Università degli Studi di Padova

SPRITZ
Security & Privacy
Research Group

HUMAN INSPIRED TECHNOLOGY
Research Centre

DIPARTIMENTO
MATEMATICA

Introduction to Cyber-Physical Systems and IoT Security

Alessandro Brighente

About me

Education

- M.Sc in Telecommunication Engineering
- Ph.D. in Information Engineering
- Visiting researcher at Nokia Bell Labs and University of Washington
- Assistant professor, Department of Mathematics

Research Interests:

Security and Privacy in

- Network Security
- Cyber-Physical Systems
- Distributed ledger technology

Contacts

- Mail: alessandro.brighente@unpd.it
- Website: https://www.math.unipd.it/~abrighen/

Basic Information

- **Language:** 🇬🇧
- **Credits:** 6 CFU
- **Schedule:** I semester (course schedule is published HERE).
- **Lectures mode:** you can attend the course at the University. Lectures will be also recorded and available in the Moodle platform.

Course Details

- The course will be on Wednesday and Friday
- Educational Offer link
- 6 credits = 48 hours = 24 lectures
- Stem URL: **https://stem.elearning.unipd.it/course/view.php?id=4703**

Course Details

- During classes, we will explore attacks and countermeasures for CPS and IoT security
- We will provide you some code and simulators to test attacks and gain some insights on specific applications

Fundamentals

- What is a Cyber-Physical System
- Security Requirements in CPS

Automotive Security

- The CAN bus protocol
- Error handling in CAN bus and bus-off attack
- Network attacks on CAN bus
- Keyless cars security and attacks to distance bounding protocols

Course Details

Autonomous Driving

- Introduction to controllers
- Levels of automation and modes of operation
- Attacks on controllers and countermeasures

Hardware Security

- Execution flow of modern processors
- Evict+Time, Prime+Probe, Flush+Reload
- Spectre and Meltdown attacks
- Side channel attacks

Course Details

Industrial Control Systems

- Industrial Control Network Protocols
- PLC and their functioning
- Attacks and countermeasures to industrial control systems

Drones

- Drone components and basic functioning
- Protocols for drone location and fail-safe procedures
- Drone detection systems

Internet of Things

- Network protocols for the internet of things
- Remote attestation
- Intrusion and anomaly detection

Exam

The overall exam grade is divided according to the following criteria:

- 40%: mid-term report on work implementing attacks and countermeasures on a topic chosen from the first part of the course
- 40%: final report on work implementing attacks and countermeasures on a topic of your choice from the second part of the course
- 20%: final theoretical exam (10 multiple choice questions)

Target Skills and Knowledge

At the end of the course, the student will be able to

- Analyze a control flow and understand its fundamental operations, with particular reference to the CAN protocol.
- Ability to implement control layer and network layer attacks. Ability to analyze CAN bus traffic and infer information on its operation.
- Implement simple controllers and test their safety.
- Analyze a ladder logic program for PLC and understand how it works. Implement attacks capable of altering its functioning and design secure programs.

Target Skills and Knowledge

At the end of the course, the student will be able to

- Understand the functioning of the main industrial protocols, implement integrity and availability attacks, and develop countermeasures.
- Implement side channel attacks for sensitive information inference. Implement power analysis techniques for the inference of sensitive data in implementations of cryptographic algorithms (e.g., AES)
- Understand how drone positioning protocols and fail safe procedures work. Implement GPS spoofing attacks to divert trajectories.
- Implement remote attestation protocols for IoT devices and analyze their performance.

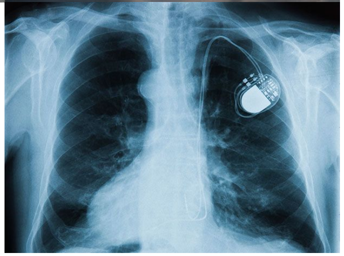
Cyber-Physical Systems

Cyber-Physical Systems (CPSs) are characterized by the deep complex intertwining among :

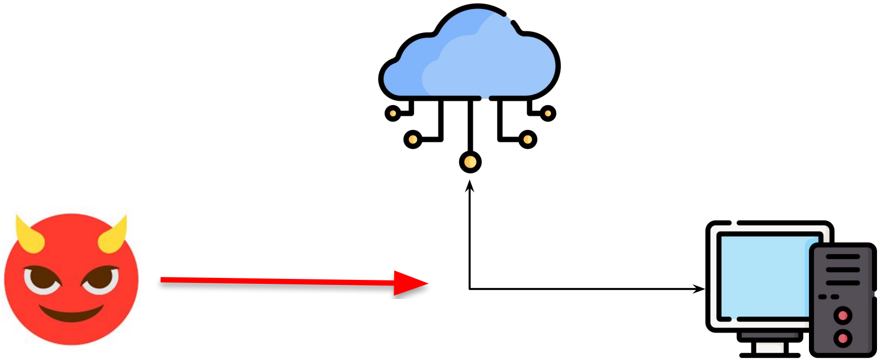
- The world of Physical Processes, or Operational Technology, or OT
- The world of Information Technology, or IT.

Some Example:

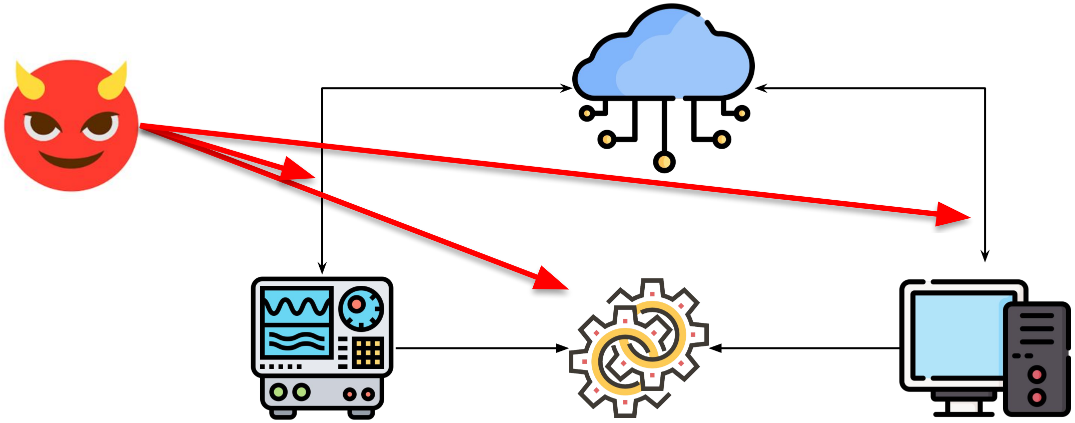
- *Smart Grid*
- *Smart Cars*
- *Industrial Control Systems*
- *e-Health Devices*



Attack Surfaces



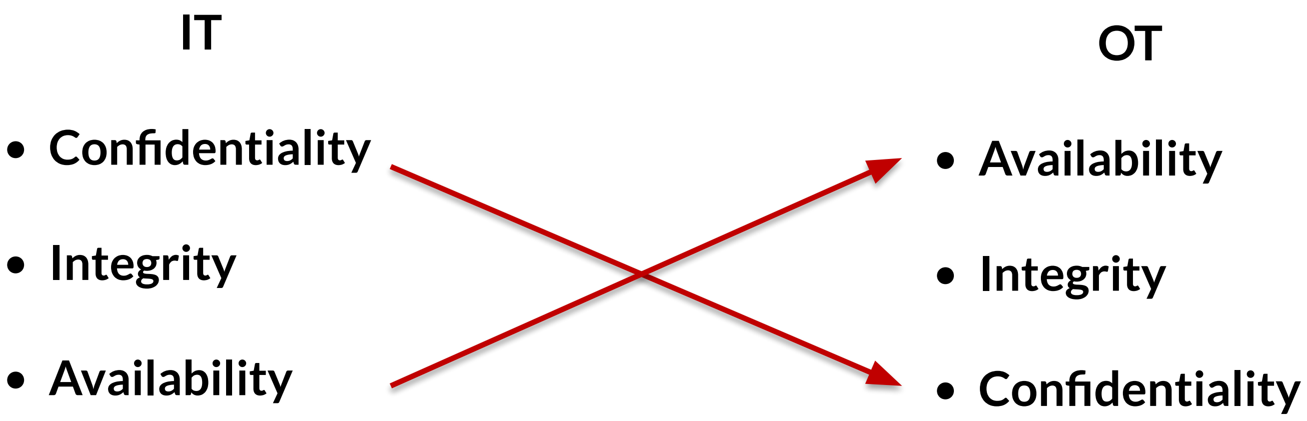
Traditional IT Systems



Cyber-Physical Systems

Confidentiality, Integrity, and Availability (CIA)

According to the literature on CyberSecurity, CIA paradigm is **reversed**:



IT

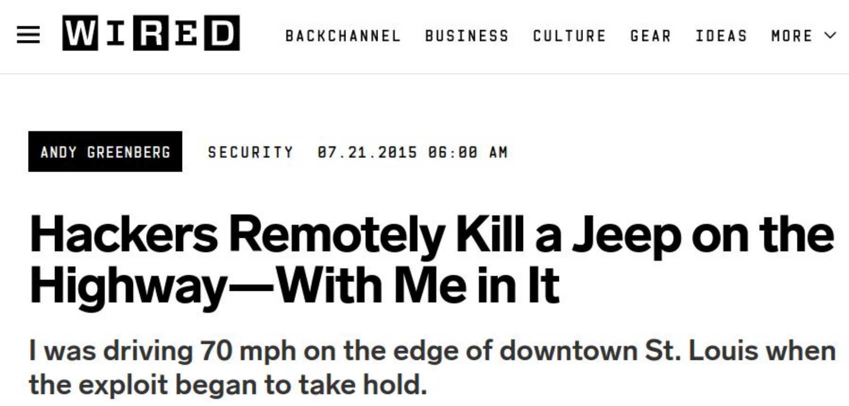
- **Confidentiality**
- **Integrity**
- **Availability**

OT

- **Availability**
- **Integrity**
- **Confidentiality**

What if we lose <u>Availability</u> of nuclear plants monitoring data?

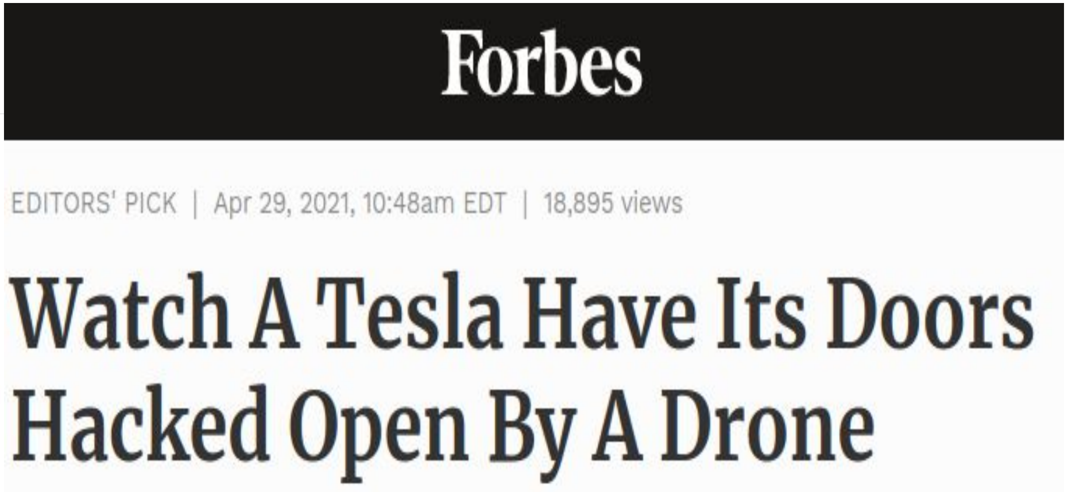
Do we have to care?



ANDY GREENBERG SECURITY 07.21.2015 06:00 AM

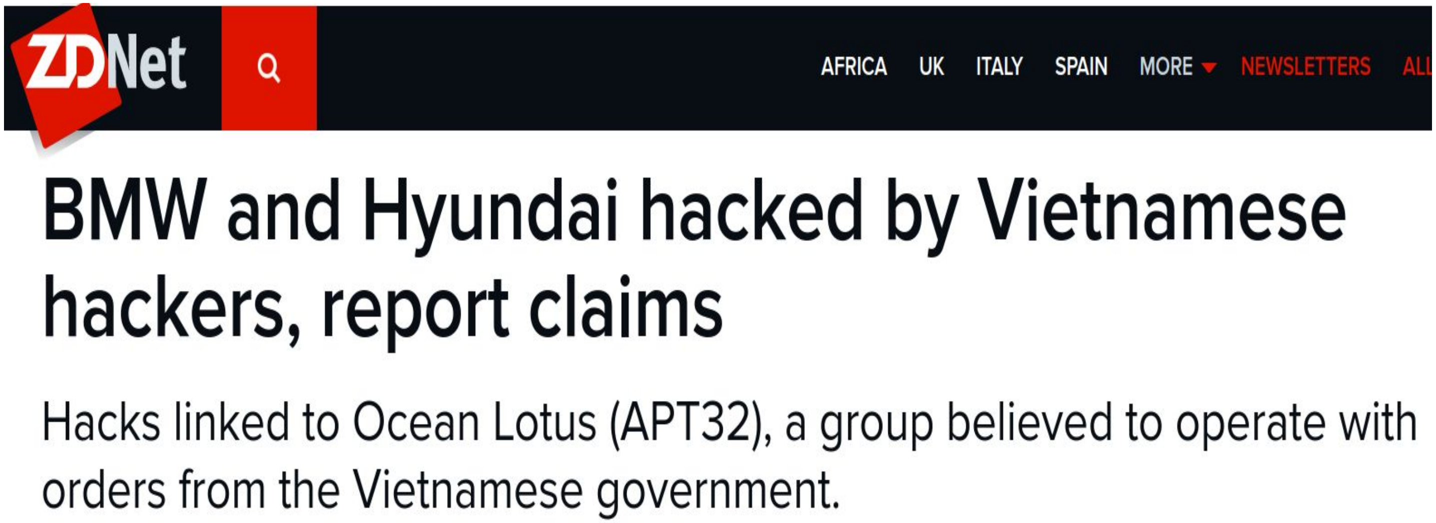
Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.



EDITORS' PICK | Apr 29, 2021, 10:48am EDT | 18,895 views

Watch A Tesla Have Its Doors Hacked Open By A Drone

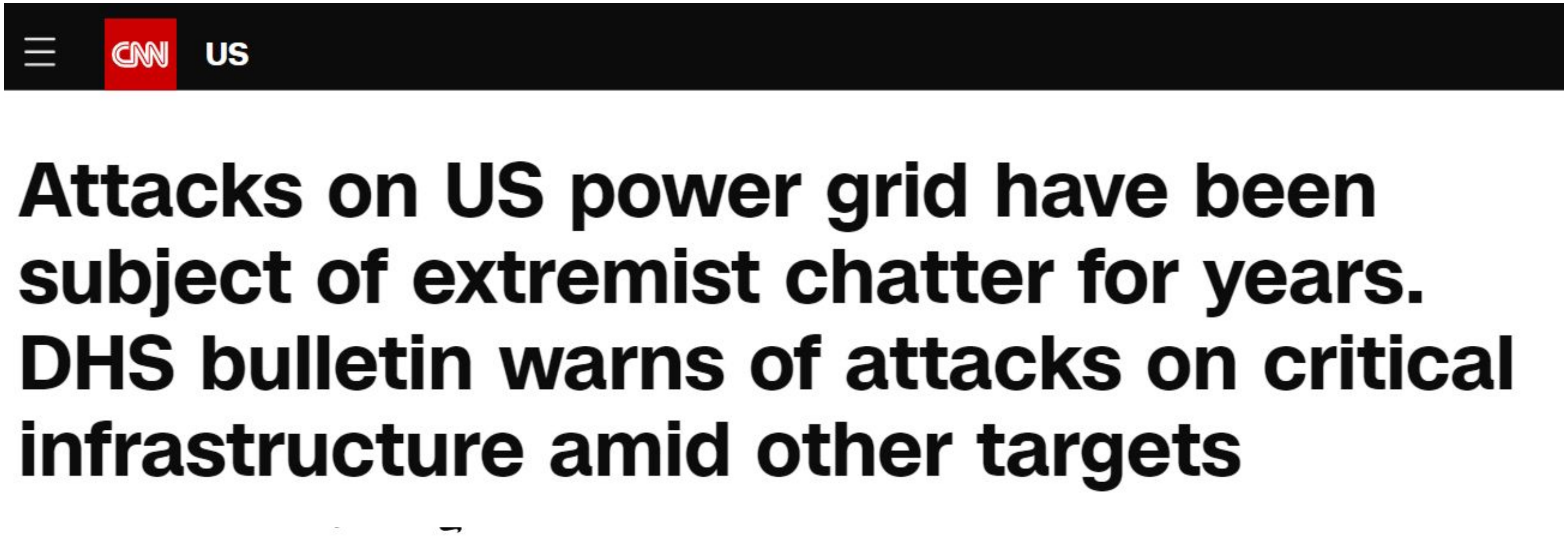


BMW and Hyundai hacked by Vietnamese hackers, report claims

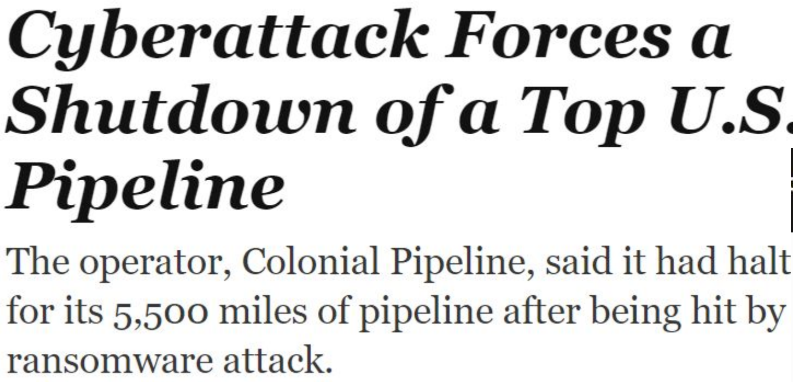
Hacks linked to Ocean Lotus (APT32), a group believed to operate with orders from the Vietnamese government.

Click me for the video!

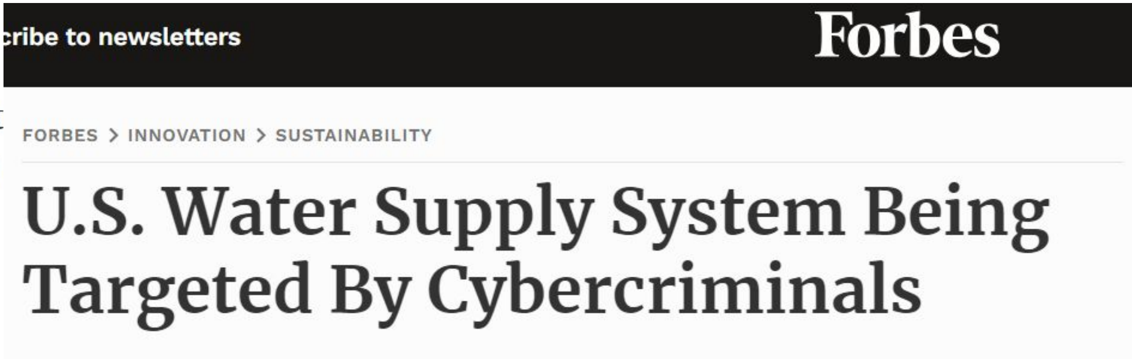
Do we have to care?


CNN US

Attacks on US power grid have been subject of extremist chatter for years. DHS bulletin warns of attacks on critical infrastructure amid other targets


Cyberattack Forces a Shutdown of a Top U.S. Pipeline

The operator, Colonial Pipeline, said it had halt for its 5,500 miles of pipeline after being hit by ransomware attack.

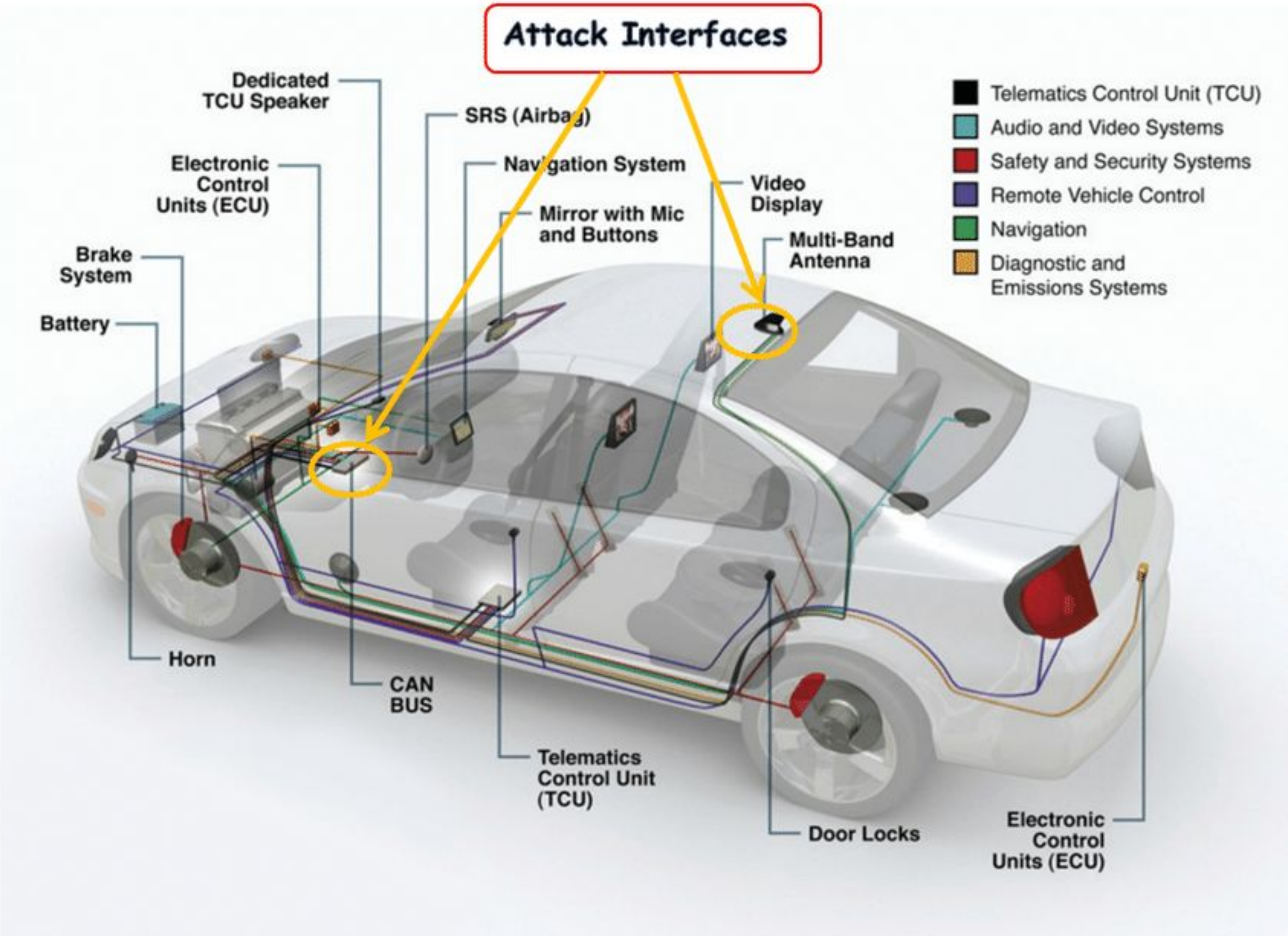

cribe to newsletters

Forbes

FORBES > INNOVATION > SUSTAINABILITY

U.S. Water Supply System Being Targeted By Cybercriminals

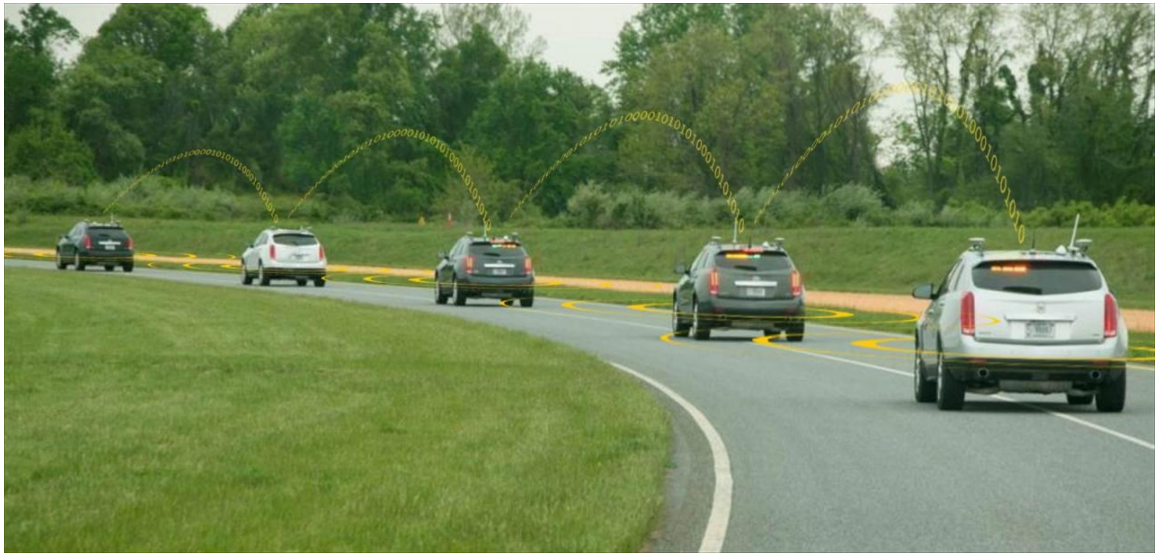
CAN bus


Attack Interfaces
Dedicated TCU Speaker
SRS (Airbag)
Navigation System
Electronic Control Units (ECU)
Mirror with Mic and Buttons
Video Display
Multi-Band Antenna
Brake System
Battery
Horn
CAN BUS
Telematics Control Unit (TCU)
Door Locks
Electronic Control Units (ECU)
■ Telematics Control Unit (TCU)
🟦 Audio and Video Systems
🟥 Safety and Security Systems
🟪 Remote Vehicle Control
🟩 Navigation
🟧 Diagnostic and Emissions Systems

Vehicles Platoon

Benefits of organizing vehicles in platoons:

- Fuel Efficiency
- Road Capacity
- Road Safety
- “Greener”

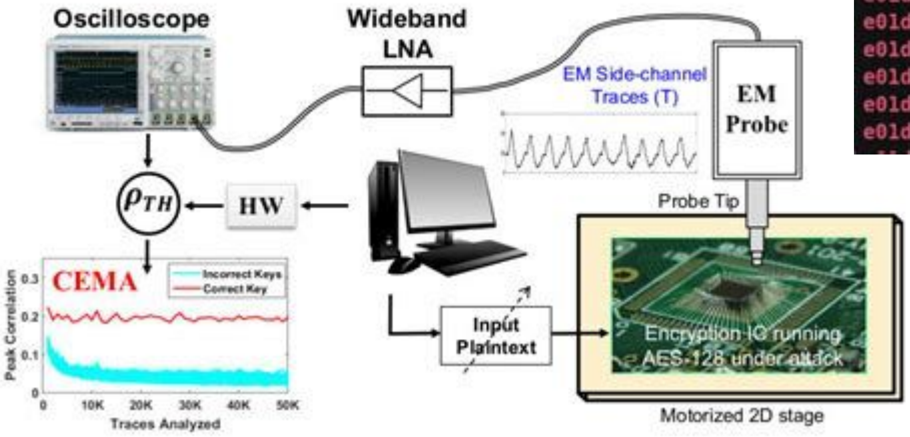


Industrial Systems

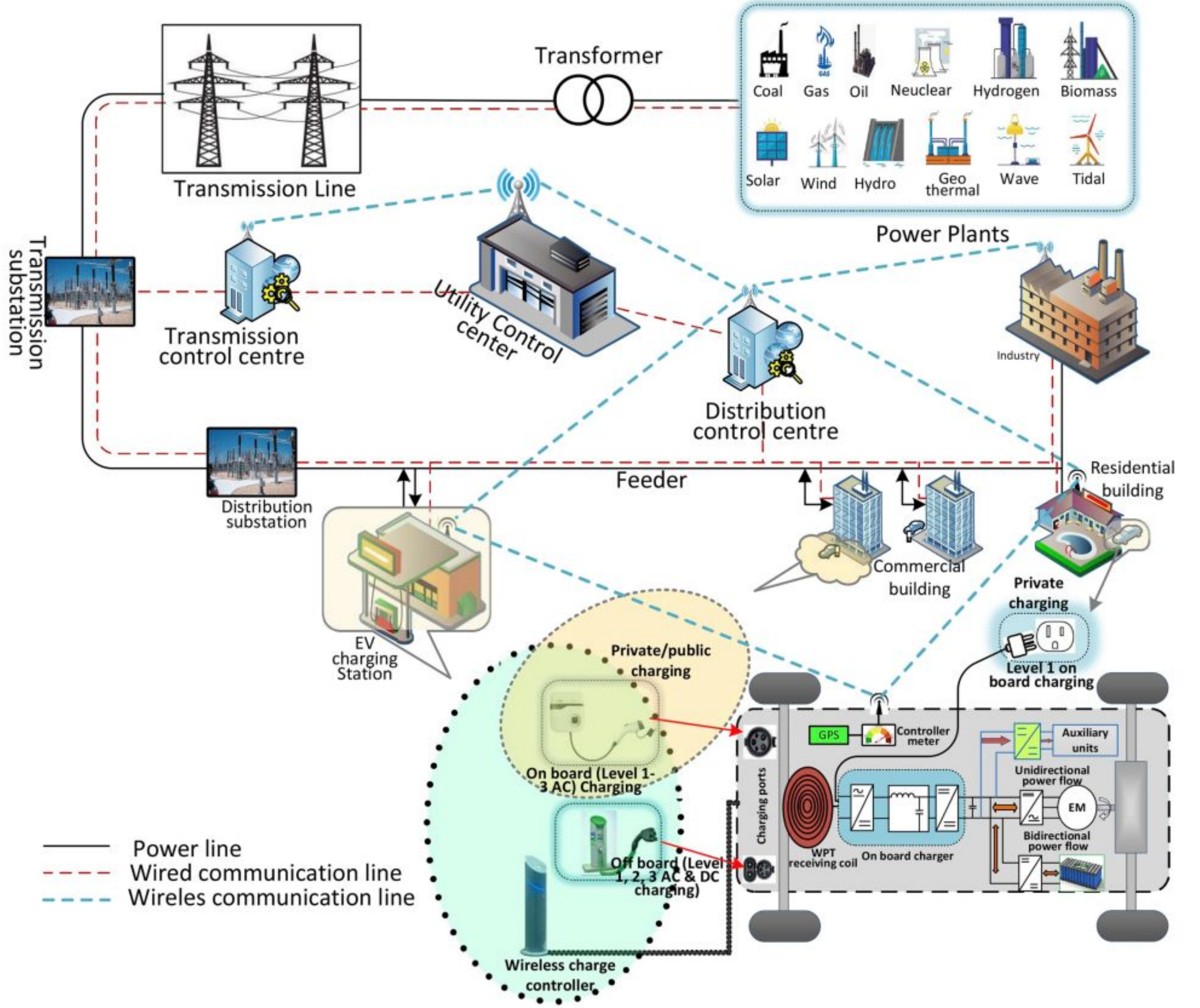
- Industrial systems have dedicated networks and components
- Operational technology + information technology
- Dedicated computing systems

Hardware Security

- How do modern CPU works
- How can we leverage their physical components to extract secrets?

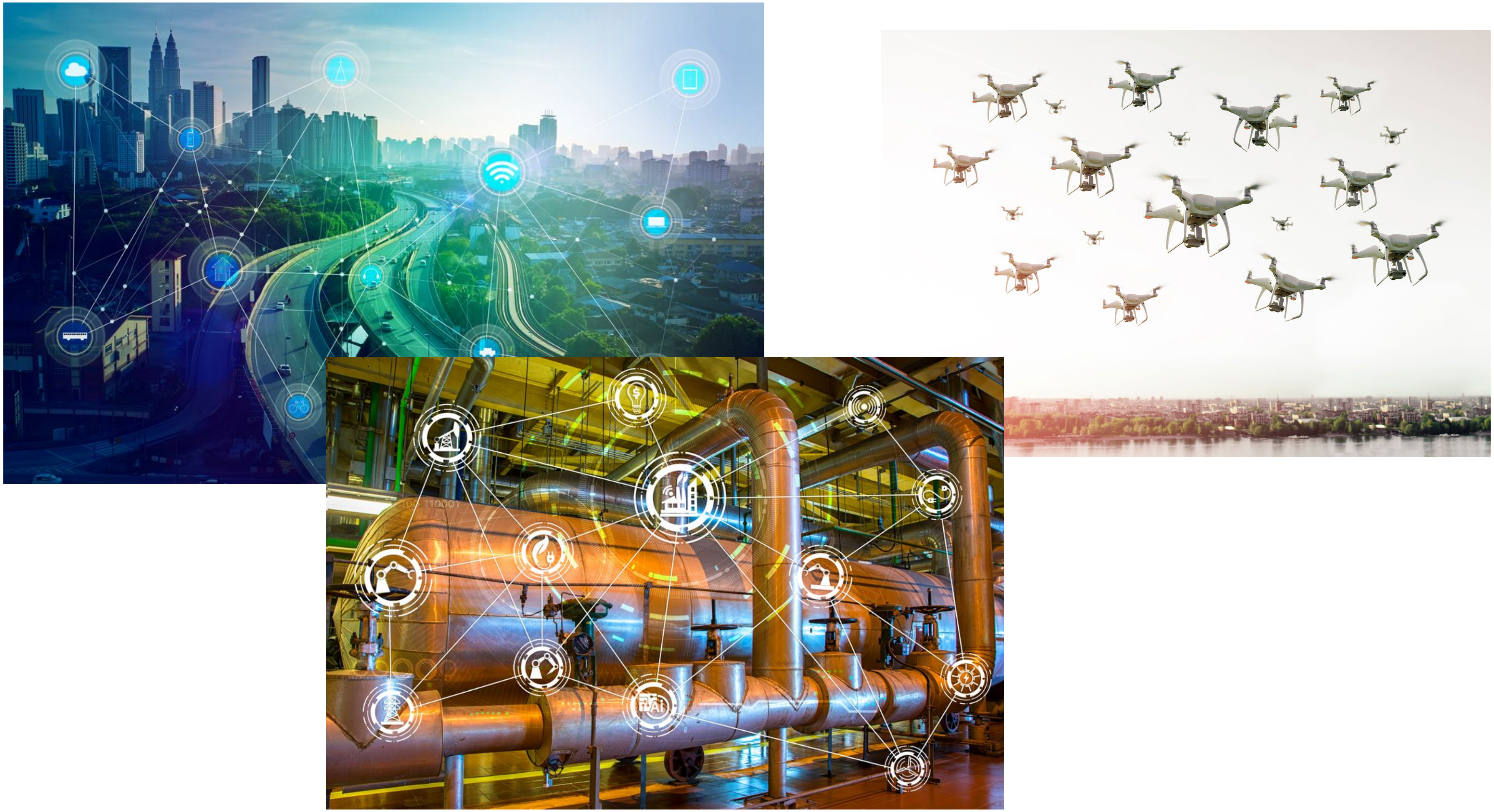


Vehicle-to-Grid (V2G)



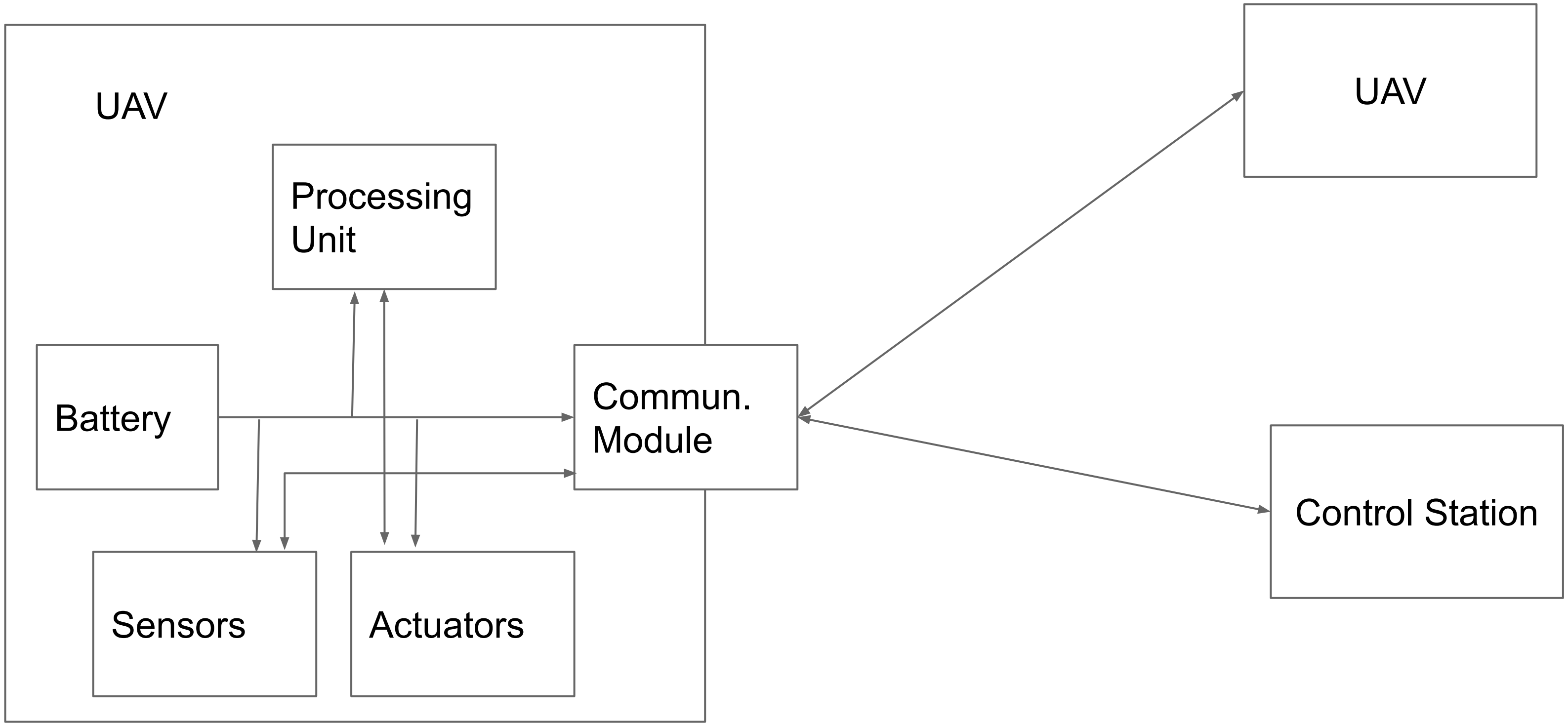
Security Implications in IoT

- IoT devices are employed in safety-critical systems



Structure of a Drone

- Multiple modules to acquire and process data
- Communication module as enabler


UAV
Processing Unit
Battery
Commun. Module
Sensors
Actuators
UAV
Control Station