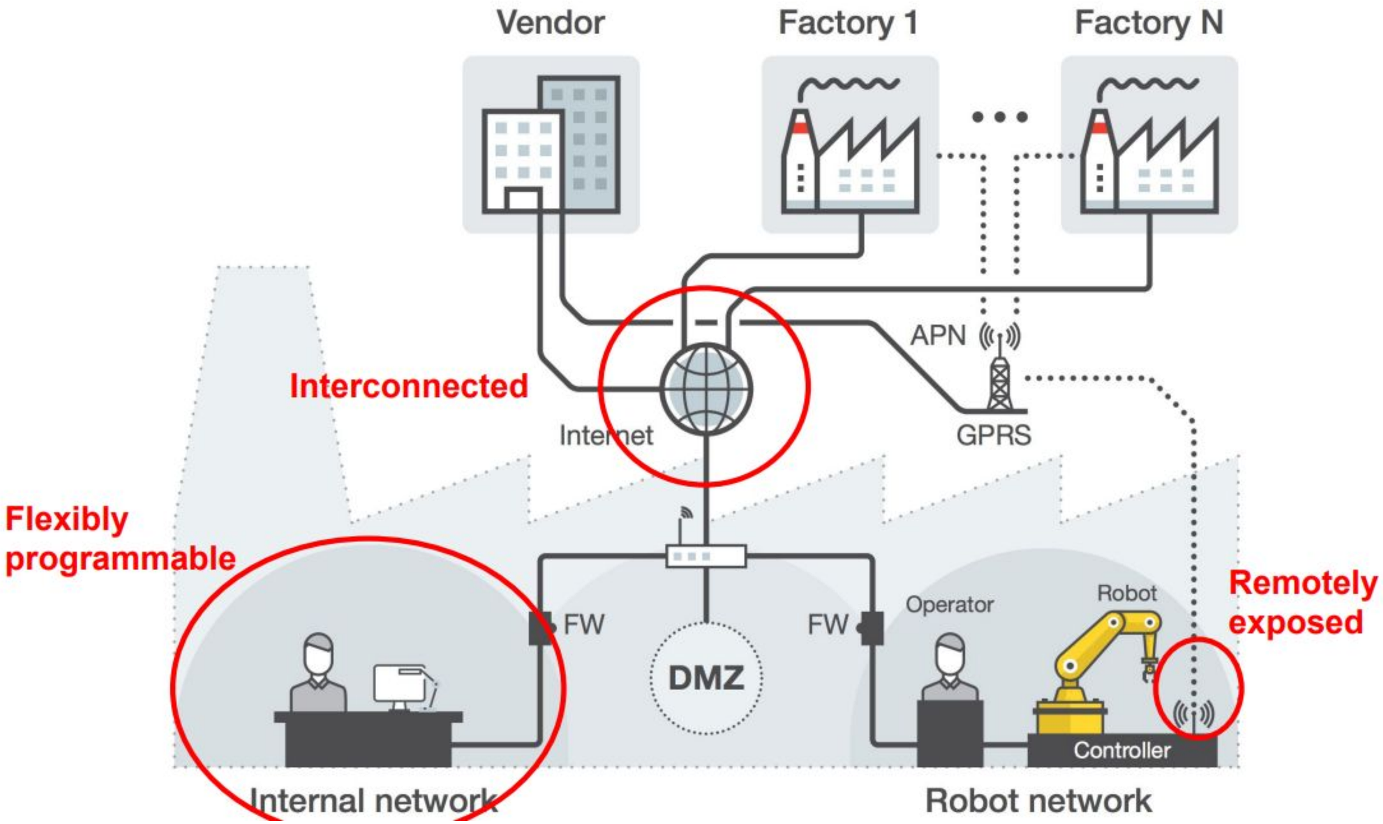
San José (CA), May 22nd, 2017 38th IEEE Symposium on Security and Privacy

Contents

Industrial Robot Controller



Motivations – Industrial 4.0 Trends



Motivations – Lack of Awareness

Survey: Robot users vs. system security

50 domain experts—users interviewed: 20 answers

- **28%*** access control policies *not enforced*
- **30%** robots accessible *over Internet*
- **76%** *never* performed a pentest
- **> 50%** not a *realistic* threat

* some users did not answer all the questions

Robot-specific attacks

Q. How do we define a robot-specific attack?

A. Need to find Requirements for robots (laws of robotics)

1. I/O Accuracy
   a. Read precise values
   b. Issue correct/accurate commands
2. Safety
   a. Never harm humans
   b. Correctly inform operator
3. Integrity
   a. No damage to the robot

Robot-specific Attack:

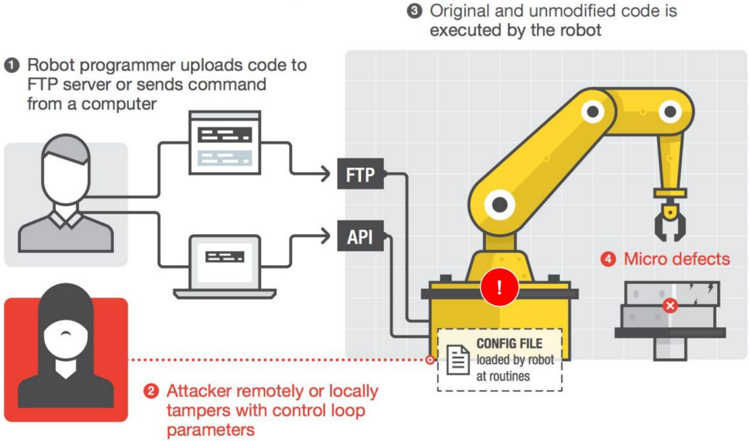
Digital-borne violation of any of these requirements

Robot-specific attacks

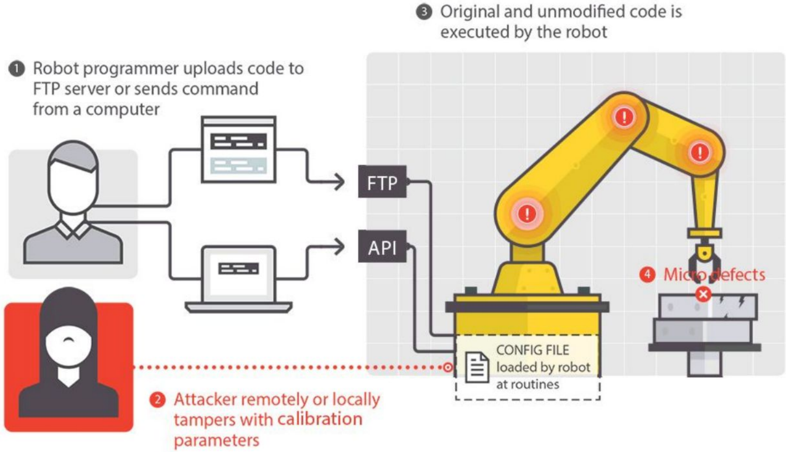
- Attacker Model
  - Target System: Industrial manufacturing robot
  - Goal: production outcome altering, physical damage, production plant halting, unauthorized access
  - Access Level: network attacker, remote exposure, physical attacker

Robot-specific Attacks

Attack 1: Control Loop Alteration

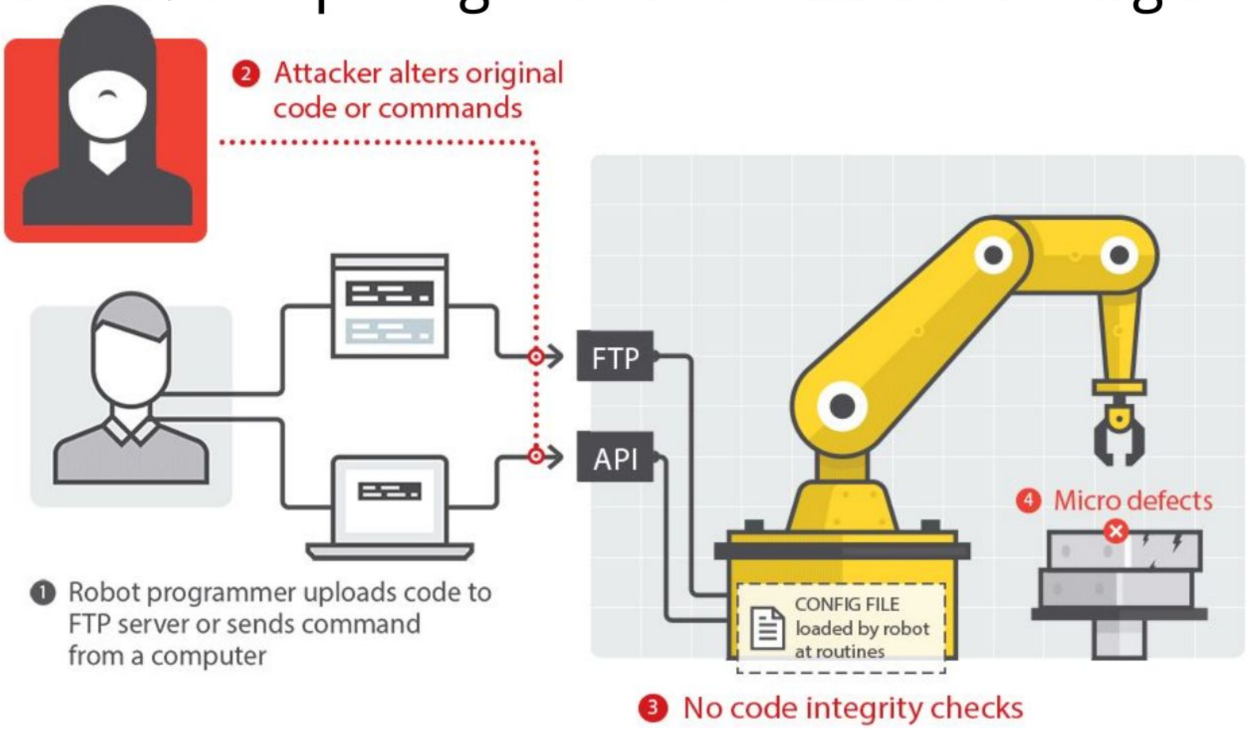


Attack 2: Tampering with Calibration Parameters



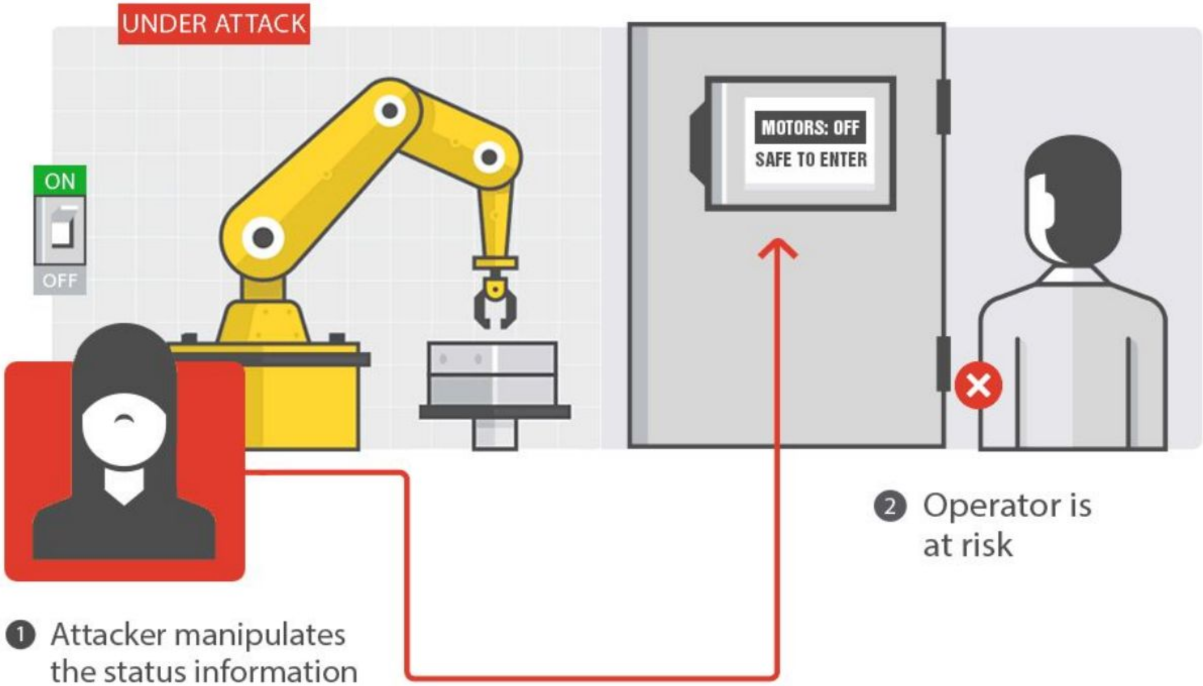
Robot-specific Attacks

Attack 3: Tampering with the Production Logic



Robot-specific Attacks

Attack 4 & 5: (Perceived) Robot State Alteration



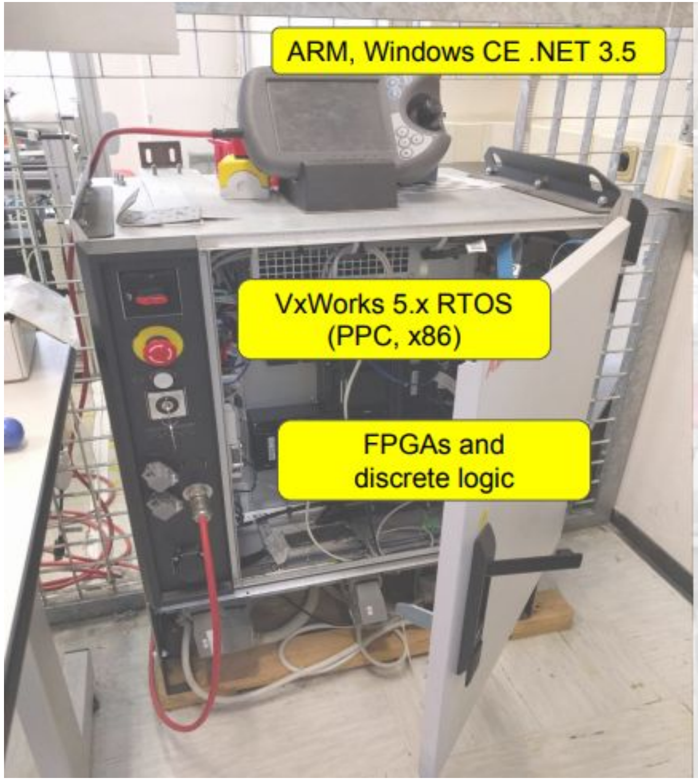
Robot-specific Attacks

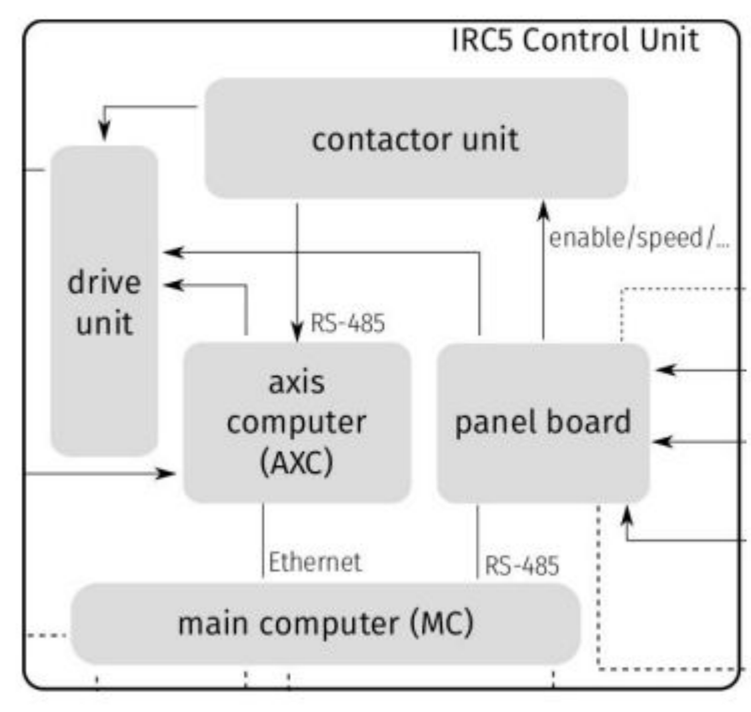
- From Attacks to Threats Scenarios

1) Production Plant Halting
2) Production Outcome Alteration
3) Physical Damage
4) Unauthorized Access
5) Ransom requests to disclose micro defects

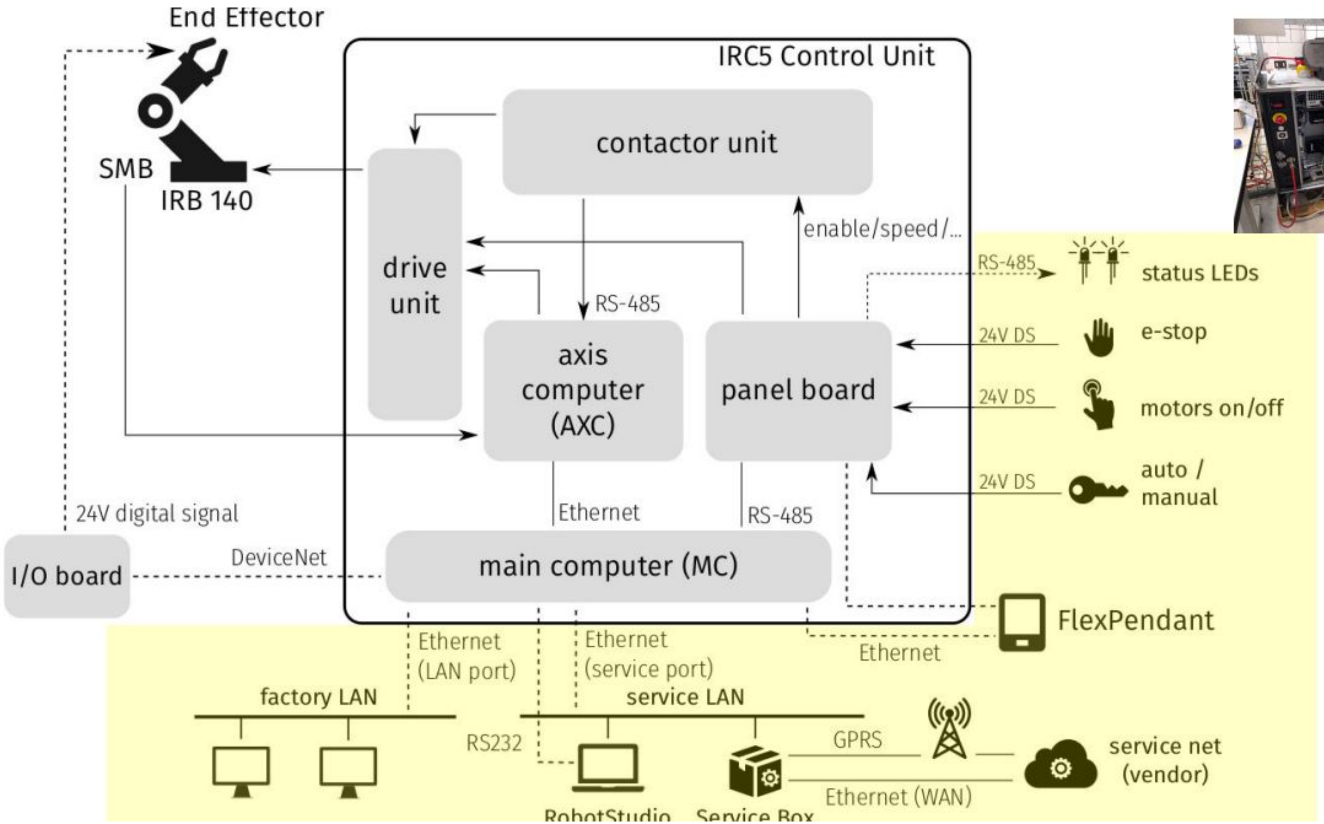
Case Study

Case Study


ARM, Windows CE .NET 3.5
VxWorks 5.x RTOS
(PPC, x86)
FPGAs and
discrete logic


IRC5 Control Unit
contactor unit
drive unit
enable/speed/...
RS-485
axis computer (AXC)
panel board
Ethernet
RS-485
main computer (MC)

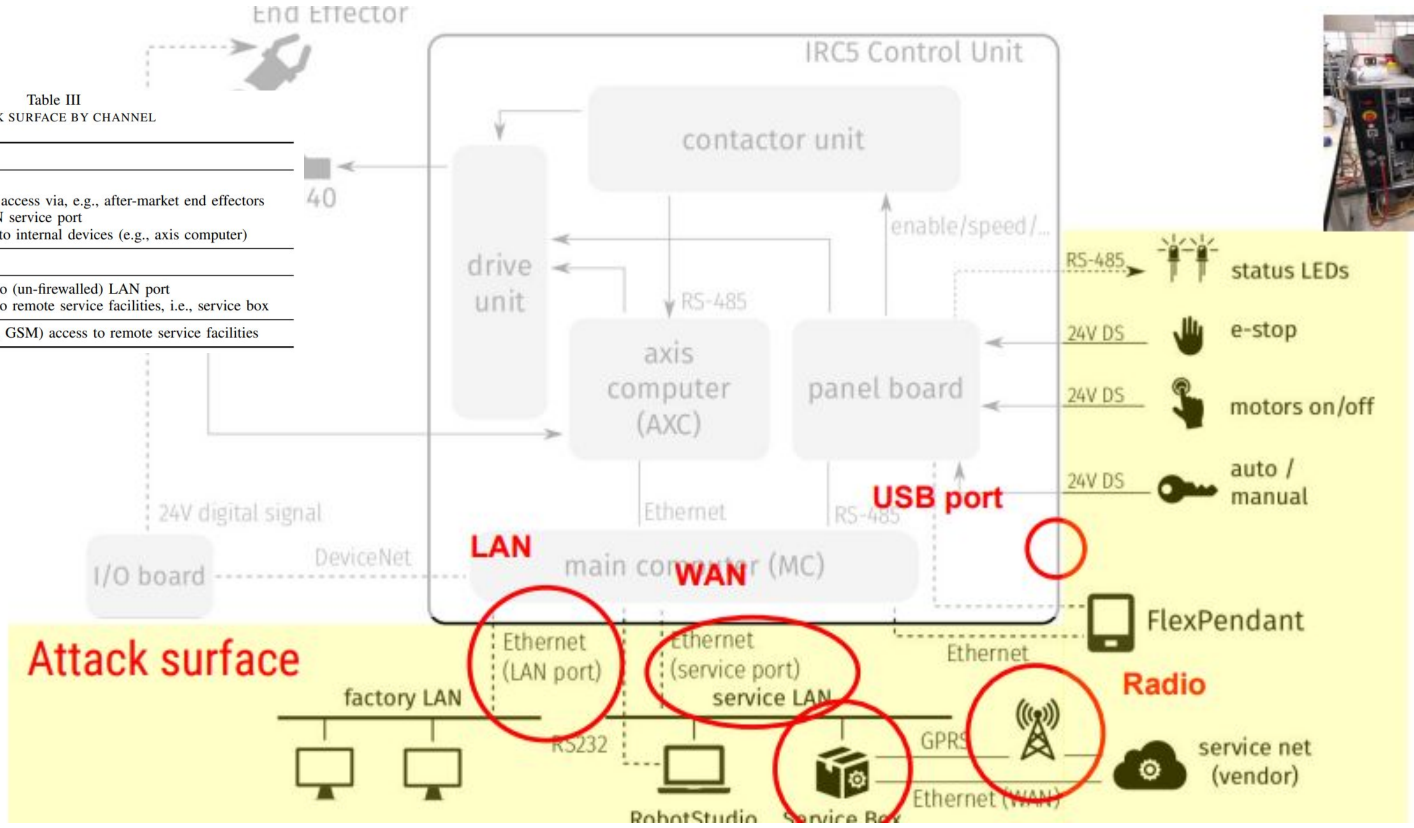
Case Study


End Effector
IRC5 Control Unit
contactor unit
SMB
IRB 140
drive unit
enable/speed/...
RS-485
status LEDs
RS-485
axis computer (AXC)
panel board
24V DS
e-stop
24V DS
motors on/off
24V DS
auto / manual
24V digital signal
Ethernet
RS-485
I/O board
DeviceNet
main computer (MC)
FlexPendant
Ethernet (LAN port)
Ethernet (service port)
Ethernet
factory LAN
service LAN
RS232
GPRS
service net (vendor)
Ethernet (WAN)
RobotStudio
Service Box

Case Study

Table III
ATTACK SURFACE BY CHANNEL

Access	Channel
Physical	- USB port - Industrial bus access via, e.g., after-market end effectors - Ethernet: LAN service port - Direct access to internal devices (e.g., axis computer)
Local	- LAN port
Remote	- WAN access to (un-firewalled) LAN port - WAN access to remote service facilities, i.e., service box
Wireless	- Wireless (e.g., GSM) access to remote service facilities



SYSSEC KAIST

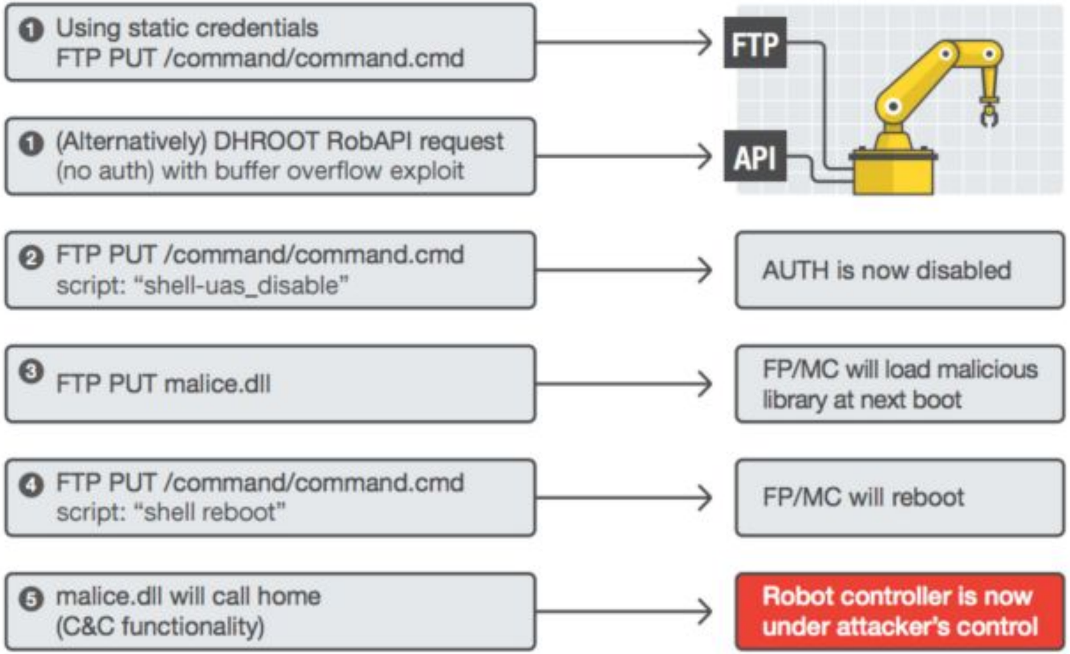
Case Study

- Vulnerabilities

a. **BOF leading to RCE** (ABBVU-DMRO-124641)
b. **BOF in FlexPendant** (ABBVU-DMRO-124645)
c. **BOF in /command endpoint** (ABBVU-DMRO-128238)
d. **Command Injection** (ABBVU-DMRO-124642)
e. **Authentication bypass** (ABBVU-DMRO-124644)

Case Study

- Full Controller Exploitation



Attack POCs

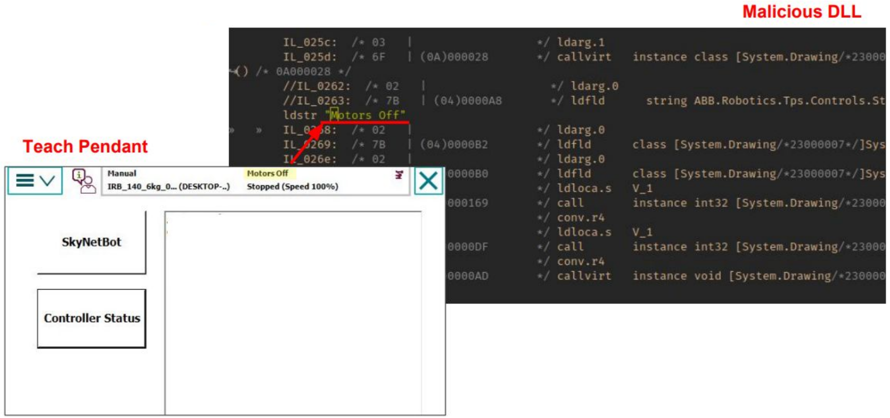
1) **Accuracy** Violation: PID parameters detuning (Attack 1) **DEMO**
2) **Safety** Violation: User-Perceived Robot State Alteration (Attack 4)
3) **Integrity** Violation: Control-loop alteration (Attack 1)

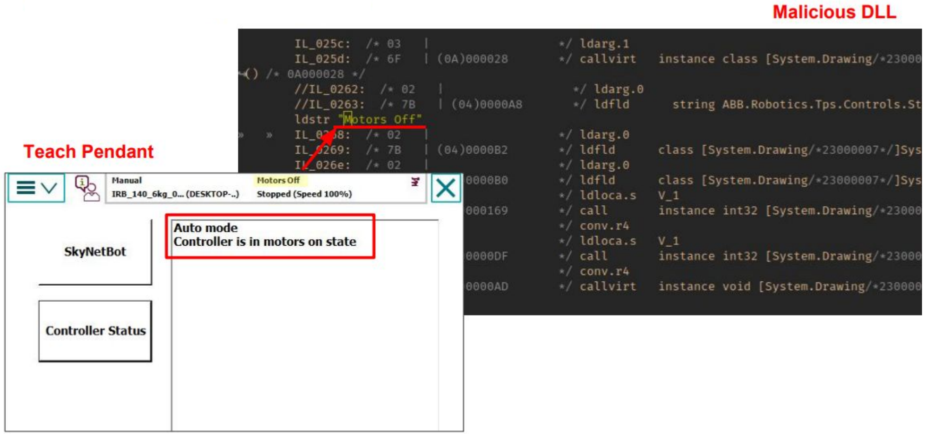
Attack POCs

- POC 1: Accuracy Violation

Attack POCs

❖ POC 2: Safety Violation





Attack POCs

- POC 3: Integrity Violation
  - Robot's arm collapse on itself
  - Motors substantially damaged

Quite a risky POC!
Verified with a robotics' expert

Discussion & Limitation

- Discussion
  - Lack of standards explicitly accounting for cyber-security threats
  - Security Measures and Challenges
    - Human interaction, Attack detection, System hardening, Program protection, etc.

- Limitation
  - Cost of Exploit Testing
  - Generality
  - Survey

Conclusion

- Conclusion
  - New standards, beyond safety issues
  - Attack detection and hardening
  - Secure collaborative robots
  - (Detailed countermeasures in the paper)

Best Questions

- **(Mumin Hasan)** What impact do robot-specific vulnerabilities have on broader factory ecosystems (e.g., other connected devices)? Could attackers pivot through compromised robots to access unrelated systems?

  (Jiwoo Suh) Attack scenarios on systems utilizing two or more robots and the cascading disasters this attack could cause.

- **(Jiwoo Suh)** Are there any attacks that could exploit vulnerabilities unique to the robot's hardware or operational behavior (this paper focus more on software vulnerabilities)?

More Questions

- **Defense methods in robot security**
  - Fuzz testing in a simulation environment to mitigate software and hardware vulnerabilities of robots
  - Strategies to make software-dependent systems immune to cyber-attacks
  - Machine learning techniques to detect and respond to anomalous behavior in industrial robots

- **Challenges of applying security to a new system**
  - Retrofitting legacy industrial systems with modern encryption and authentication mechanisms
  - Zero-trust security architectures for industrial environments, and trade-offs in terms of system complexity and performance
  - Balance the need for security patching with minimizing downtime
  - Difficulties to apply established software development practices to such systems
  - Reasons for the use of default credentials persist in industrial setups despite known risks. Factors discourage enforcing stronger authentication (e.g., cost, convenience)
  - Cost-benefit trade-offs of implementing mandatory firmware code signing and impact for the operational efficiency of robot programming

https://robosec.org/

Q & A

Thank you for listening :)

This material is adapted and refined based on the research paper and presentation by Davide Quarta et al., presented in IEEE S&P (2017)