CS 6963/5963
University of Utah

Cyber-physical Systems and IoT Security

Module 1c: Real-world Attacks & Defenses

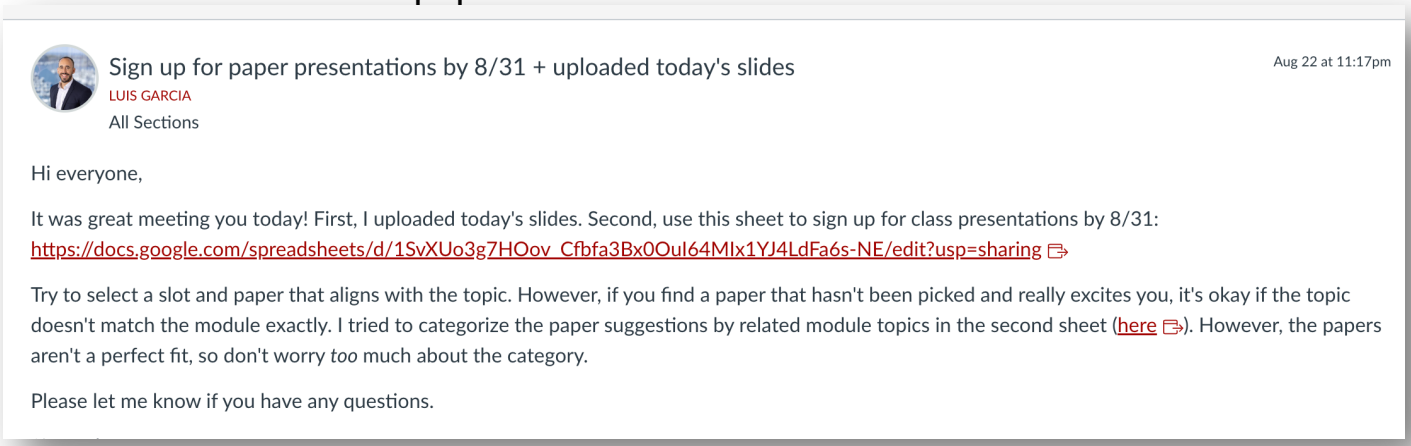
Attacks on Industrial Control Systems

Attacks on Medical Implants

Attacks on Autonomous Vehicles

Announcements

- We didn't get a new room ☹
- Beware parking/traffic on Thursday (football game)
- Sign up for presentations by 8/31!
  - Link is on Canvas + Piazza announcements
  - Make sure to choose a paper that hasn't been selected!



Sign up for paper presentations by 8/31 + uploaded today's slides

Aug 22 at 11:17pm

LUIS GARCIA

All Sections

Hi everyone,

It was great meeting you today! First, I uploaded today's slides. Second, use this sheet to sign up for class presentations by 8/31: https://docs.google.com/spreadsheets/d/1SvXUo3g7HOov_Cfbfa3Bx0OuI64MIx1YJ4LdFa6s-NE/edit?usp=sharing

Try to select a slot and paper that aligns with the topic. However, if you find a paper that hasn't been picked and really excites you, it's okay if the topic doesn't match the module exactly. I tried to categorize the paper suggestions by related module topics in the second sheet (here). However, the papers aren't a perfect fit, so don't worry *too* much about the category.

Please let me know if you have any questions.


Questions?

Today's Goals

- Show some motivating real-world CPS attacks
- Show how you can get engaged with different CPS security research domains
- Inspire project ideas

Please reach out to me if you're struggling with ideas!

CPS Real-world Attacks Part 1: Industrial Control Systems

Safety-Critical Industrial Control Systems

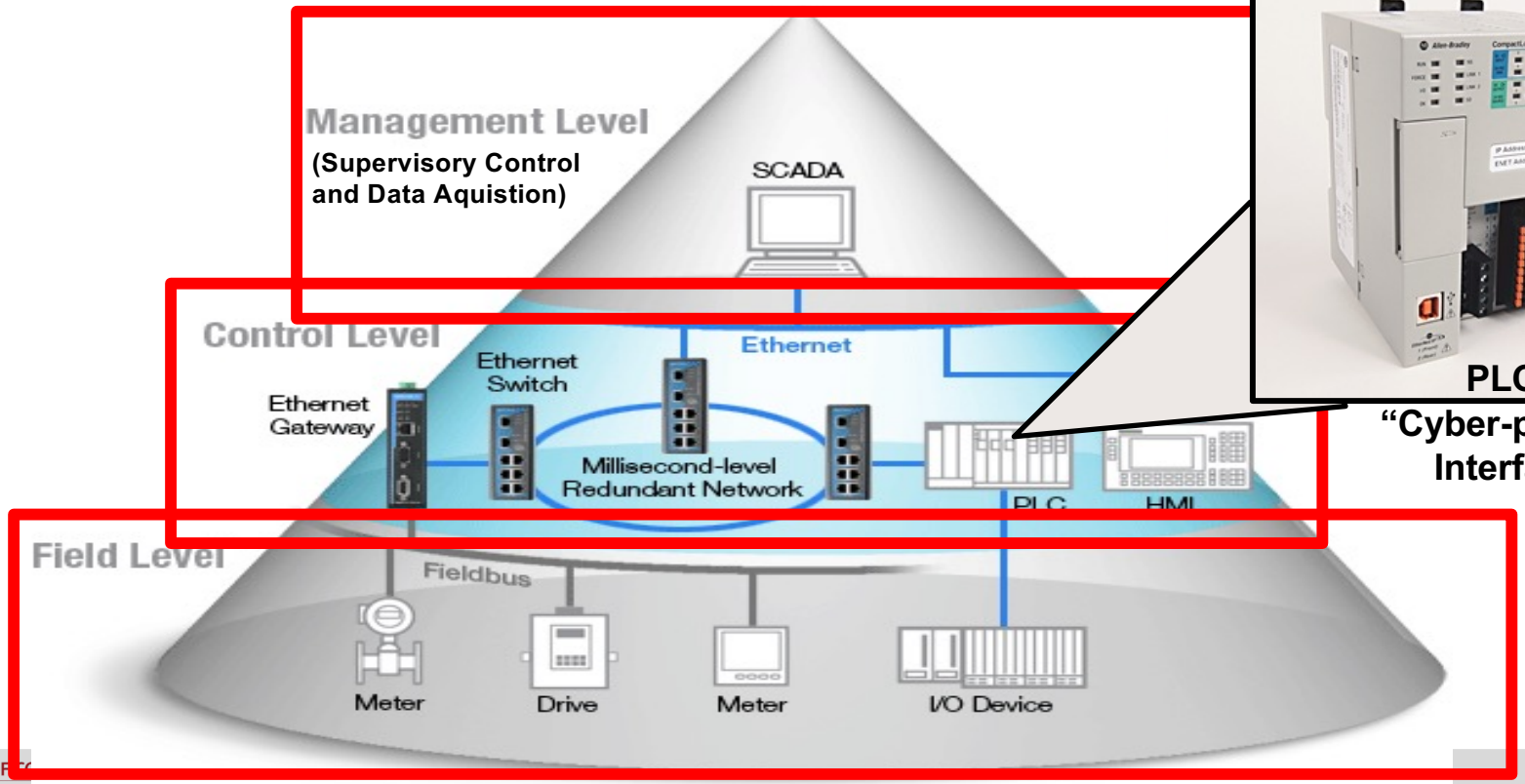
Water Treatment

Factory Automation

Electric Power Grid

Nuclear Reactor

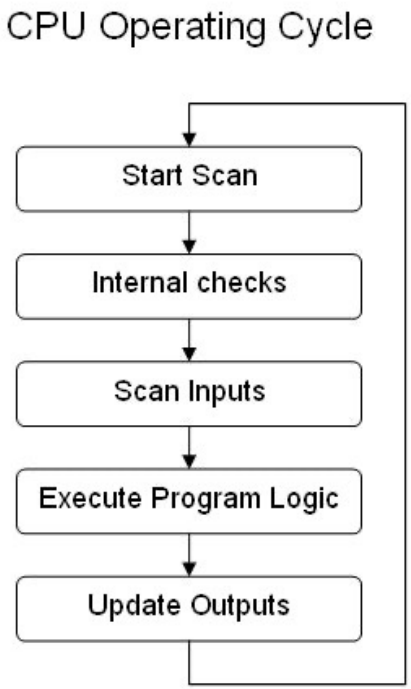
Programmable Logic Controllers (PLCs) and Industrial Control Systems (ICS)



PLCs: "Cyber-physical Interface"

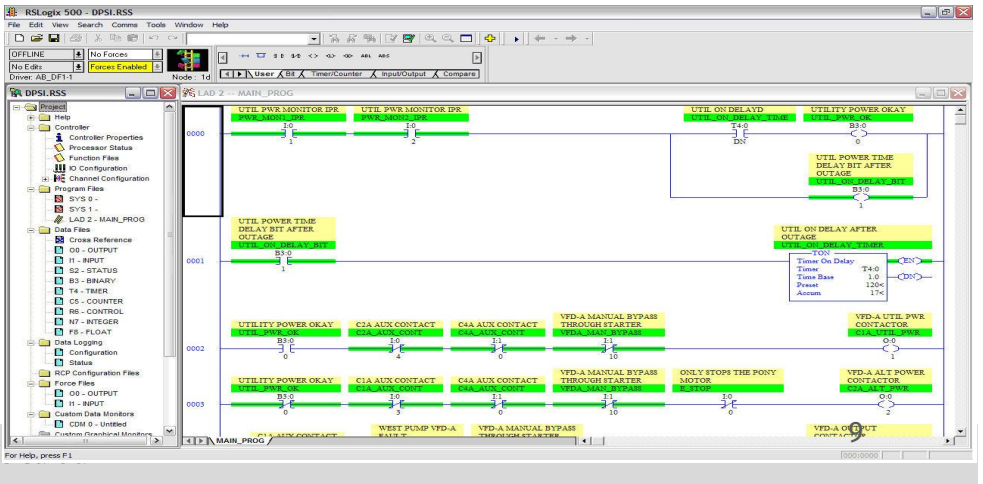
Programmable Logic Controllers

- Industrial digital computers:
  - ”ruggedized”
  - Modularized
  - Adapted for control manufacturing processes
- **Usually the target of attacks**



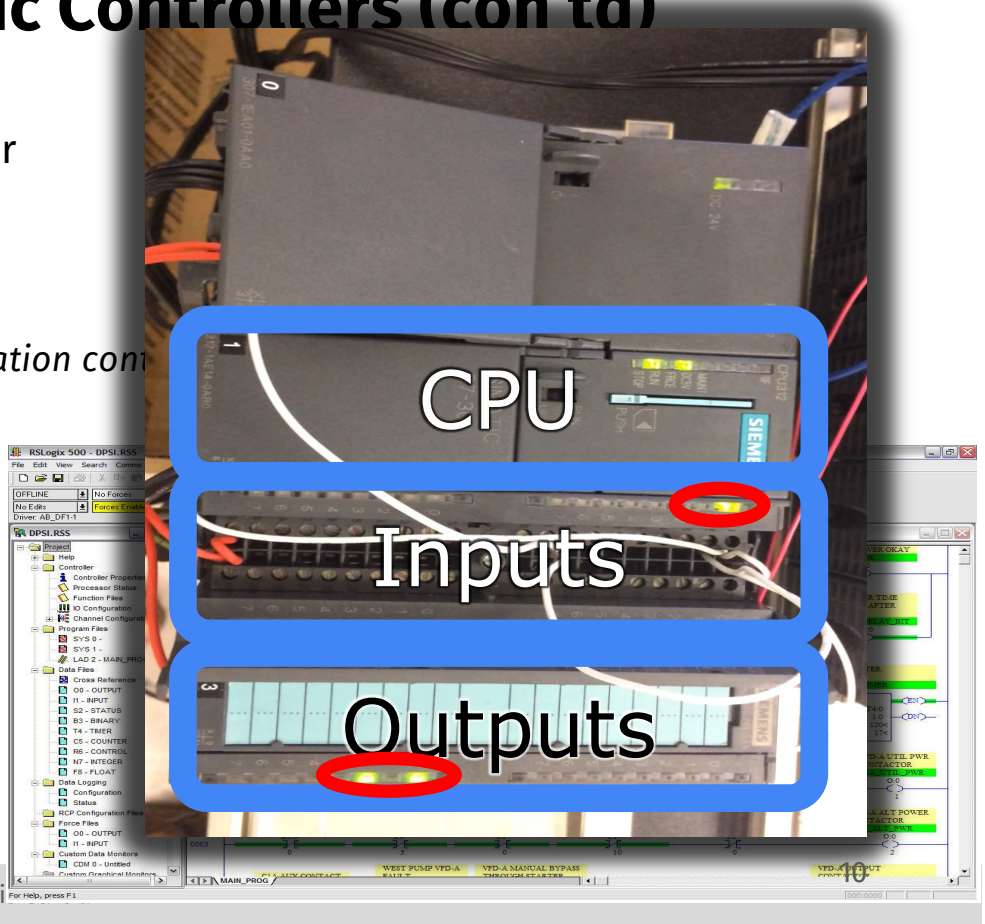
Programmable Logic Controllers (con’td)

- **MIMO** digital **reprogrammable** computer
  - *CPU, Input sensors, output controls*
- Industrial **control automation**
  - *Assembly lines, nuclear plants, generation control*
- **Simple programming** languages
  - *Ladder logic, instruction list*
- Cyclic **IO scans**: reading inputs and updating output wires
  - *100 times per second*

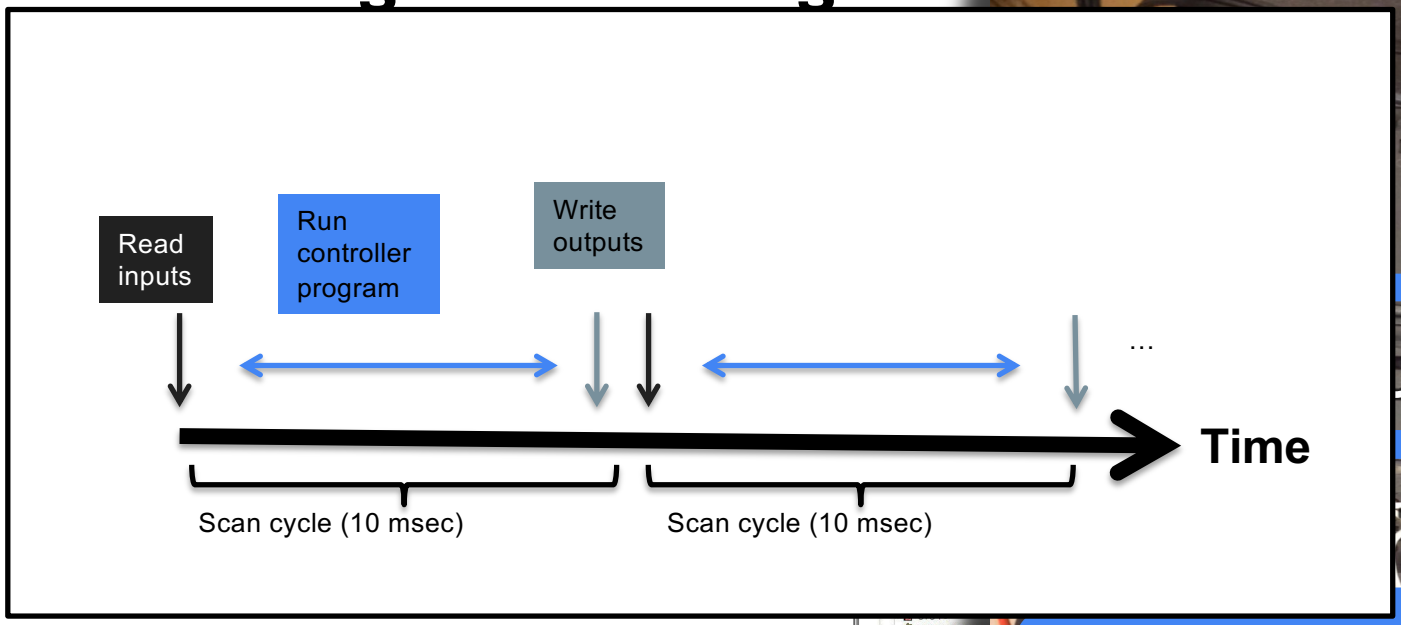


Programmable Logic Controllers (con'td)

- **MIMO** digital **reprogrammable** computer
  - *CPU, Input sensors, output controls*
- Industrial **control automation**
  - *Assembly lines, nuclear plants, generation cont*
- **Simple programming** languages
  - *Ladder logic, instruction list*
- Cyclic **IO scans**: reading inputs and updating output wires
  - *100 times per second*

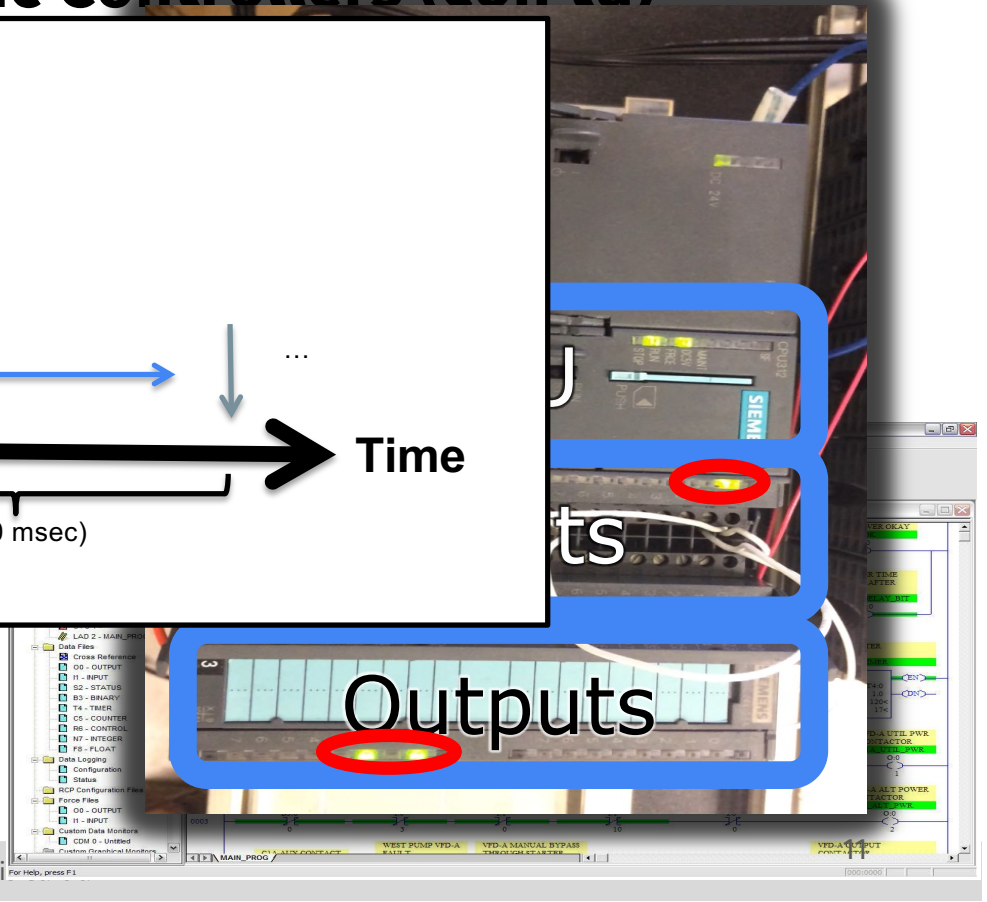


Programmable Logic Controllers (con'td)



and updating output wires

- *100 times per second*



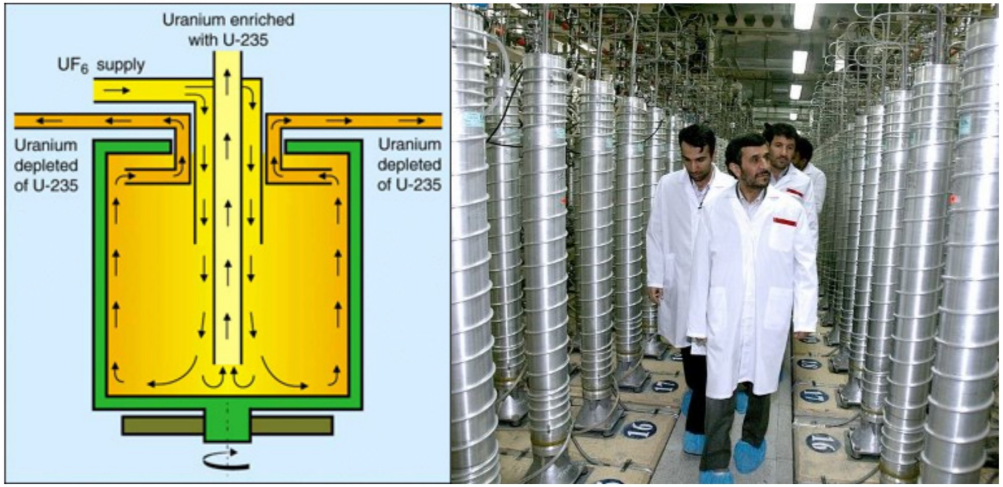
The Trouble with SCADA

- **Designed over 20 years ago**
  - Isolated
  - No security in mind
  - Access was local (not remote; no internet)
- **Today**
  - Connected to too many things
  - Remote control access
- **General Issues**
  - Lots of (vulnerable) proprietary protocols
  - Very hard to patch (reluctant vendors)

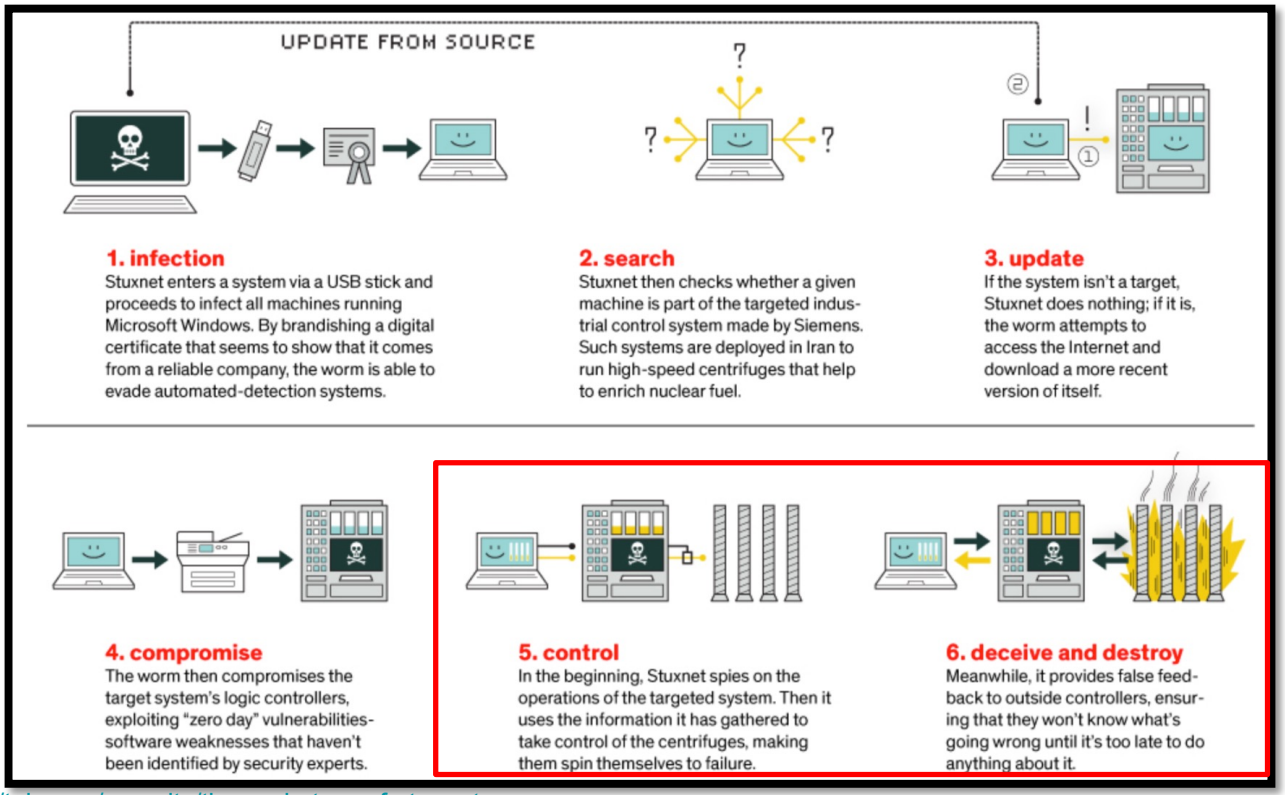
”Legal Informatics, Privacy, and Cyber Crime,” Sandro Etalle, ‘18

First Major "CPS" Attack: Stuxnet (2009)

- Attack on Iranian nuclear enrichment facilities
- History:
  - Iranian nuclear program dates back to 1950's when allies with US
  - After revolution in 1979, needed to enrich it's own Uranium
  - Provided designs and key components for centrifuges in 1980's
    - Suspected same generation were in place during infection

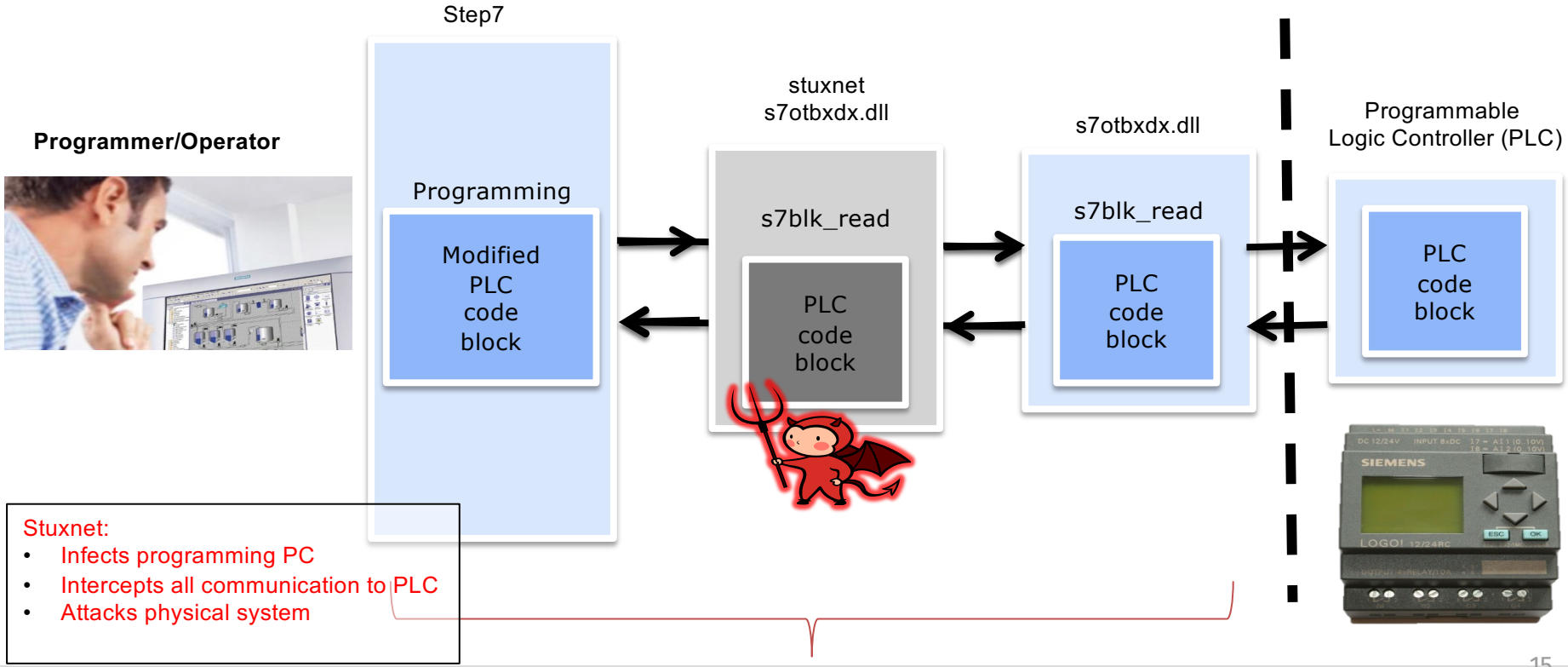


Stuxnet Attack (2009) overview

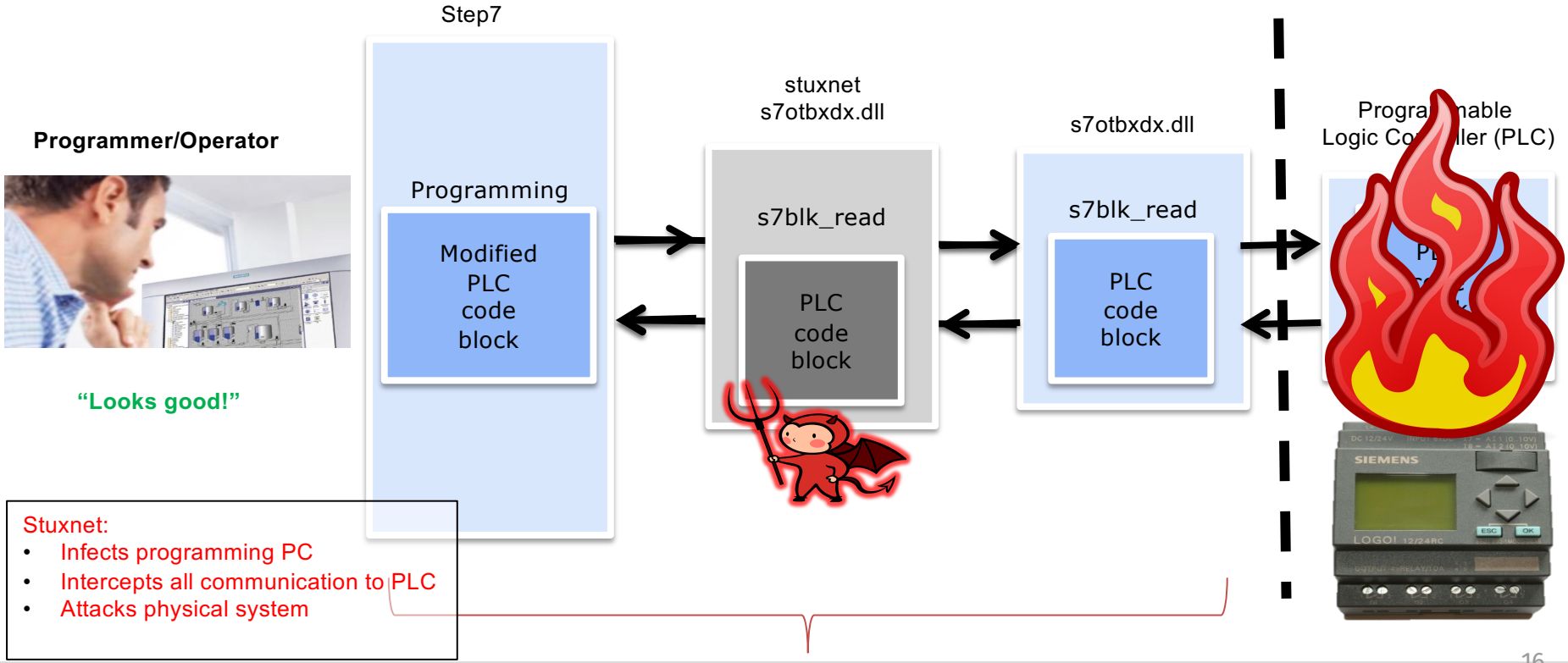


https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

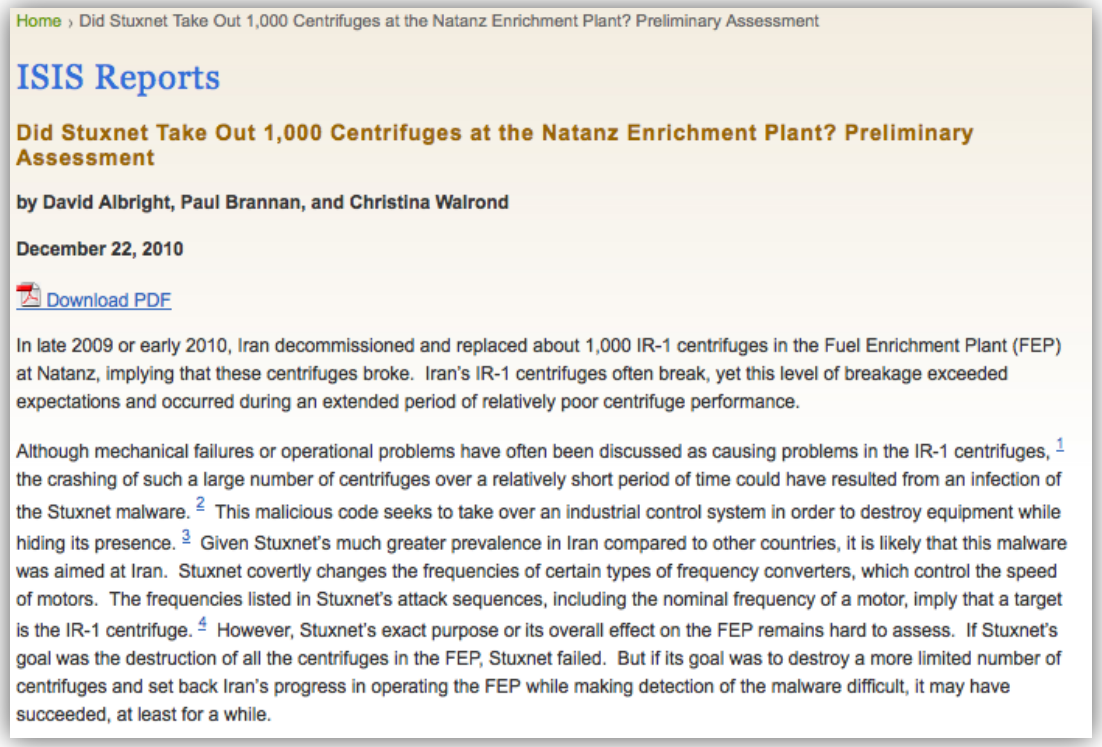
Representative Industrial Cyber-physical Attack: Stuxnet



Representative Industrial Cyber-physical Attack: Stuxnet



Stuxnet's Immediate Consequences



Home › Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment

ISIS Reports

Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment

by David Albright, Paul Brannan, and Christina Walrond

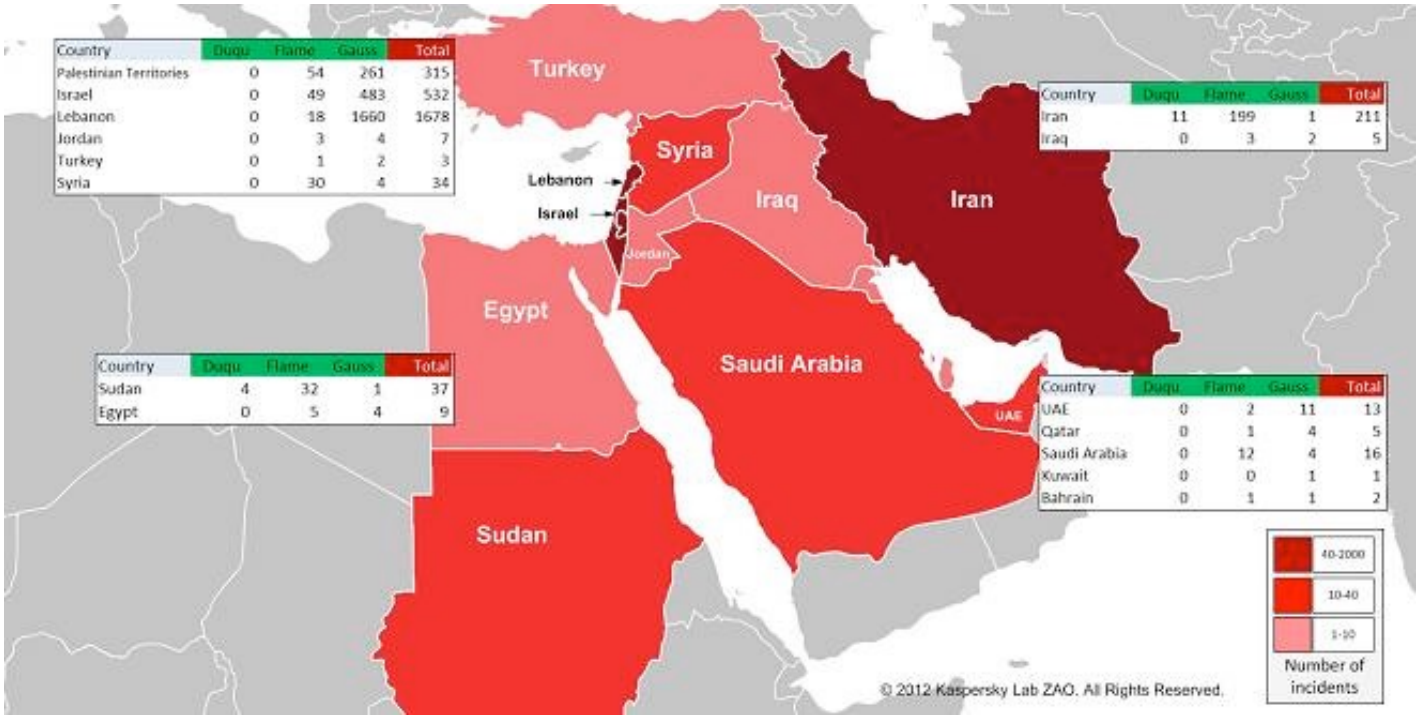
December 22, 2010

Download PDF

In late 2009 or early 2010, Iran decommissioned and replaced about 1,000 IR-1 centrifuges in the Fuel Enrichment Plant (FEP) at Natanz, implying that these centrifuges broke. Iran's IR-1 centrifuges often break, yet this level of breakage exceeded expectations and occurred during an extended period of relatively poor centrifuge performance.

Although mechanical failures or operational problems have often been discussed as causing problems in the IR-1 centrifuges, [1] the crashing of such a large number of centrifuges over a relatively short period of time could have resulted from an infection of the Stuxnet malware. [2] This malicious code seeks to take over an industrial control system in order to destroy equipment while hiding its presence. [3] Given Stuxnet's much greater prevalence in Iran compared to other countries, it is likely that this malware was aimed at Iran. Stuxnet covertly changes the frequencies of certain types of frequency converters, which control the speed of motors. The frequencies listed in Stuxnet's attack sequences, including the nominal frequency of a motor, imply that a target is the IR-1 centrifuge. [4] However, Stuxnet's exact purpose or its overall effect on the FEP remains hard to assess. If Stuxnet's goal was the destruction of all the centrifuges in the FEP, Stuxnet failed. But if its goal was to destroy a more limited number of centrifuges and set back Iran's progress in operating the FEP while making detection of the malware difficult, it may have succeeded, at least for a while.

Stuxnet's Long-term Consequences: Duqu, Flame, and Gauss Variant Worms



Country	Duqu	Flame	Gauss	Total
Palestinian Territories	0	54	261	315
Israel	0	49	483	532
Lebanon	0	18	1660	1678
Jordan	0	3	4	7
Turkey	0	1	2	3
Syria	0	30	4	34

Country	Duqu	Flame	Gauss	Total
Iran	11	199	1	211
Iraq	0	3	2	5

Country	Duqu	Flame	Gauss	Total
Sudan	4	32	1	37
Egypt	0	5	4	9

Country	Duqu	Flame	Gauss	Total
UAE	0	2	11	13
Qatar	0	1	4	5
Saudi Arabia	0	12	4	16
Kuwait	0	0	1	1
Bahrain	0	1	1	2

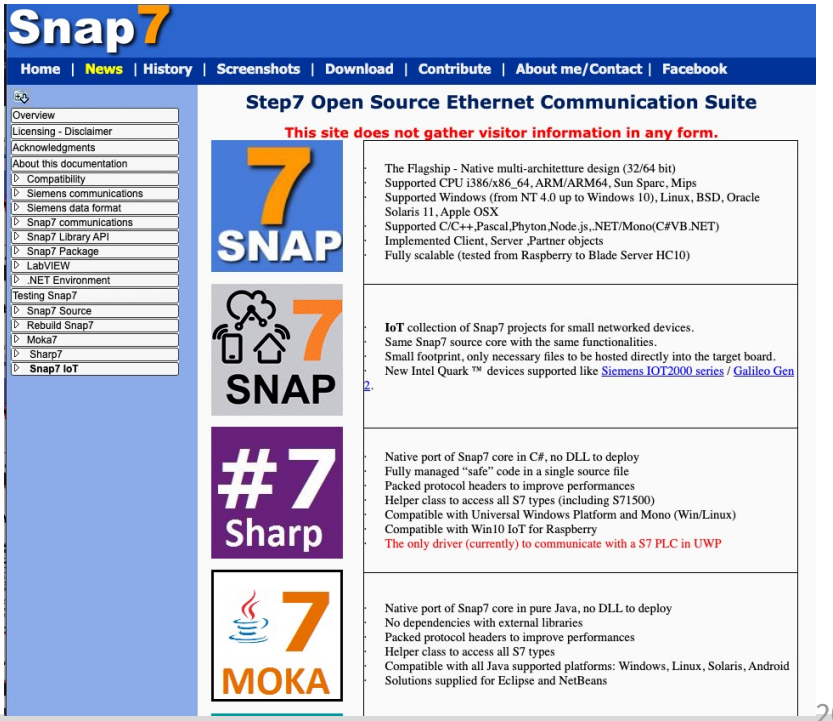
Subsequent Attacks on the Power Grid: Ukraine Power Grid Attacks –2015 & 2016

	December 2015	December 2016
Malware	Black Energy, Kill Disk	Industroyer / Crash Override
Attack stages	1. Manual reconnaissance 2. Manual shutdown of relays via remote connection to SCADA workstations 3. Destroyed SCADA drives 4. Disabled battery backup 5. Destroyed serial-to-Ethernet devices	1. Automated reconnaissance 2. Automated shutdown of relays via native ICS commands 3. DoS on Siemens relays 4. Destroyed ABB configuration files
Architecture	Human	Modular & extensible
Target	50+ substations	Transmission station
Impact	135 MW	200 MW
Significance	1st public cyberattack on civilian infrastructure	1st public discovery of autonomous & targeted ICS malware

Encryption in ICS – SmartGridComm '17

Stuxnet Long-term Consequences: Script Kiddies

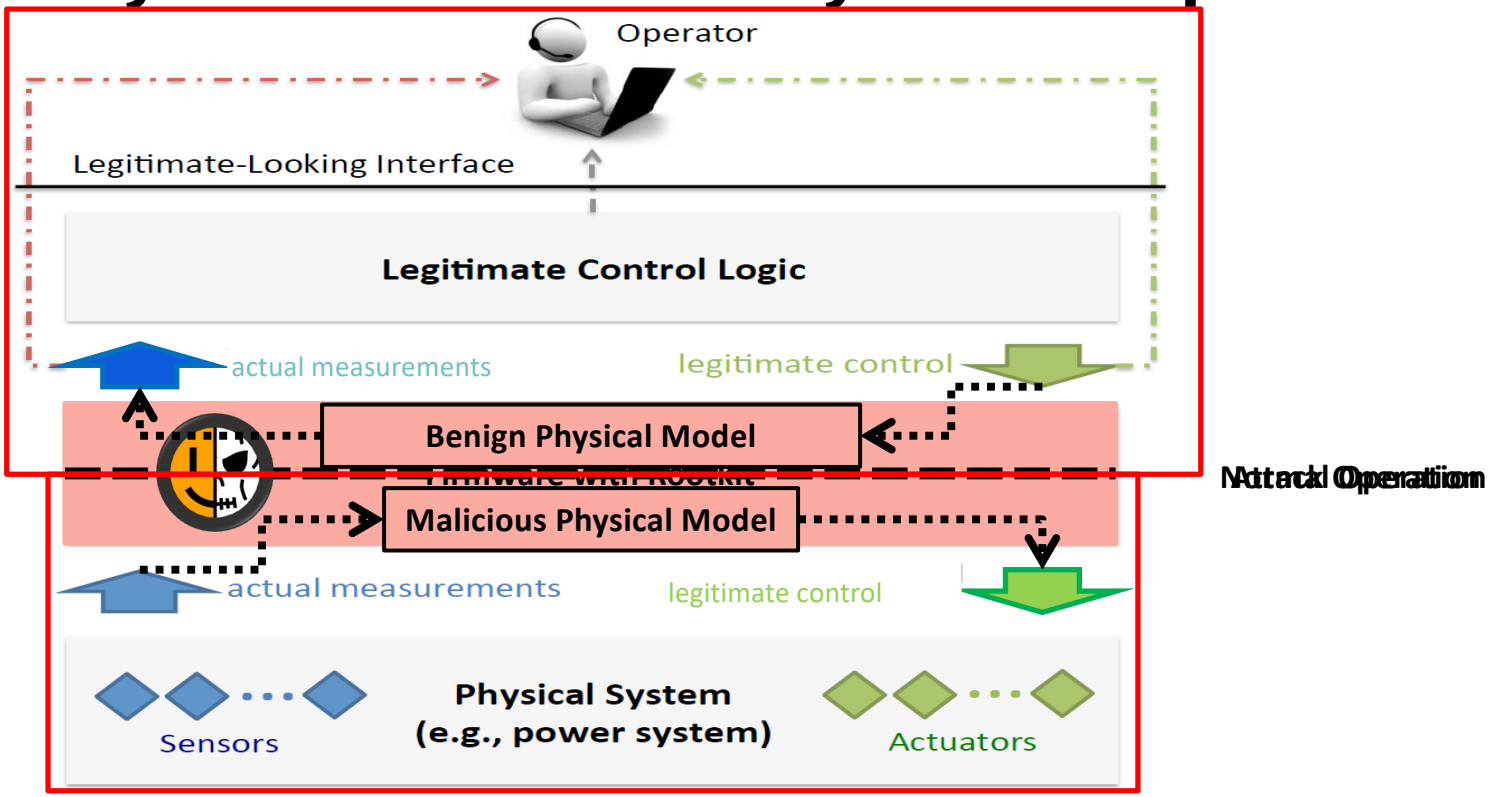
- Lots of open-source frameworks available from BlackHat community to communicate with these devices
  - https://github.com/arnaudsoullie/scan7



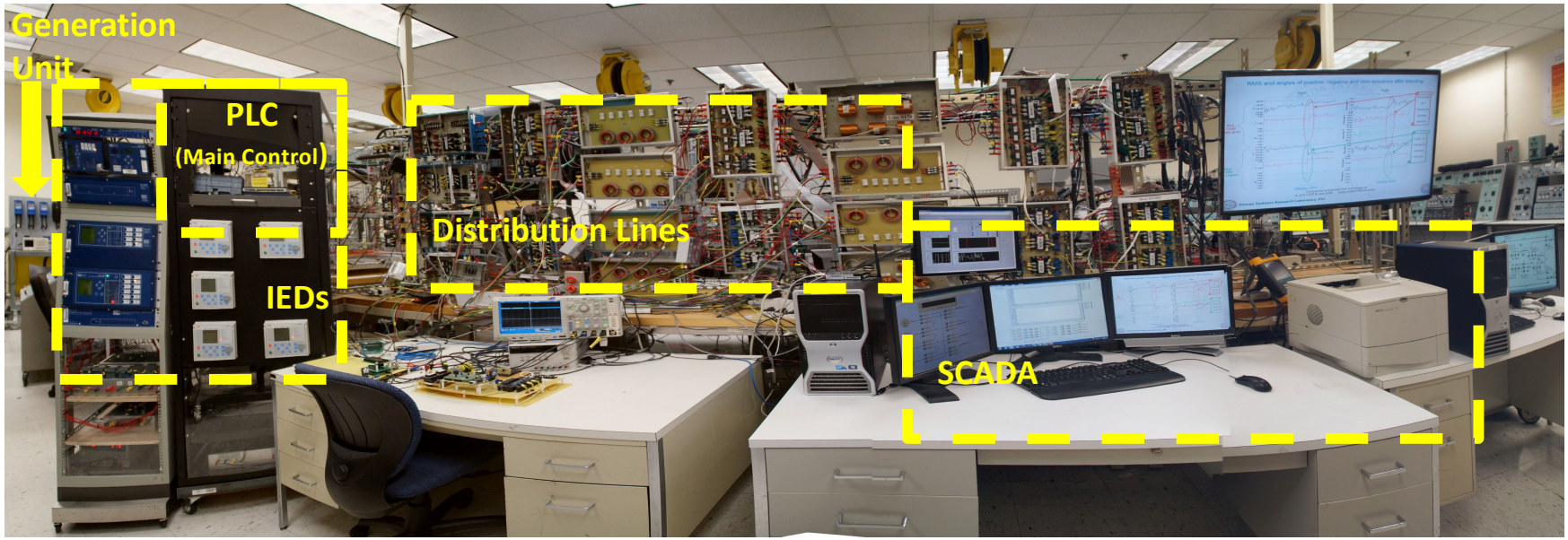
Harvey: Model-Aware Rootkit (NDSS 2017)

- A malware that takes into account the physical topology of the ICS
- Model
  - Uses physical models to optimize control commands for an adversarial objective function
- PLC infection: compromising the PLC's firmware
  - Utilize the firmware update mechanism to replace firmware over the network
  - Local firmware modifications, e.g., SD card or JTAG implantation
  - Run-time attacks, e.g., network exploits or remote code execution vulnerabilities (FrostyURL)

Physics-Awareness: 2-Way Data Manipulation

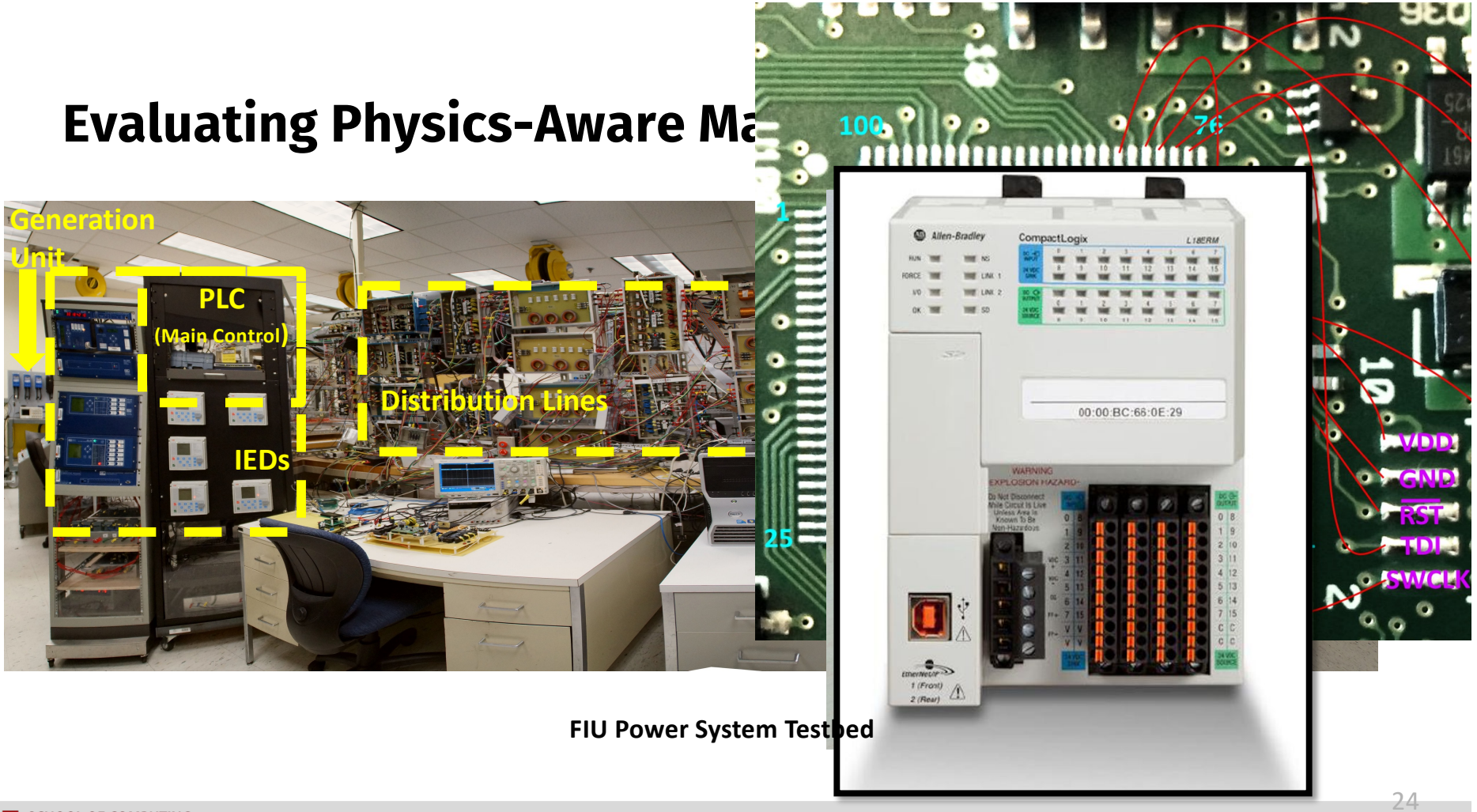


Evaluating Physics-Aware Malware on a Power System



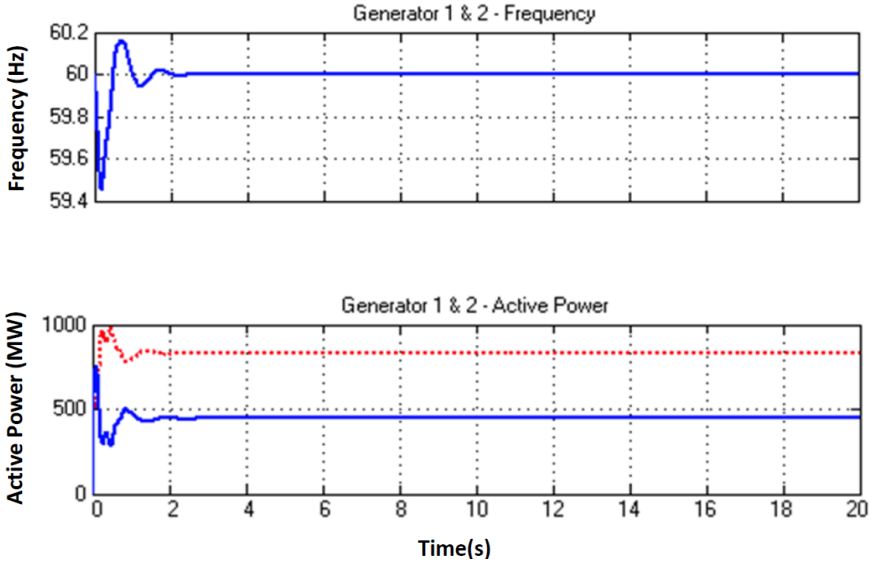
FIU Power System Testbed

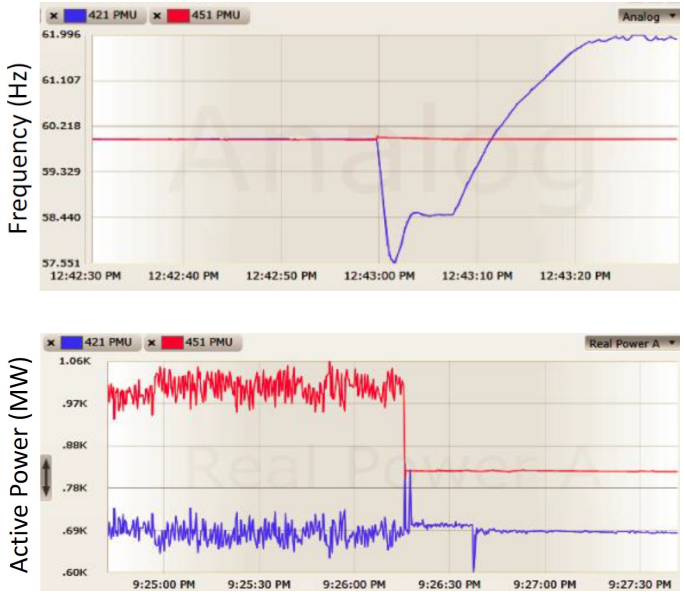
Evaluating Physics-Aware Ma



FIU Power System Testbed

Evaluating Physics-Aware Malware on a Power System





HMI Measurements

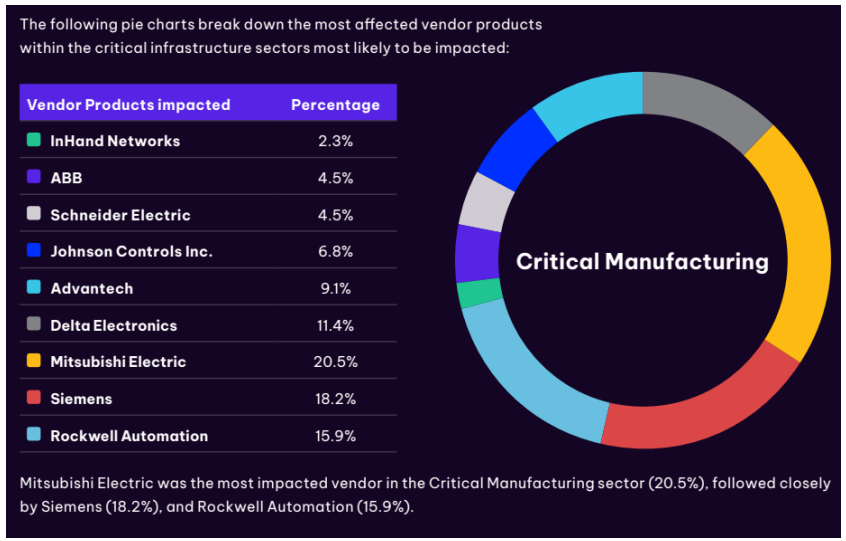
looks like stable operation…

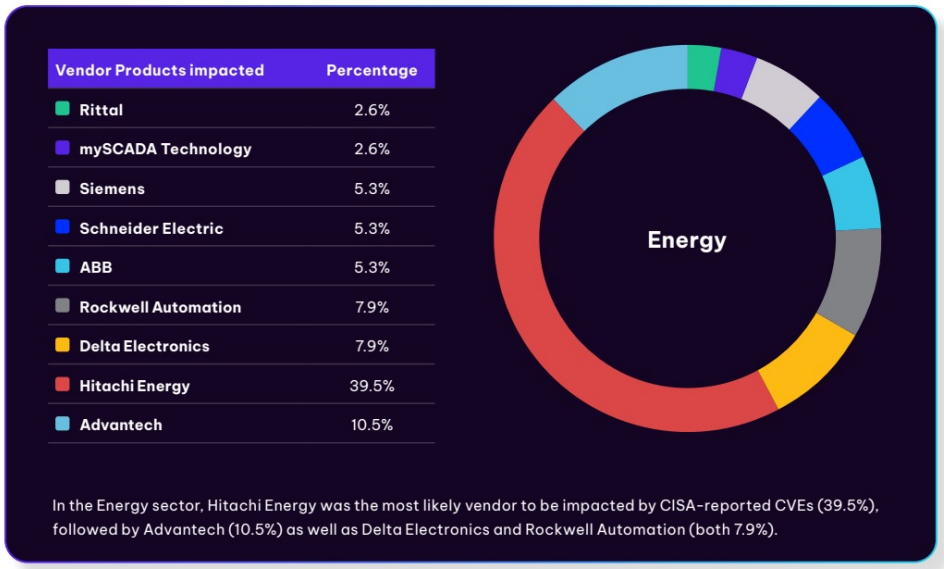
Actual System Measurements

…in reality, it's unstable!

Recent ICS Vulnerability Trends

- CISA ICS Advisory Report 2023: **670** new ICS-related vulnerabilities in **first half** of 2023





"ICS CVE Research Report: First Half of 2023," SynSaber + ICS[AP] Analysis

ICS Vulnerability Trends

- CISA ICS Advisory Report 2023
- **Most Dangerous Software Weaknesses:**

More about these in embedded systems security lecture!

"ICS Vulnerabilities: First Half of 2023," Sy

ICS Vulnerability Trends

- CISA ICS Advisory Report 2023
- **”Forever-Day” Vulnerabilities:**
  - Architectural and interoperability impacts
  - No simple way to “patch” a protocol vulnerability
  - Orgs have to deal with these CVEs for a long time

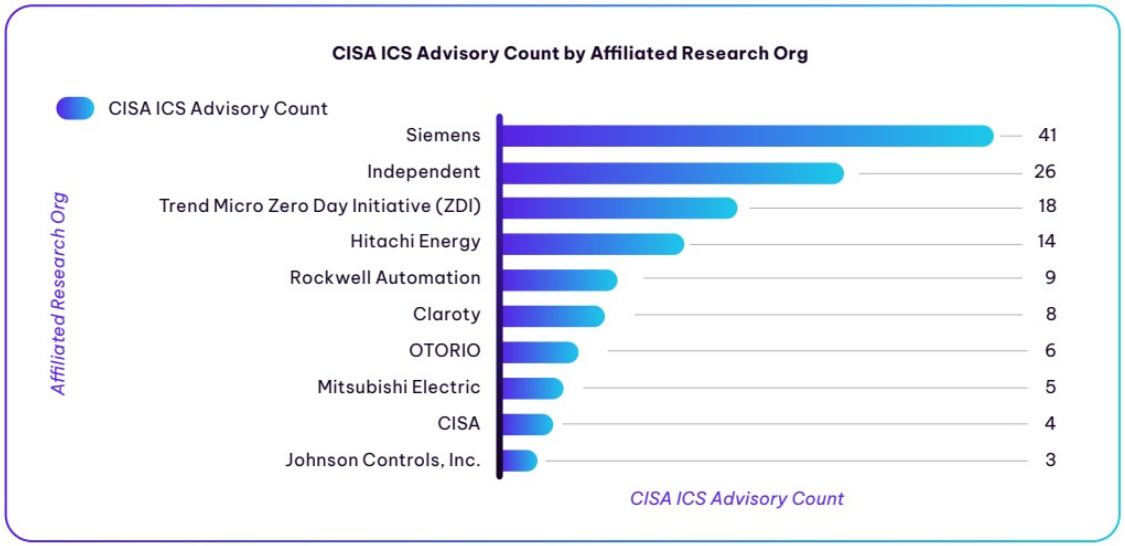
CVEs with NO Patch or Remediation (“Forever-Days”)

	1H23 Count	1H23%	1H22 Count	1H22%
No patch or remediation available at this time	227 of 670	34%	88 of 681	13%

“ICS Vulnerabilities: First Half of 2023,” SynSaber + ICS[AI

ICS Vulnerability Trends

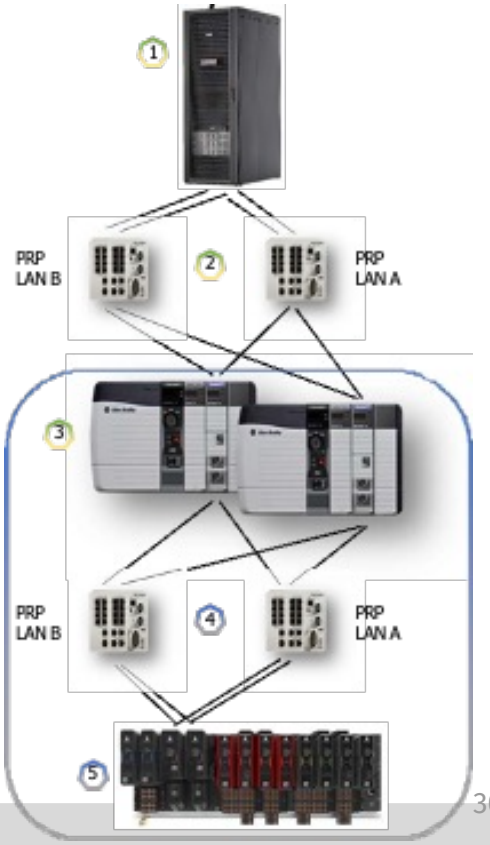
- CISA ICS Advisory Report 2023
- **Siemens continues to be a common target…**



"ICS Vulnerabilities: First Half of 2023," SynSaber + ICS[AP] Analysis

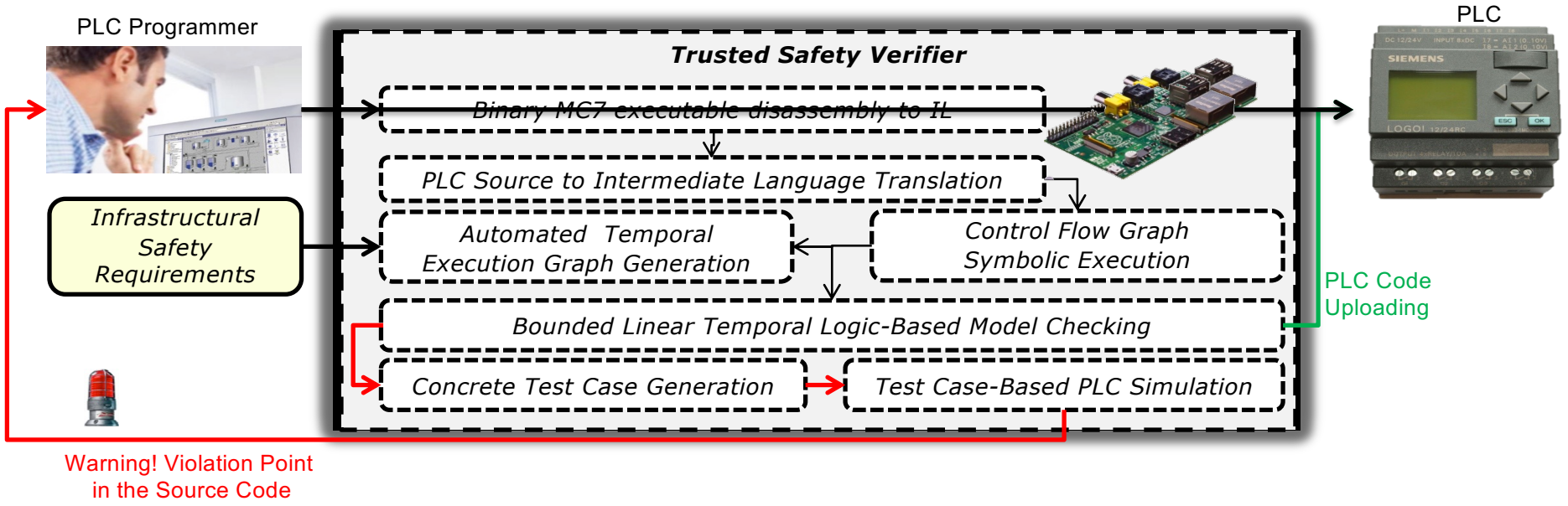
Defense Solutions from the Industry: Redundancy

- Virtualization 1
  - Virtual PCs on physically redundant servers
- Server Redundancy 1
  - Availability of operator interactions
- Network Redundancy 2
  - Availability of network/communication paths
- Controller (PLC) redundancy 3
  - Availability of control actions
- Communications redundancy 4
  - Availability of ICS communications
- I/O redundancy 5
  - Availability of device communications



"Security in a Modern DCS," Rockwell Automation

Research Defense: Trusted Safety Verifier (TSV) Overview



Bump-in-the-wire to verify uploaded code against safety requirements

Infrastructural Safety Requirements

- Formulated using linear temporal logic (LTL) expressions
- Example safety requirement
  - *English expression*
    - *Relay R_1 should **NOT** open **UNTIL** Generator G_2 turns on*
  - *Logical expression*
    - *Atomic propositions*
      - a_1: "Relay R_1 is open"
      - a_2: "Generator G_2 is on"

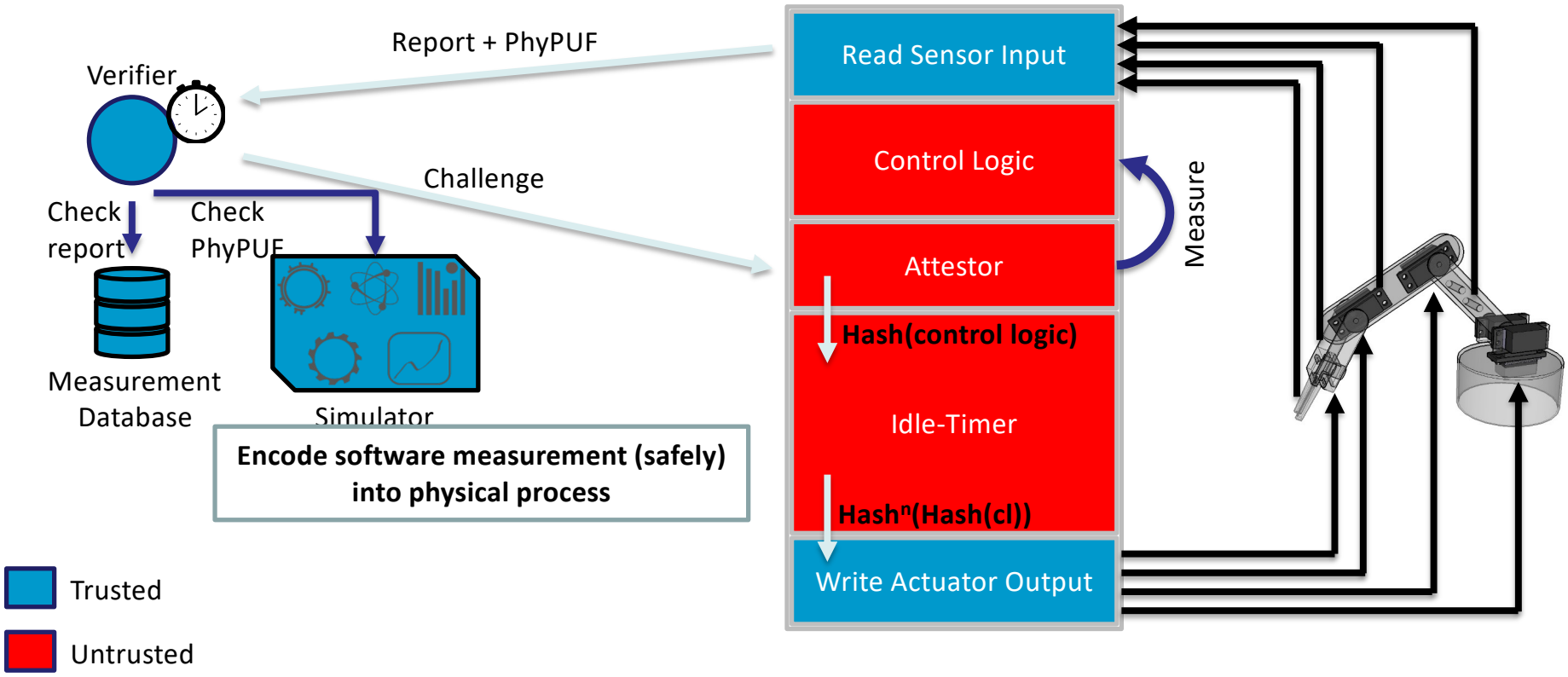
LTL: $!a_1$ **U** a_2

More Defenses: Physics for the Sake of Security

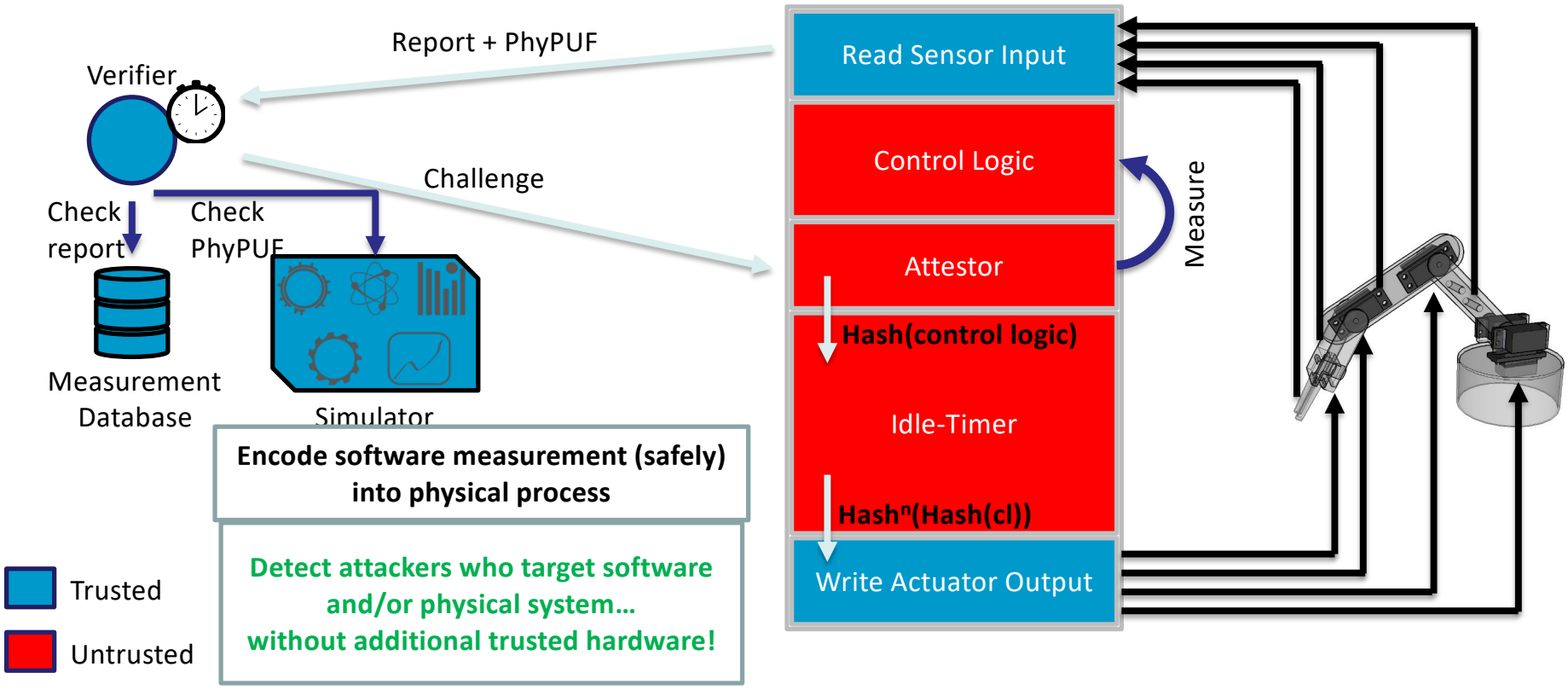
- **Problem:** Legacy devices (such as PLCs) don't support a hardware trusted computing base (TCB) for remote attestation

Patt: Physics-based Attestation of Control Systems (RAID '19)

Patt: Cyber-Physical Remote Attestation for PLCs

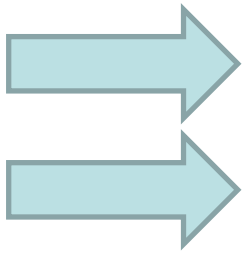


Patt: Cyber-Physical Remote Attestation for PLCs



More Defenses: Physics for the Sake of Security

- **Problem:** Legacy devices (such as PLCs) don't support a hardware trusted computing base (TCB) for remote attestation
- **Problem:** How can we monitor physical semantics in distributed settings?

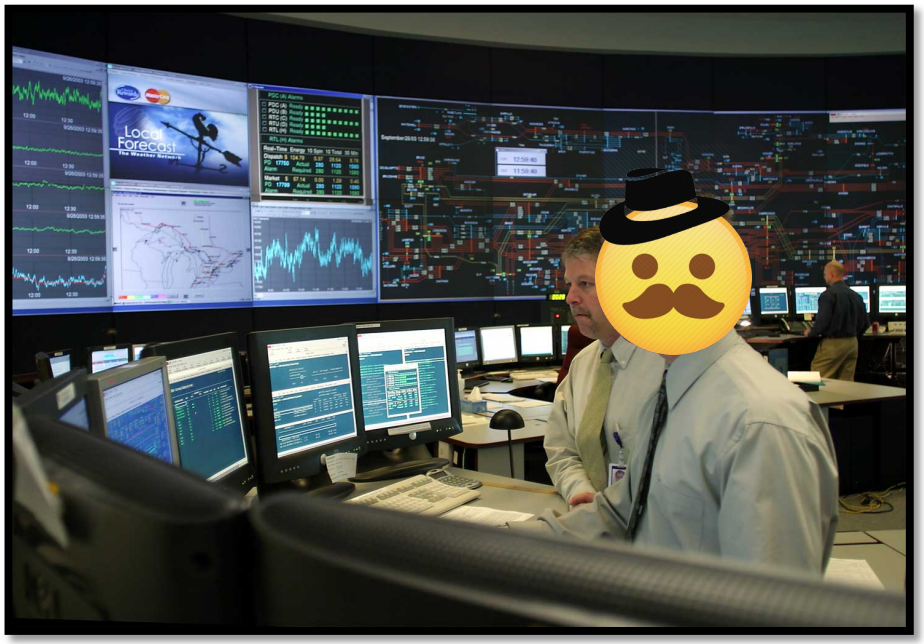


Patt: Physics-based Attestation of Control Systems (RAID '19)

Cyber-physical Control Behavior Integrity (ICCPS '20)

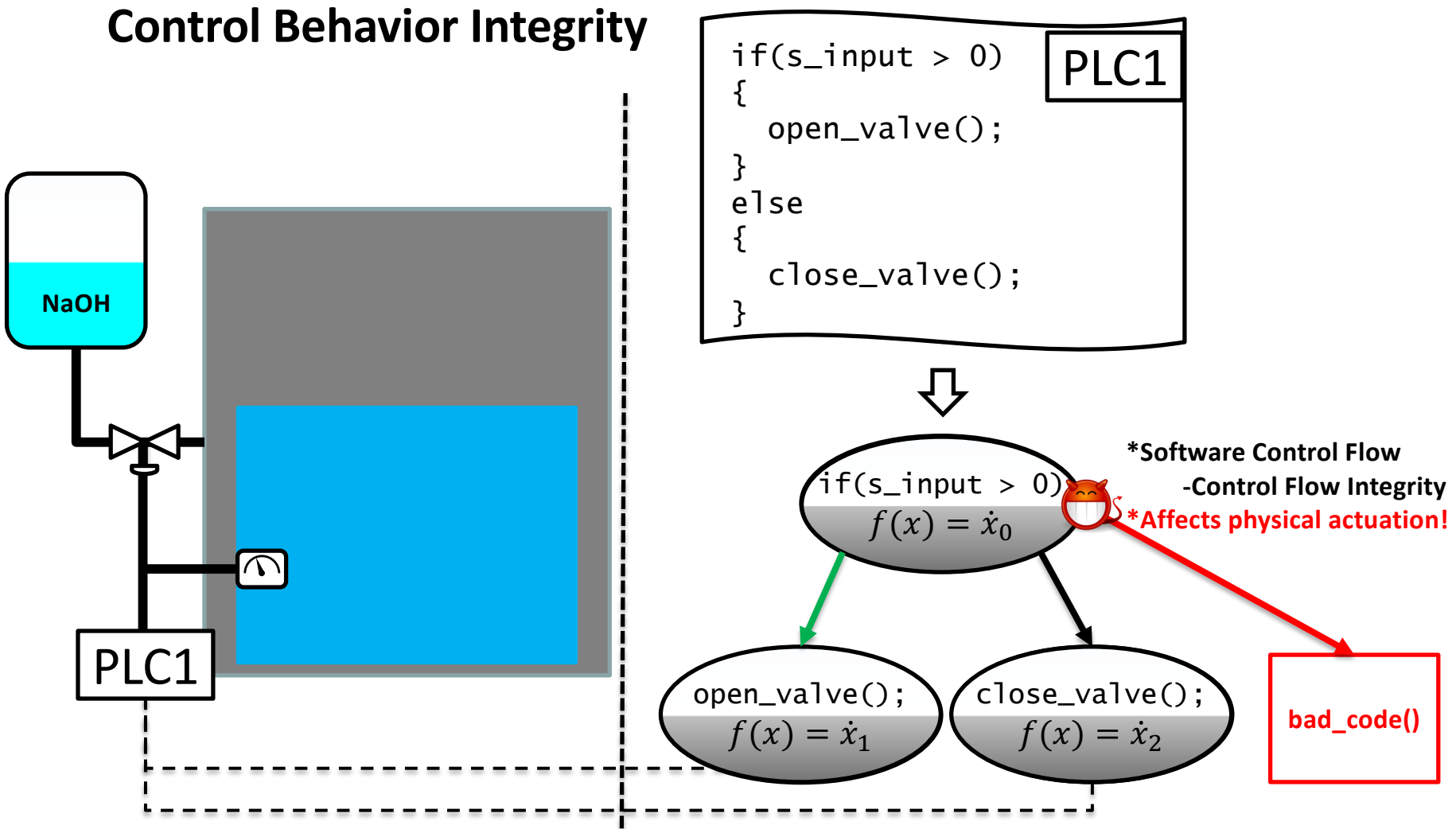
Scadman: Control Behavior Intrusion Detection

- An intrusion detection solution for distributed ICS
- Hybrid model
  - Uses physical state estimation for IDS
  - Updates physical state estimation based on software control flow

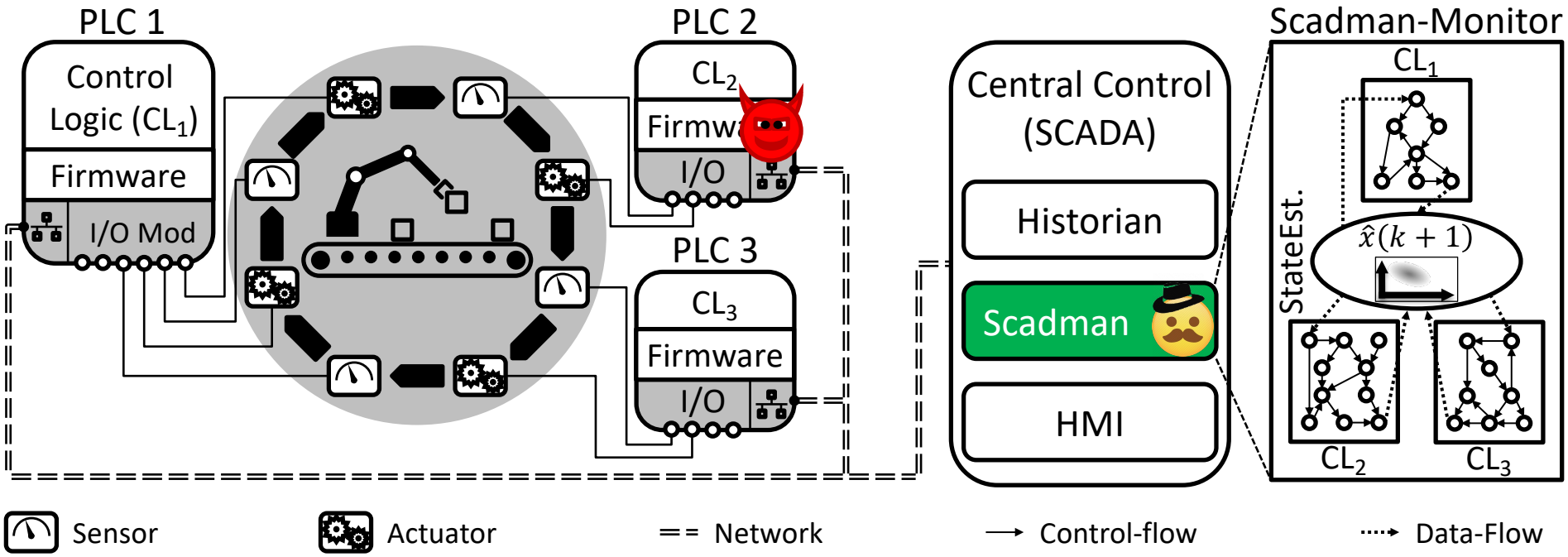


"Control Behavior Integrity for Distributed Cyber-physical Systems," **ICCPS '20**

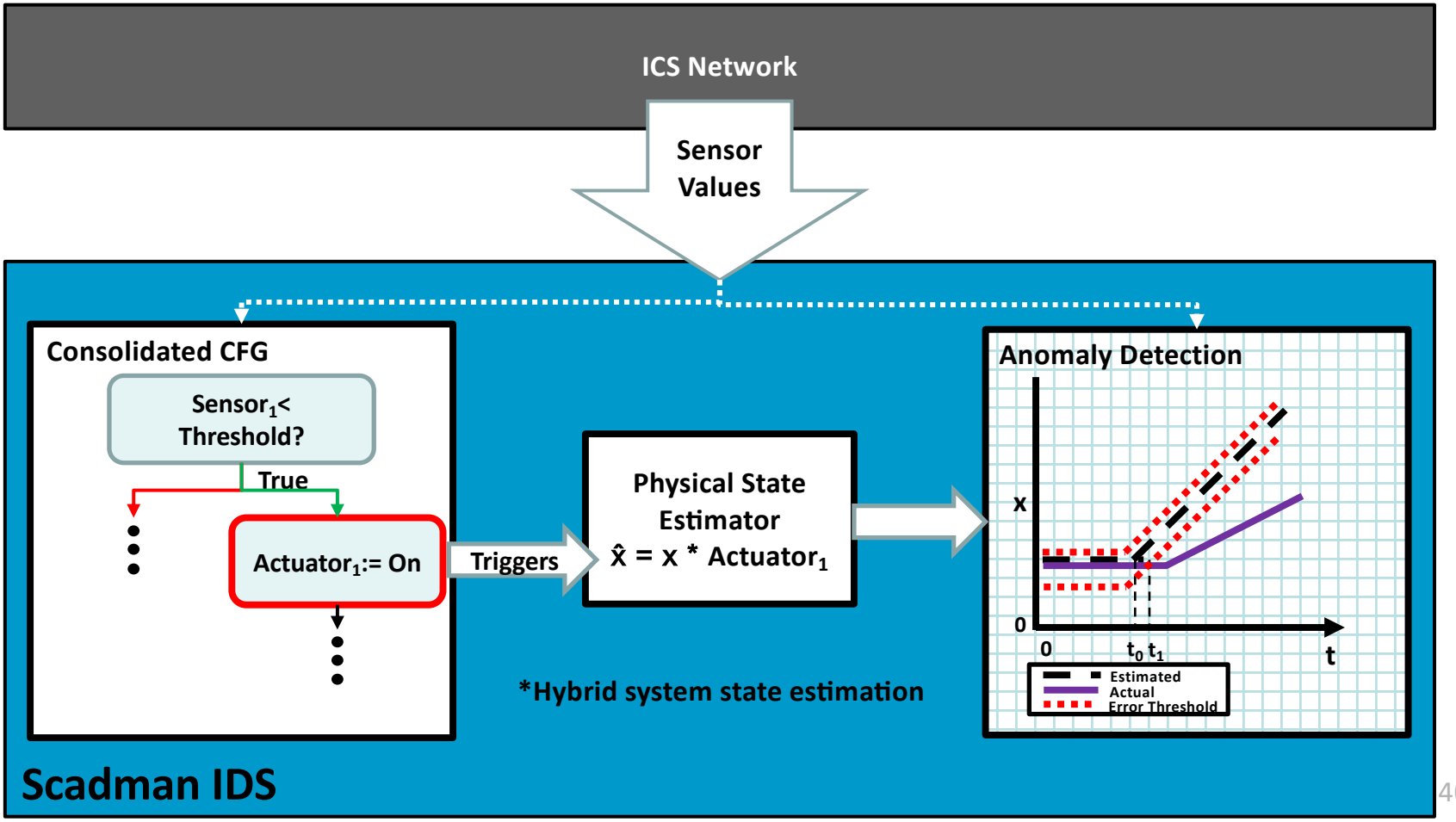
Control Behavior Integrity



Scadman Overview



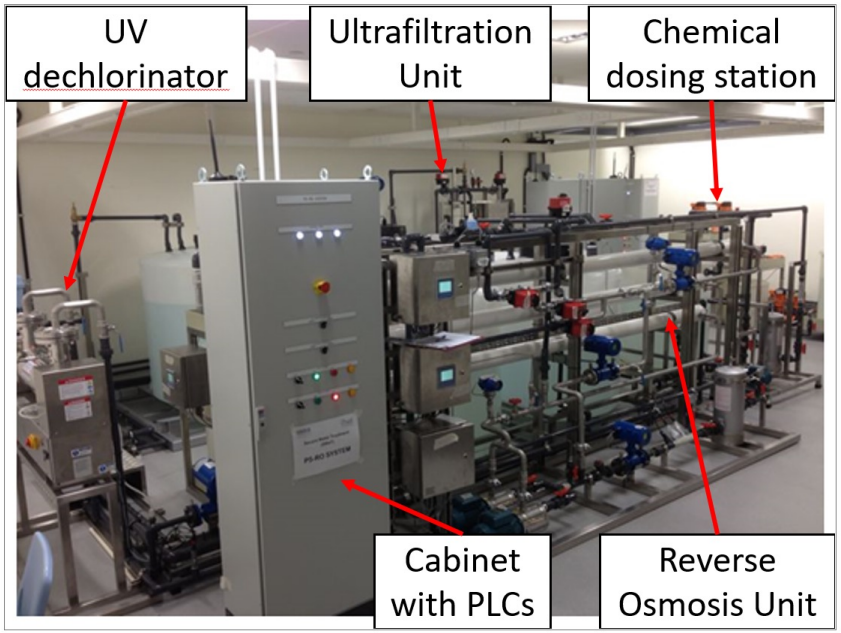
"Control Behavior Integrity for Distributed Cyber-physical Systems," **ICCPS '20**


ICS Network
Sensor Values
Consolidated CFG
Sensor$_1$< Threshold?
True
Actuator$_1$:= On
Triggers
Physical State Estimator
$\hat{X}$ = x * Actuator$_1$
*Hybrid system state estimation
Anomaly Detection
x
0
0
t_0 t_1
t
Estimated
Actual
Error Threshold
Scadman IDS

Evaluation: Water Treatment Testbed

- Evaluated against known set of ICS attacks from
  - 7 days worth of data
  - Multi-point attacks included
- Detected all attacks
  - Also detected faulty sensor data
  - Zero false positives
- No overhead on ICS operation
  - Scadman utilizes historian data

We can effectively monitor software and physical state across a large ICS!



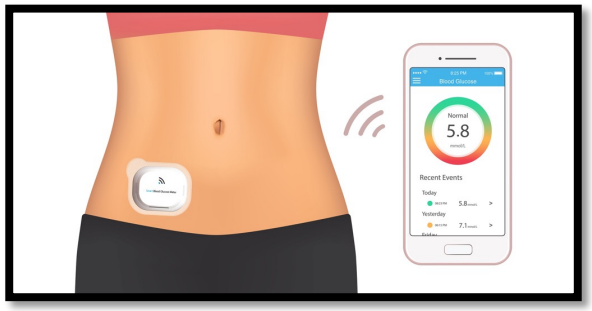
How to do CPS Research in ICS Security

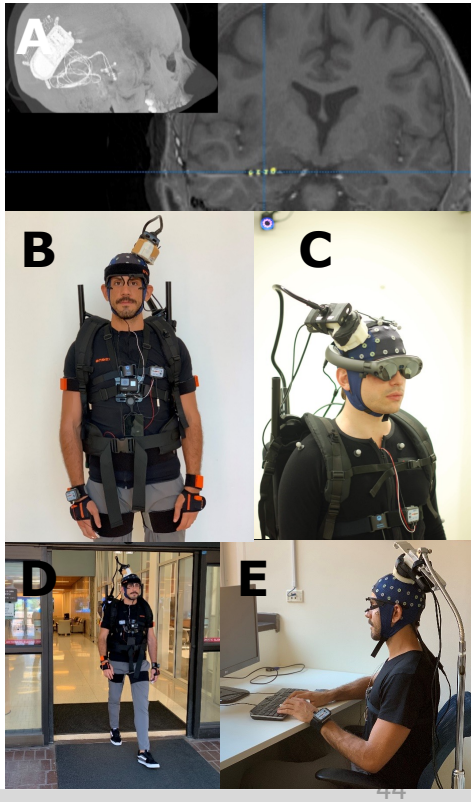
- Simulate small-scale testbeds
  - Add fidelity when necessary
  - Leverage open-source software/simulators that adhere to industrial standards
    - OpenPLC → can run on a Raspberry Pi
    - MiniCPS
    - PyModbus
  - Have a path to validate fidelity of experiments on real testbeds
    - “transitive proof of concept”
  - Be resourceful!
- Leverage existing testbeds through collaboration
  - Go through research papers and see which labs used which testbeds!
- Leverage existing datasets
  - E.g., SUTD has electric power, IoT, secure water treatment, and water distribution datasets with various attack scenarios: https://itrust.sutd.edu.sg/testbeds/

CPS Real-world Attacks Part 2: Medical IoT

Connected Medical Devices Overview

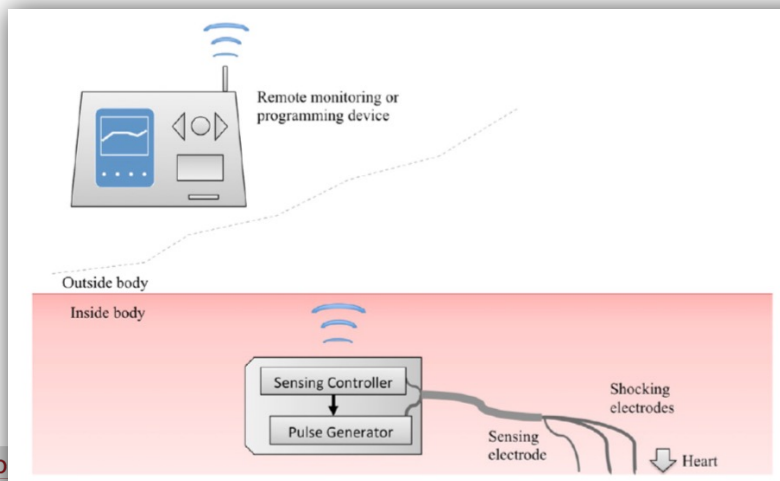
- **Trends**
  - Increasingly common
  - Increasingly complex
- **Characteristics**
  - Severe resource and safety constraints
  - Difficult to replace hardware
- **Increased susceptibility to CPS attacks**
  - Personal information leakage
  - Physical harm to subject

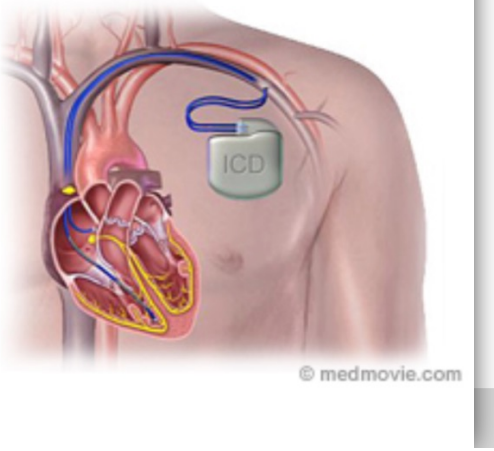




Case Study 1: Implantable Cardioverter Defribrilators

- Delivers electrical pulses to pace the heart
  - Can also send big shock to reset rhythm
- Wireless communication with remote devices
  - Long-range: one-way comms to inform doctor of malfunction
  - Short-range: typically few inches from the patient

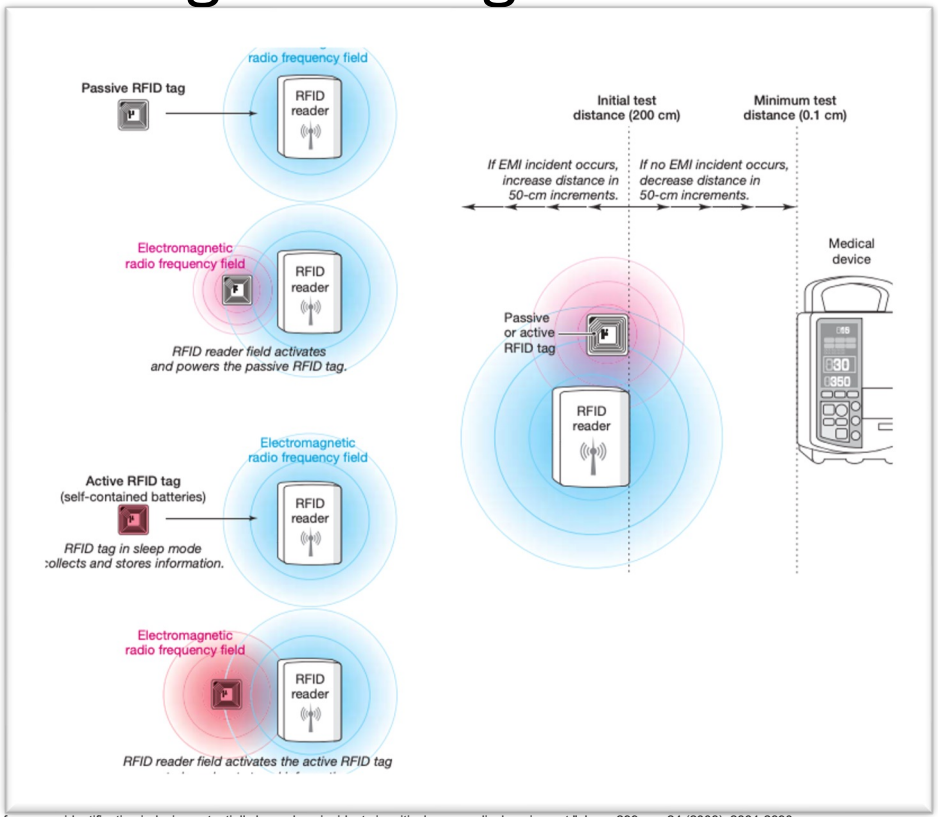




Attack #1: Interference using Radio Signals

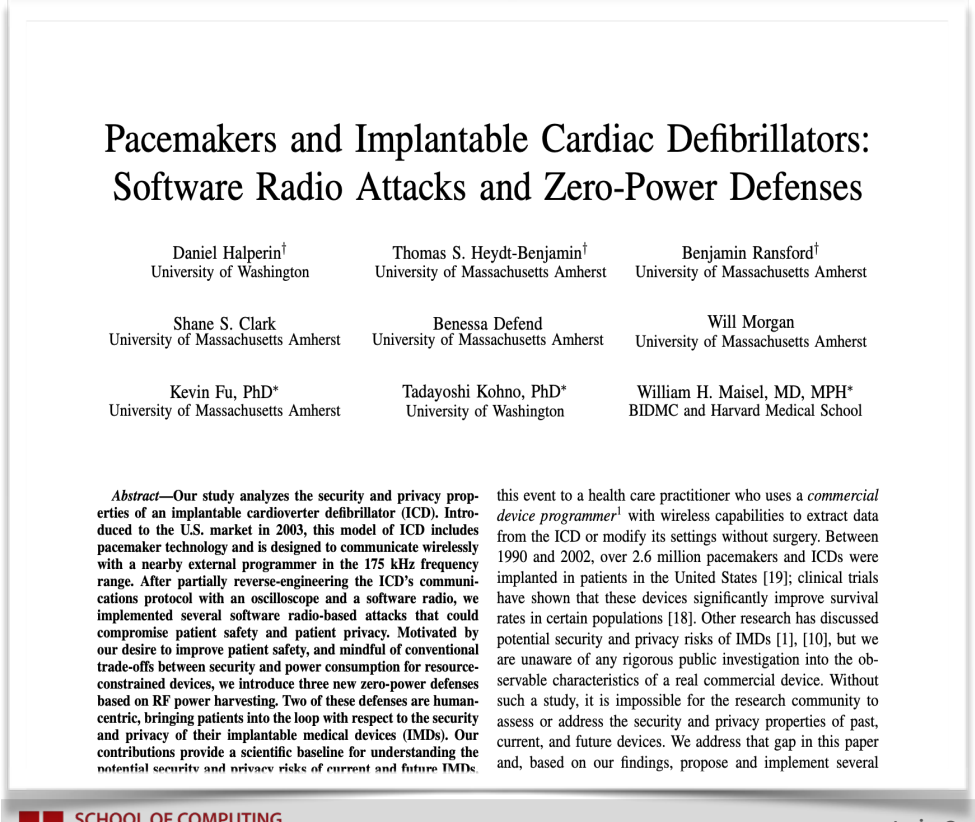
- Place 2 RFID devices near defribrillator to cause EM interference
  - Misinterpreted as a heart signal
  - Similar attack works with syringe pumps, pacemakers ,ventilators, etc.

- Faulty systems can cause damage too!
  - Interference can be done via metal detectors, surveillance devices, etc.
  - 72-year-old man received four shocks next to a store's electronic anti-theft system
    - The defribrilator thought heart was in tachycardia



Van Der Togt, Remko, Erik Jan van Lieshout, Reinout Hensbroek, Euro Beinat, Jan M. Binnekade, and P. J. M. Bakker. "Electromagnetic interference from radio frequency identification inducing potentially hazardous incidents in critical care medical equipment." Jama 299, no. 24 (2008): 2884-2890.

Attack #2: Exploit Wireless Link



Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Daniel Halperin† University of Washington

Thomas S. Heydt-Benjamin† University of Massachusetts Amherst

Benjamin Ransford† University of Massachusetts Amherst

Shane S. Clark University of Massachusetts Amherst

Benessa Defend University of Massachusetts Amherst

Will Morgan University of Massachusetts Amherst

Kevin Fu, PhD* University of Massachusetts Amherst

Tadayoshi Kohno, PhD* University of Washington

William H. Maisel, MD, MPH* BIDMC and Harvard Medical School

***Abstract*—Our study analyzes the security and privacy properties of an implantable cardioverter defibrillator (ICD). Introduced to the U.S. market in 2003, this model of ICD includes pacemaker technology and is designed to communicate wirelessly with a nearby external programmer in the 175 kHz frequency range. After partially reverse-engineering the ICD's communications protocol with an oscilloscope and a software radio, we implemented several software radio-based attacks that could compromise patient safety and patient privacy. Motivated by our desire to improve patient safety, and mindful of conventional trade-offs between security and power consumption for resource-constrained devices, we introduce three new zero-power defenses based on RF power harvesting. Two of these defenses are human-centric, bringing patients into the loop with respect to the security and privacy of their implantable medical devices (IMDs). Our contributions provide a scientific baseline for understanding the potential security and privacy risks of current and future IMDs.**

this event to a health care practitioner who uses a *commercial device programmer*[1] with wireless capabilities to extract data from the ICD or modify its settings without surgery. Between 1990 and 2002, over 2.6 million pacemakers and ICDs were implanted in patients in the United States [19]; clinical trials have shown that these devices significantly improve survival rates in certain populations [18]. Other research has discussed potential security and privacy risks of IMDs [1], [10], but we are unaware of any rigorous public investigation into the observable characteristics of a real commercial device. Without such a study, it is impossible for the research community to assess or address the security and privacy properties of past, current, and future devices. We address that gap in this paper and, based on our findings, propose and implement several

- Wireless communication not encrypted
- Intercept messages
  - Extract device and patient information
- Tamper with therapy settings
- Denial-of-service attack

Defibrillator Attack Summary

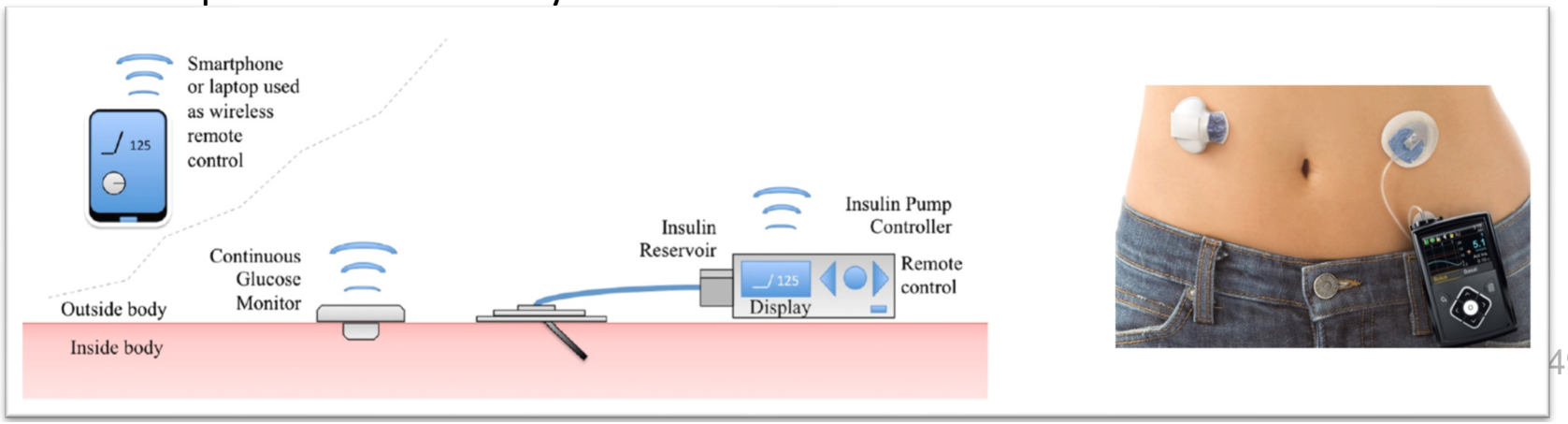
- Hacking a defibrillator is difficult but possible
  - Practical enough to cause concern

"So, when Cheney needed his implanted defibrillator replaced in 2007, Reiner ordered the manufacturer to disable the wireless feature, thus preventing anyone from sending a signal to the device and shocking the vice president into cardiac arrest."

Another Case Study: Insulin Pump

- Delivers Insulin into layer of fat below the skin
  - Control level of glucose

- Digital interface for adjusting infusion rates
  - typical design to minimize mechanical/electrical faults
  - Multiple errors over the years



Attacks on Insulin Pumps

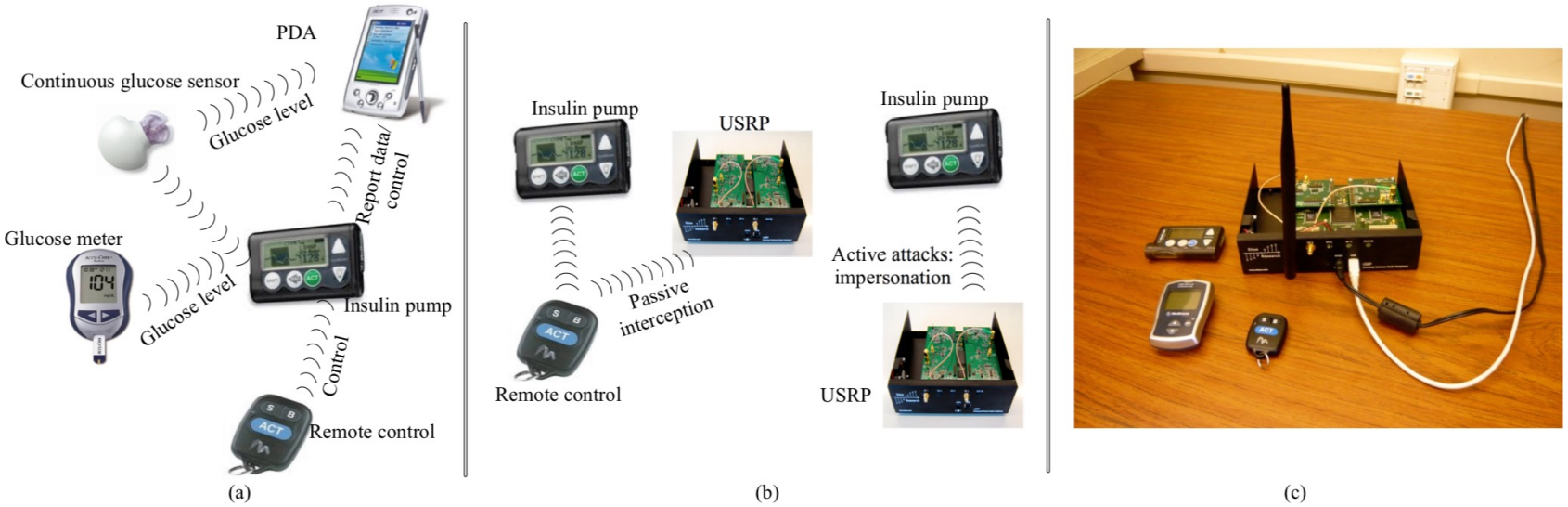
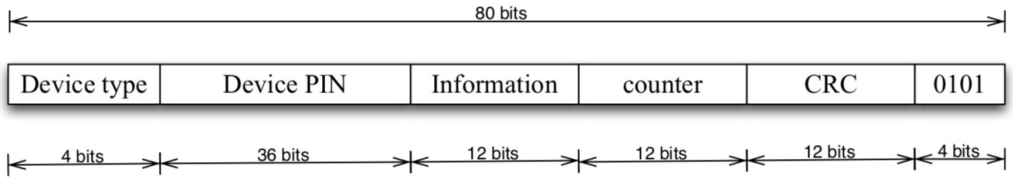


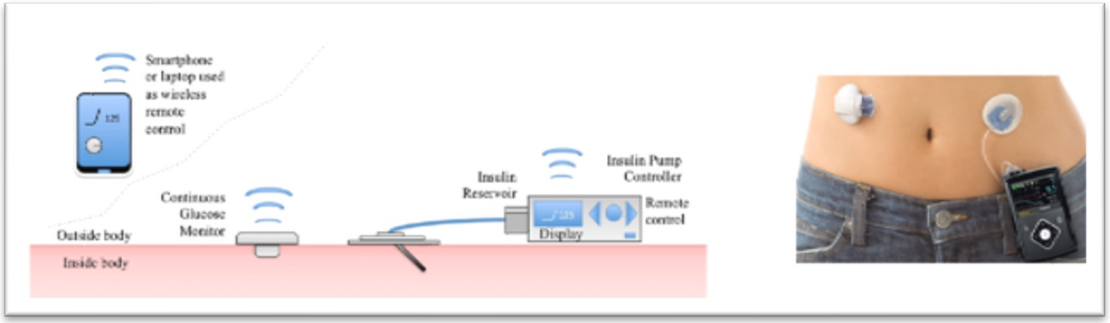
Fig. 1. (a) Insulin delivery system, (b) security attacks, and (c) experimental setup used in the attacks



https://pdfs.semanticscholar.org/ee25/16feb3359d3ba7fe75034dae337429c9fbd5.pdf

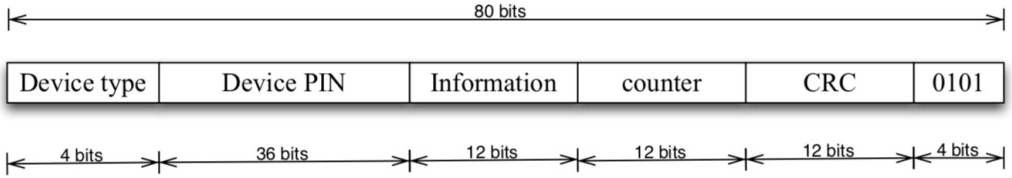
Attacks on Insulin Pump: Without Knowledge of PIN

- Privacy Attacks via eavesdropping
  - Existing of therapy
  - Glucose level
  - Device type + PIN



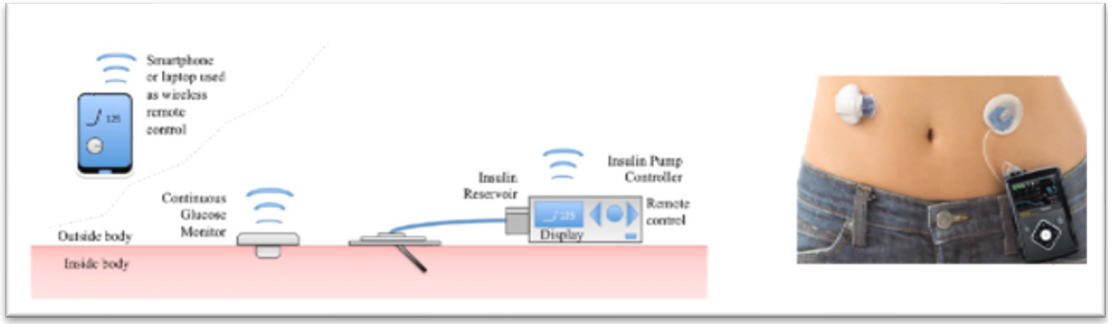
- Integrity attacks
  - **We'll discuss integrity in "Security in a nutshell"**
  - Attacker can still control insulin pump by replaying incorrect "past" glucose reading

- Availability attacks
  - Jamming the wireless channel



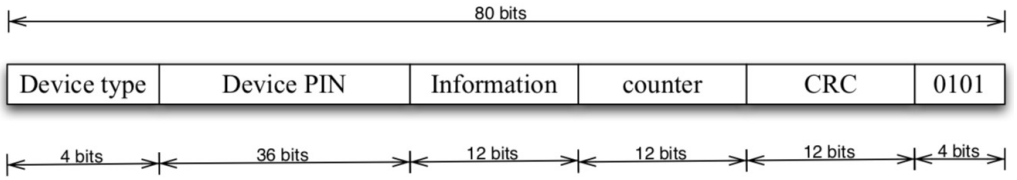
Attacks on Insulin Pump: With Knowledge of PIN

- PIN can be inferred in multiple ways
  - Reverse engineering radio protocol
  - Insider info (or datasheets!)



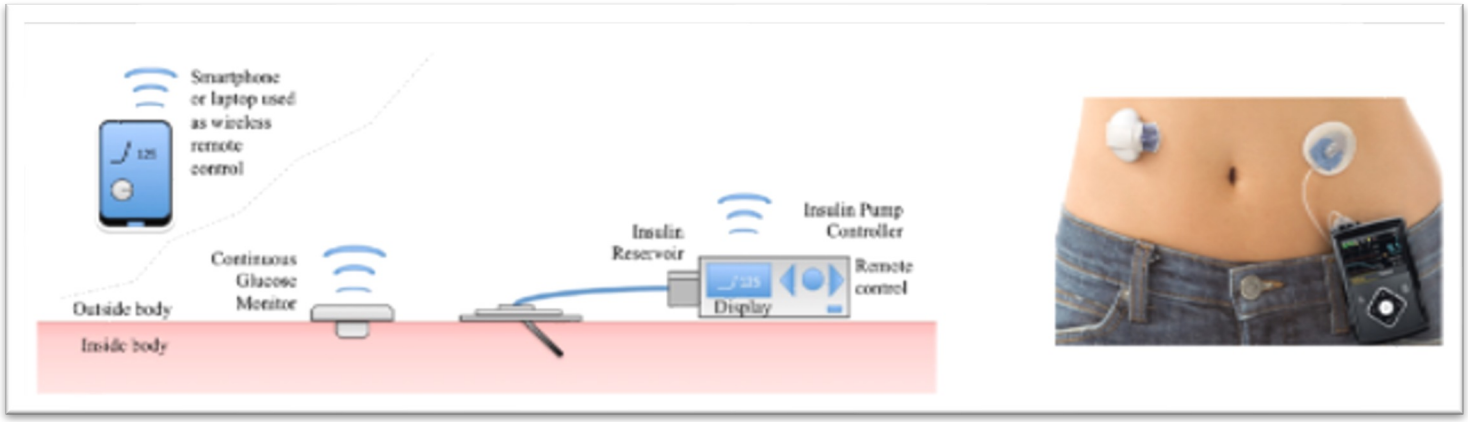
- Remote control's PIN
  - Stop insulin injection
  - Resume insulin injection

- Continous glucose monitor's PIN
  - Report a false reading to the pump and mislead patient into injecting more or less insulin



Attacks on Insulin Pump: Via Smartphone App

- Install malware on phone to change stored glucose values
- Malware could obtain patient info from phone
- Malware could make phone send dangerous control commands to device



Defibrillator Attack Impact

"The flaws primarily stem from a lack of encryption in the communication between the device's two parts: the insulin pump itself and the meter-remote that monitors blood sugar levels and remotely tells the pump how much insulin to administer."

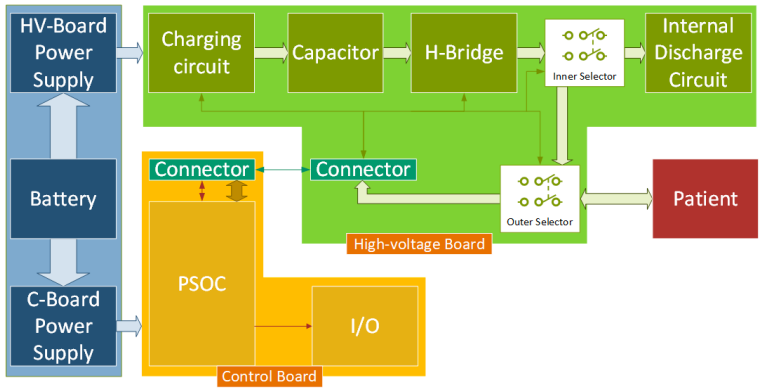
Security challenges in Medical IoT

- **Must communicate wirelessly with outside world**
  - Device's health status→ reconfigure without re-implant
  - Enables vulnerabilities
- **Must be energy efficient**
  - Weaker or no encryption
  - Vulnerable to side-channel power draining attacks (more on that in a later module!)
- **Lots of vulnerabilities**
  - Security by obscurity
  - Unecrypted communication
  - Devices know too much
- **Mutual sensor authentication**
  - How do we authenticate sensors to humans, each other, and vice versa?
  - More on authentication next class!

How to do CPS Research in Medical IoT

- There are several open-source medical IoT device frameworks
  - Development boards are relatively cheap
  - Simulate interacting signals, e.g., through Flipper Zero

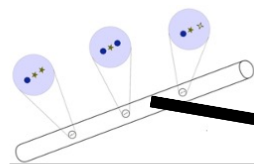
- Leverage existing datasets from other labs
  - Or my lab! (e.g., NeuroIoT framework)

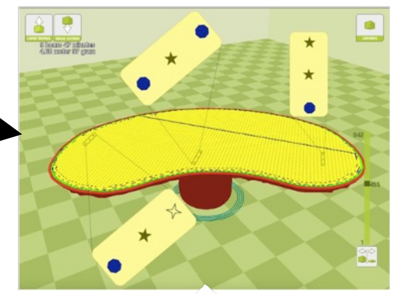


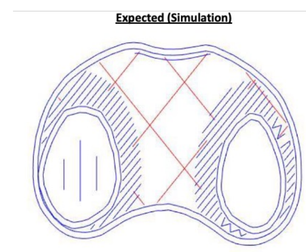
Open-source Defibrillator: https://github.com/CentroEPiaggio/Open-Automated-External-Defibrillator

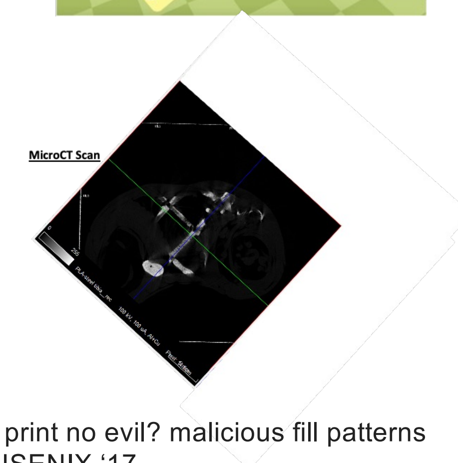
How to do CPS Research in Medical IoT

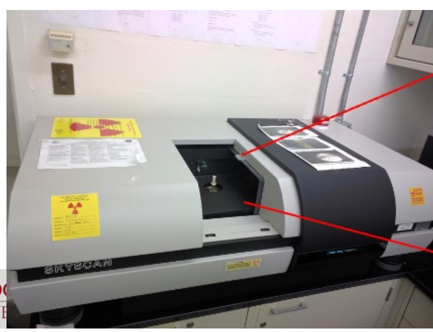
- Be resourceful (and creative)
  - Example: paper on verifying 3D printed medical implants
    - Found open-source repo for medical implant CAD designs
    - Used on-campus microCT scanner
    - Used all the 3D printers in a makerspace to record various benign and malicious prints









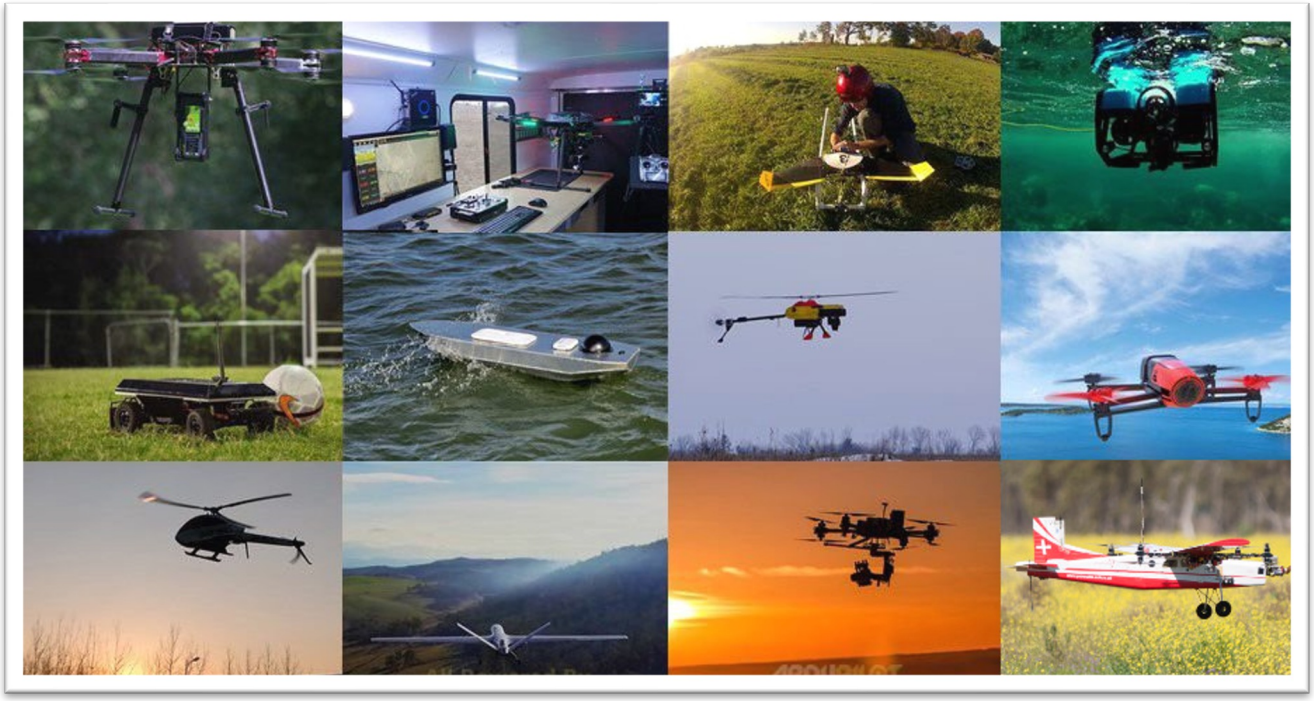


"See no evil, hear no evil, feel no evil, print no evil? malicious fill patterns detection in additive manufacturing." USENIX '17

CPS Real-world Attacks Part 3: Vehicles

* slides in collaboration with Mani Srivastava

Autonomous Vehicles: Not Just Traffic Cars



https://ardupilot.org/

Vehicle Trends: Complex Connectivity

Vehicle-to-Pedestrian (V2P)

e.g., pedestrian in walkway ahead

Vehicle-to-Network (V2N)

e.g., traffic queue in five miles ahead

Vehicle-to-Vehicle (V2V)

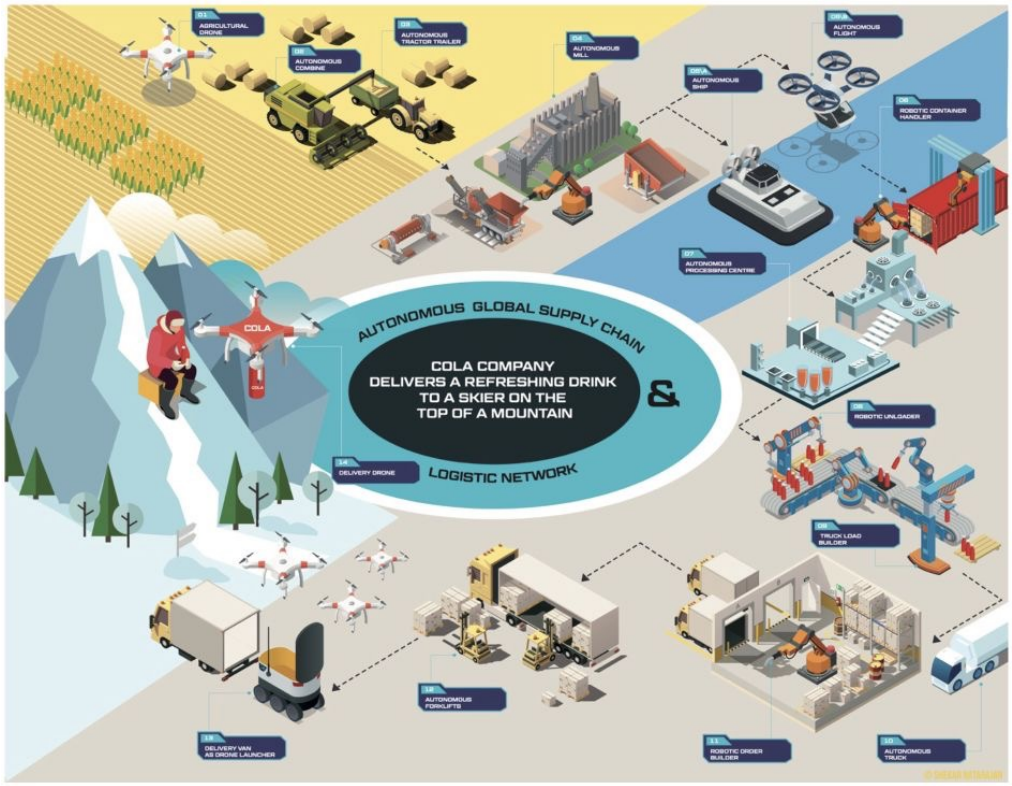
e.g., emergency vehicle approaching

Vehicle-to-Infrastructure (V2P)

e.g., traffic signal ahead turning read

https://embeddedcomputing.com/application/networking-5g/5g-is-paving-the-way-for-autonomous-cars

Vehicle Trends: Autonomous Global Supply Chain

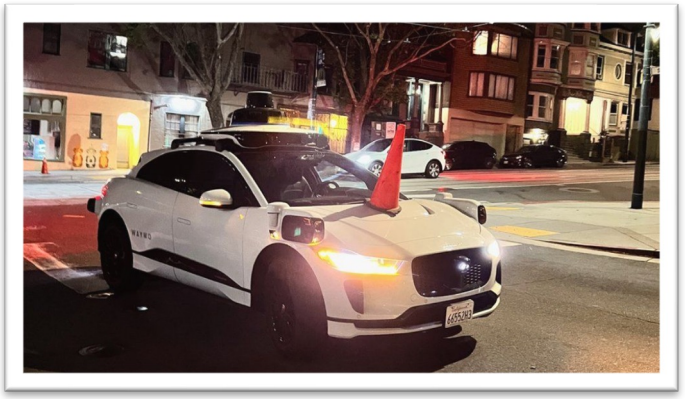


Luis Garcia

https://projectproduction.org/journal/how-autonomous-vehicles-will-disrupt-logistics-and-create-new-business-opportunities/

Vehicle Trends: Increasingly Autonomous in Society

Drone delivery (Australia, coming soon to US)

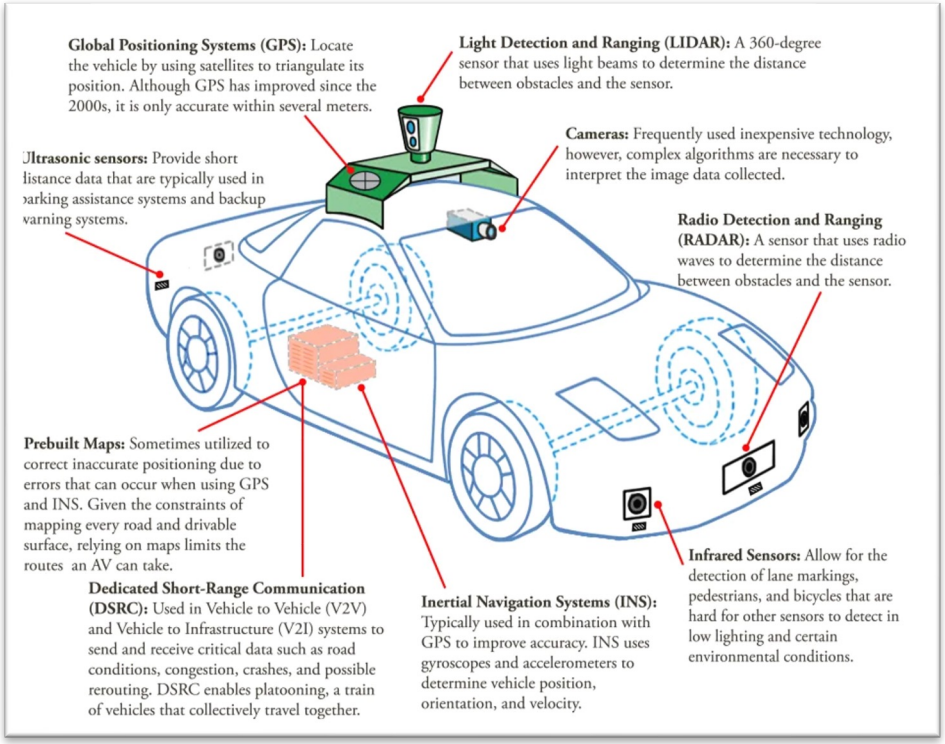


Robotaxis

https://www.bbc.com/news/technology-66611513

Autonomous Vehicle Characteristics

- Increasing number of:
  - Sensors
  - On-board computers
  - Communication systems
- Some of the most complex and difficult systems to secure against CPS
- Increased susceptibility to CPS attacks



Use Case: Car Security

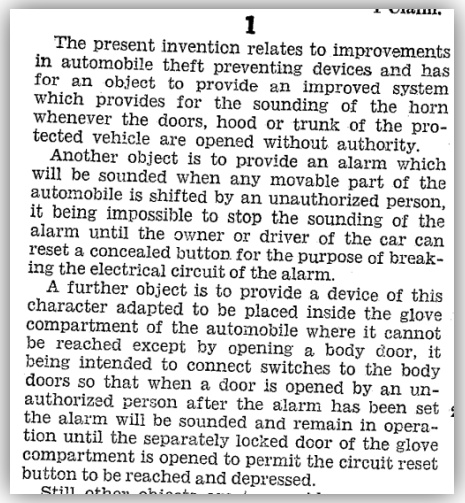
- Physical security keys

https://www.blackknighttracking.com/post/2019/07/10/a-brief-history-of-car-security-systems

Use Case: Physical Car Security

- First recorded theft: 1896
- How would we secure this car?
  - Removable steering wheel
  - Locks (doors, steering wheel, ignition)
  - Alarms

https://www.blackknighttracking.com/post/2019/07/10/a-brief-history-of-car-security-systems



1

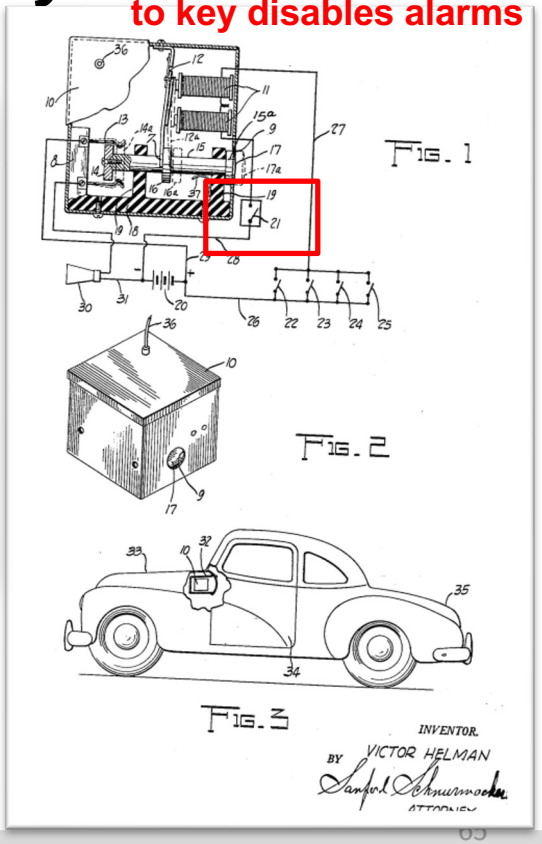
The present invention relates to improvements in automobile theft preventing devices and has for an object to provide an improved system which provides for the sounding of the horn whenever the doors, hood or trunk of the protected vehicle are opened without authority.

Another object is to provide an alarm which will be sounded when any movable part of the automobile is shifted by an unauthorized person, it being impossible to stop the sounding of the alarm until the owner or driver of the car can reset a concealed button for the purpose of breaking the electrical circuit of the alarm.

A further object is to provide a device of this character adapted to be placed inside the glove compartment of the automobile where it cannot be reached except by opening a body door, it being intended to connect switches to the body doors so that when a door is opened by an unauthorized person after the alarm has been set the alarm will be sounded and remain in operation until the separately locked door of the glove compartment is opened to permit the circuit reset button to be reached and depressed.

https://patents.google.com/patent/US2687518

Master switch connected to key disables alarms



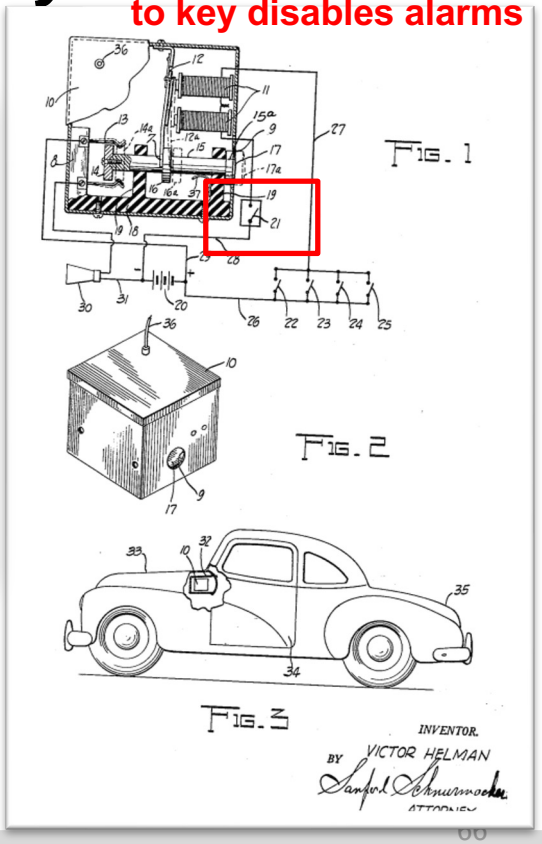
Use Case: Physical Car Security

- First recorded theft: 1896
- How would we secure this car?
  - Remova
  - Locks (d
  - Alarms

1

The present invention relates to improvements in automobile theft preventing devices and has for an object to provide an improved system which provides for the sounding of the horn

Master switch connected to key disables alarms

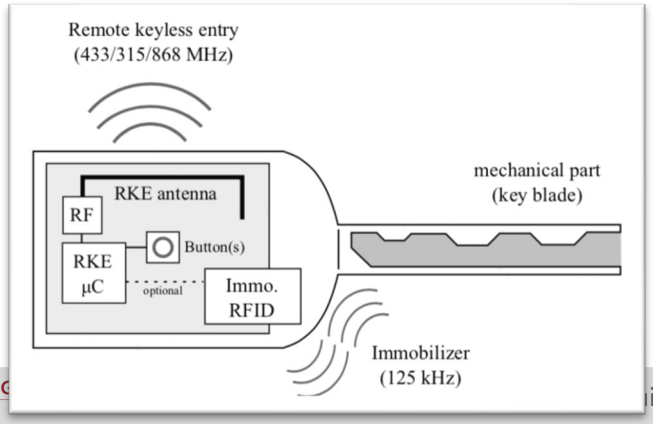


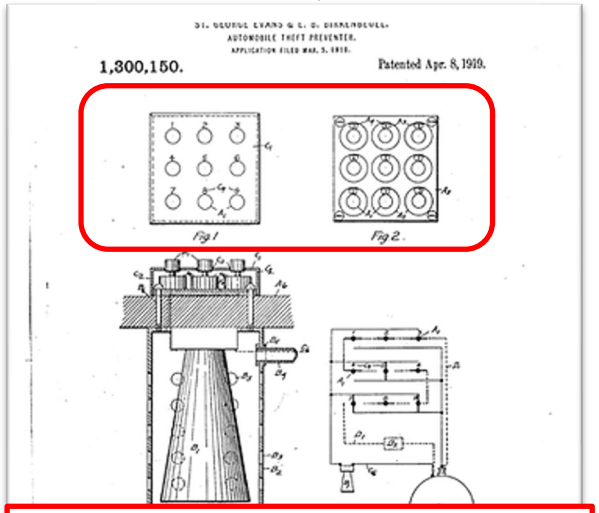
https://www.blackknighttracking.com/post/2019/07/10/a-brief-history-of-car-security-systems

Use Case: Physical Car Security–Immobilization Systems

- **Anti-theft devices** to ensure one can't startup a vehicle's engine without an authentic key
  - Prevent hot-wiring and physical key duplication

- Most modern immobilization systems rely on RFID transponder embedded in plastic shell of key
  - Challenge-response protocol used to establish authenticity





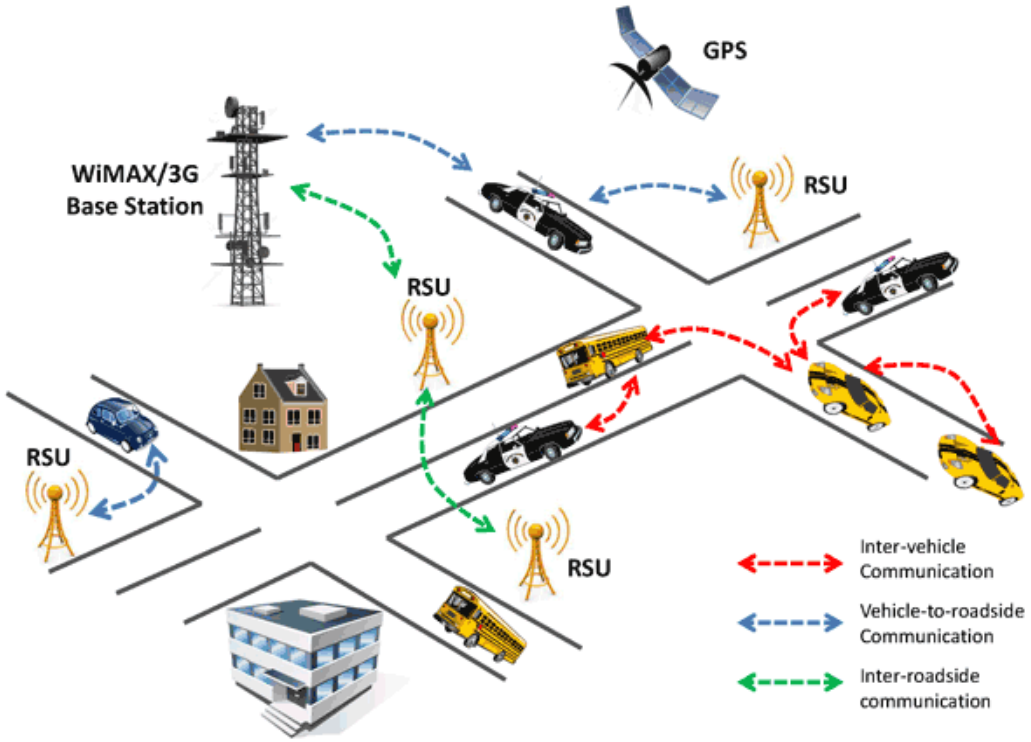
- 3x3 switch panel turned by special key
- Connected to battery, horn, and ignition
- Configuration would divert electricity to horn rather than ignition

https://patents.google.com/patent/US1300150

Common Attack Vectors: Wireless Communication Links

- **Devices in the vehicle** (Bluetooth, wifi, proprietary)
  - Occupant's smartphones, tire pressure sensor
- **Devices near the vehicle** (proprietary)
  - Keys, Garage door
- **Roadside infrastructure** (DSRC)
  - V2V and V2I for traffic control
- **GPS**
  - Location and time information
- **Remote services** (LTE, Wifi)
  - Fleet management, emergency, software and data updates
- **Nearby vehicles: VANET** (DSRC)
  - Safety, coordination, communication

Example: Cars



http://www.its-ukreview.org/building-a-connected-vehicle-testbed-to-study-the-development-and-deployment-of-c-its-in-the-uk/

Example: UAVs

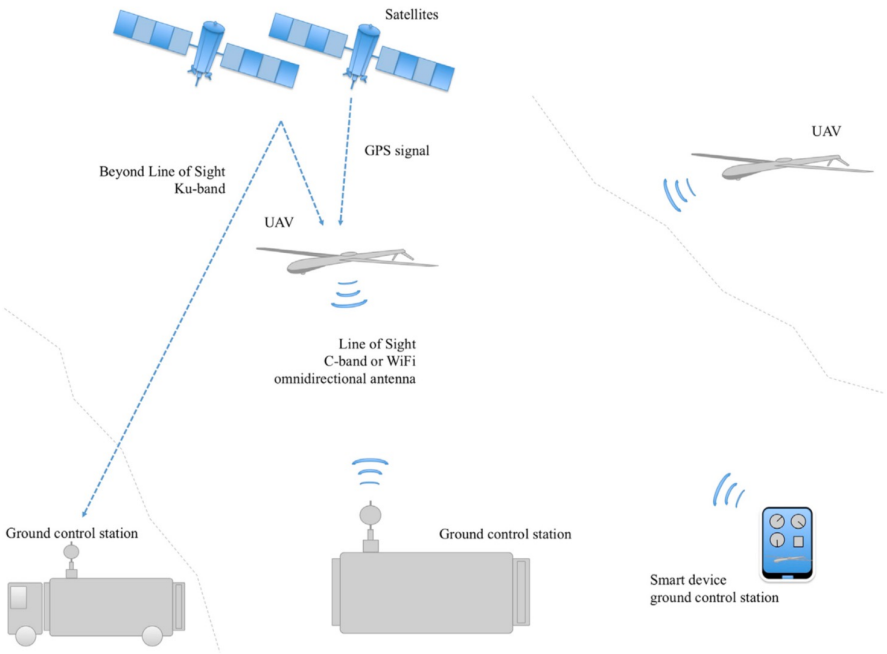


Figure 3.3 Some of the different types of communication involved in the operation of an unmanned aerial system. The example shows two UAVs that are able to communicate with each other, as well as three different ground control stations.

Attacking Wireless Communication Links

- Theoretically straightforward
  - **Disrupt**
    - Noise at the right frequency to jam→ GPS signals are weak and particularly vulnerable
    - Excessive packet traffic (flooding)
  - **Snoop**
    - Reverse-engineering, breaking ciphers, man-in-the-middle
  - **Tamper**
    - Jam + Replay + Replay, Jam + Spoof, Man-in-the-middle
- Cheap to implement!
  - Plenty of low-cost SDRs


USRP

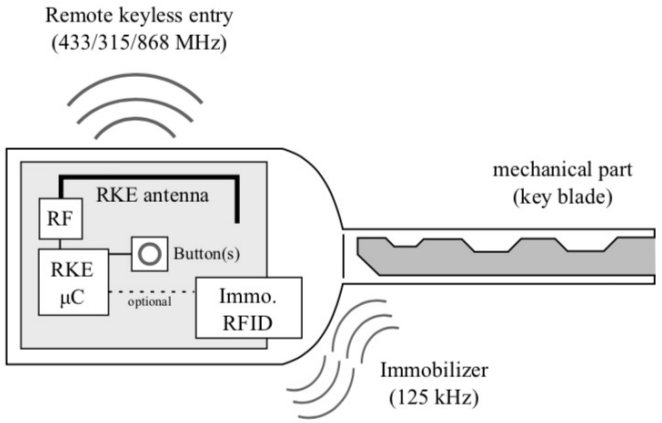
HackRF One


Kiwi SDR

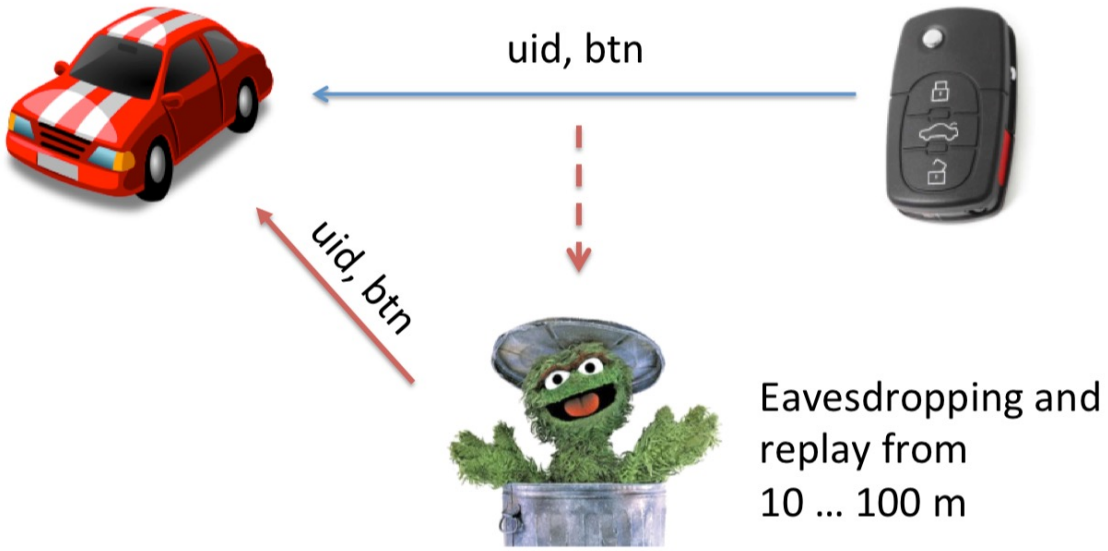

LimeSDR Mini

Use Case: Physical Car Security–Immobilization Systems

- Majority of RFI immobilizers can be cloned due to weak or poorly implemented cryptography
  - Cost, limited-energy on RFID-powered devices
  - Weak keys (especially in older vehicles)
    - Keys of 40b, 48b, 80b, 96b quite common a few years ago (still around!)
    - Can be broken in seconds/minutes with right tools
  - Flawed implementations
    - Effectively few bits of entropy than the key length would suggest



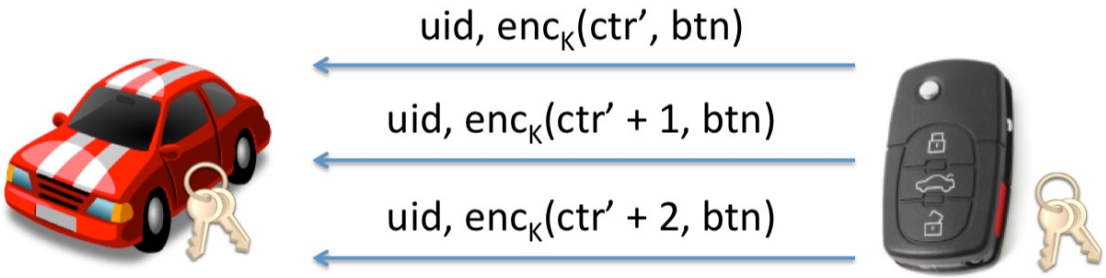
Use Case: Physical Car Security—keyless entry

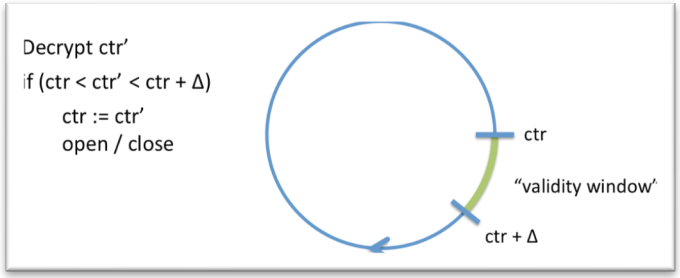


Early Schemes: Fixed Code

Garcia et. al., Usenix Security, 2016

Use Case: Physical Car Security—keyless entry

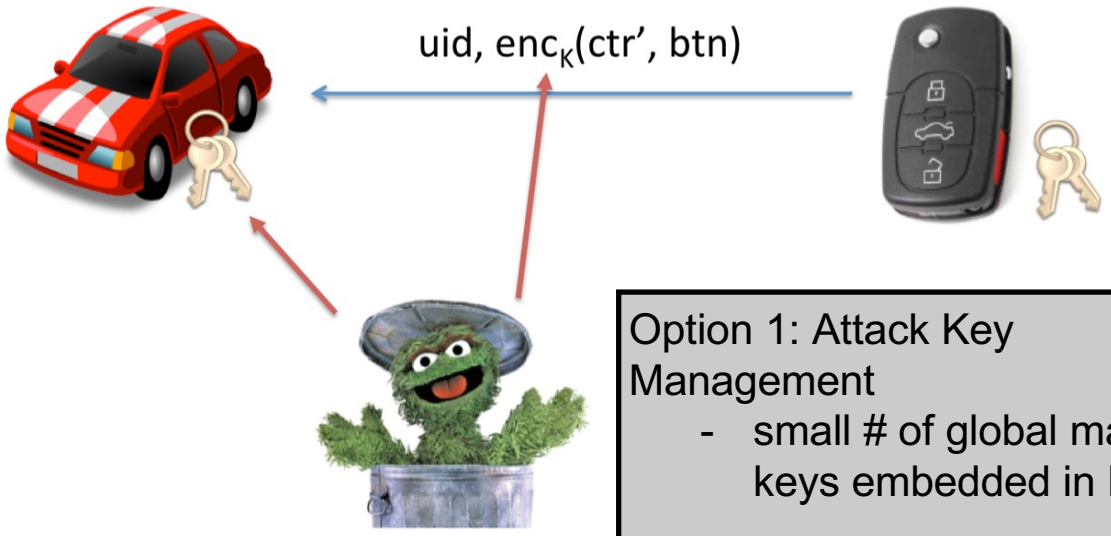




Newer Schemes: Rolling Code

Garcia et. al., Usenix Security, 2016

Use Case: Physical Car Security—keyless entry

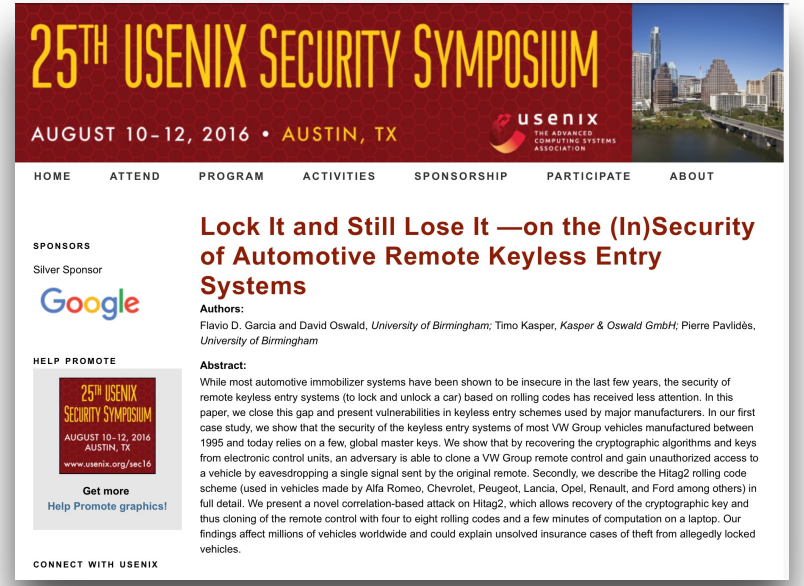


No Replay, But Still Hacked

Option 1: Attack Key Management
- small # of global master keys embedded in ECU

Option 2: Attack Crypto
- side channel attacks
- cryptanalysis

Garcia et. al., Usenix Security, 2016



25TH USENIX SECURITY SYMPOSIUM

AUGUST 10–12, 2016 • AUSTIN, TX

usenix THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

HOME ATTEND PROGRAM ACTIVITIES SPONSORSHIP PARTICIPATE ABOUT

SPONSORS

Silver Sponsor

Google

HELP PROMOTE

25TH USENIX SECURITY SYMPOSIUM
AUGUST 10–12, 2016
AUSTIN, TX
www.usenix.org/sec16

Get more
Help Promote graphics!

CONNECT WITH USENIX

Lock It and Still Lose It —on the (In)Security of Automotive Remote Keyless Entry Systems

Authors:

Flavio D. Garcia and David Oswald, *University of Birmingham;* Timo Kasper, *Kasper & Oswald GmbH;* Pierre Pavlidès, *University of Birmingham*

Abstract:

While most automotive immobilizer systems have been shown to be insecure in the last few years, the security of remote keyless entry systems (to lock and unlock a car) based on rolling codes has received less attention. In this paper, we close this gap and present vulnerabilities in keyless entry schemes used by major manufacturers. In our first case study, we show that the security of the keyless entry systems of most VW Group vehicles manufactured between 1995 and today relies on a few, global master keys. We show that by recovering the cryptographic algorithms and keys from electronic control units, an adversary is able to clone a VW Group remote control and gain unauthorized access to a vehicle by eavesdropping a single signal sent by the original remote. Secondly, we describe the Hitag2 rolling code scheme (used in vehicles made by Alfa Romeo, Chevrolet, Peugeot, Lancia, Opel, Renault, and Ford among others) in full detail. We present a novel correlation-based attack on Hitag2, which allows recovery of the cryptographic key and thus cloning of the remote control with four to eight rolling codes and a few minutes of computation on a laptop. Our findings affect millions of vehicles worldwide and could explain unsolved insurance cases of theft from allegedly locked vehicles.

wired.com

WIRED A New Wireless Hack Can Unlock 100 Million Volkswagens SUBSCRIBE

BUSINESS CULTURE DESIGN GEAR SCIENCE SECURITY TRANSPORTATION

SHARE

SHARE 29024

TWEET

COMMENT 22

EMAIL

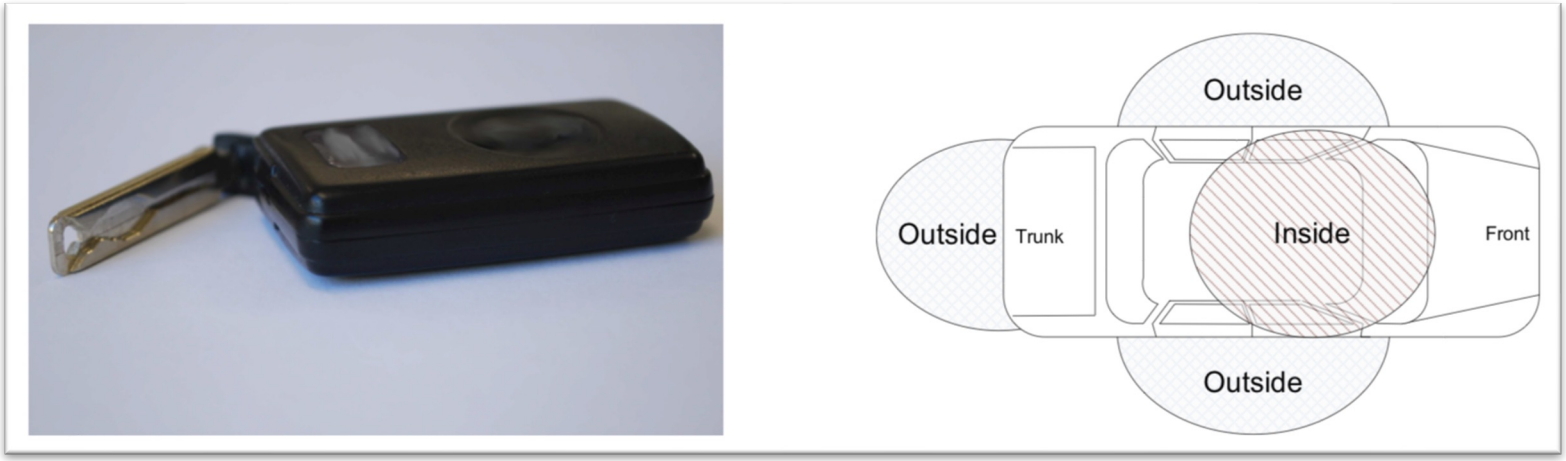
ANDY GREENBERG SECURITY 08.10.16 4:29 PM

A NEW WIRELESS HACK CAN UNLOCK 100 MILLION VOLKSWAGENS

KAZUHIRO NOGI/AFP/GETTY IMAGES

Passive Remote Keyless Entry (and Start) Systems

- Detects proximity to car: no button press required
  - When in proximity to the vehicle, the car key generates a cryptographic response to a challenge transmitted by the car



Francillon, Aurélien, Boris Danev, and Srdjan Capkun. "Relay attacks on passive keyless entry and start systems in modern cars." In IN PROCEEDINGS OF THE 18TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM. THE INTERNET SOCIETY. 2011.

Passive Remote Keyless Entry (and Start) Systems

- Detects proximity to car: no button press required
  - When in proximity to the vehicle, the car key generates a cryptographic response to a challenge transmitted by the car

- Vulnerable to **relay attack**

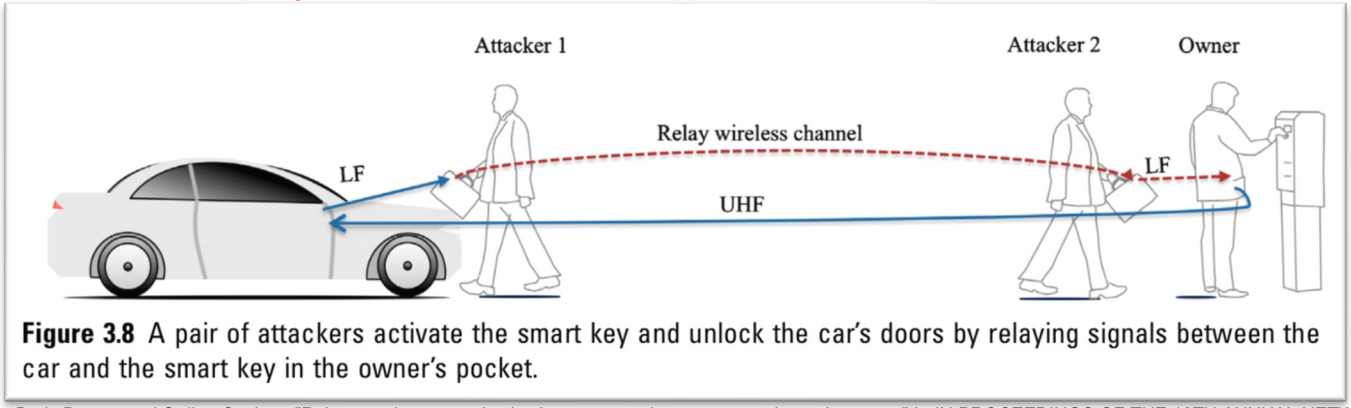
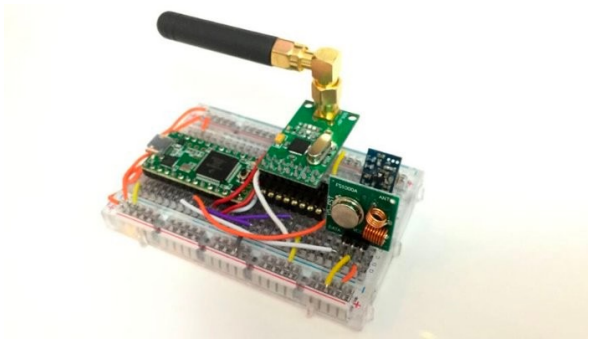
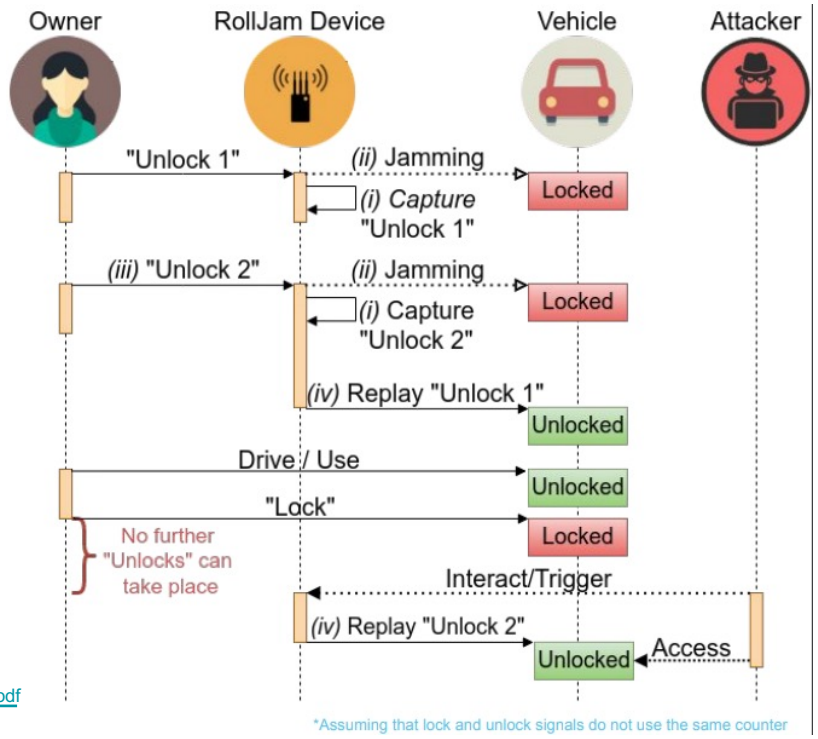


Figure 3.8 A pair of attackers activate the smart key and unlock the car's doors by relaying signals between the car and the smart key in the owner's pocket.

Francillon, Aurélien, Boris Danev, and Srdjan Capkun. "Relay attacks on passive keyless entry and start systems in modern cars." In IN PROCEEDINGS OF THE 18TH ANNUAL NETWORK AND DISTRIBUTED SYSTEM SECURITY SYMPOSIUM. THE INTERNET SOCIETY. 2011.

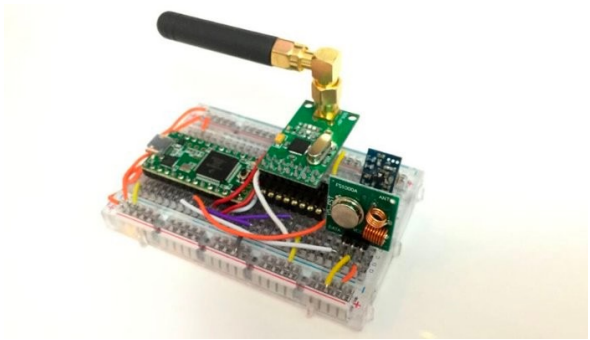
More Advanced and easy-to-use Attacks Recently: Rolljam + Rollback

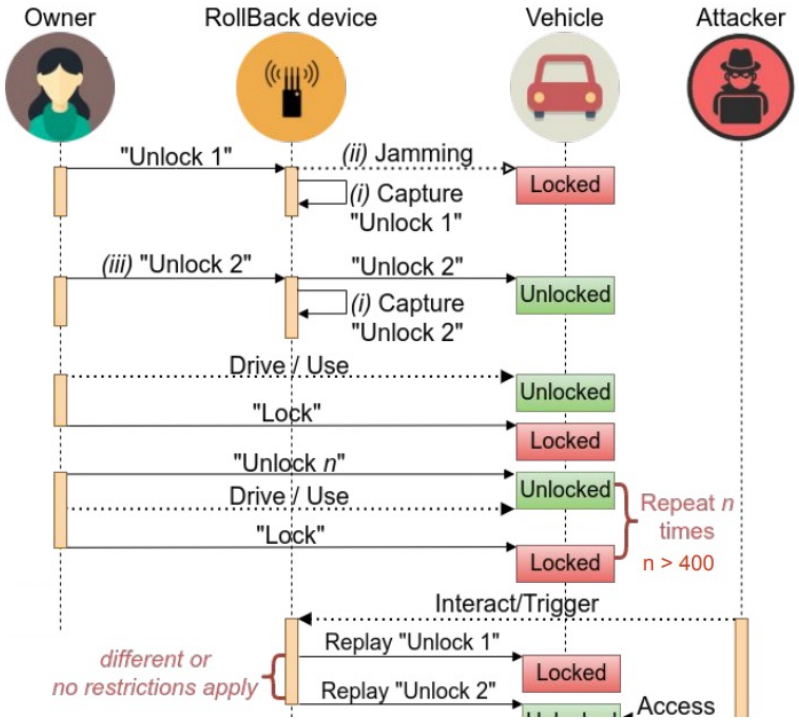




https://i.blackhat.com/USA-22/Thursday/US-22-Csikor-RollBack-A-New-Time-Agnostic-Replay-Attack.pdf

More Advanced and easy-to-use Attacks Recently: Rolljam + Rollback





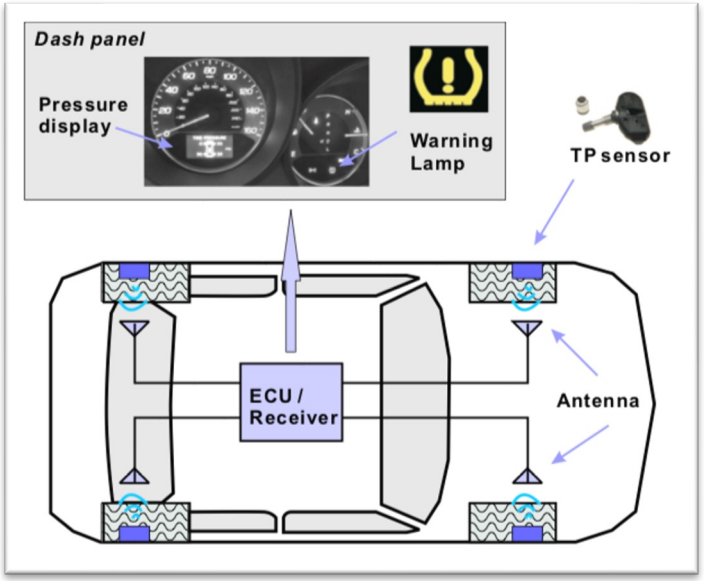
https://i.blackhat.com/USA-22/Thursday/US-22-Csikor-RollBack-A-New-Time-Agnostic-Replay-Attack.pdf

Common Attack Vector: Sensors

- **Vehicle's internal state**
  - Health of subsystems, tire pressure, fuel level, speed, wheel slippage,...
- **State of occupants**
  - Activation of airbag, fatigue, attention,...
- **Vehicle's external state**
  - Nearby cars, people, animals, obstacles,...
- **Many different ways to attack**
  - Compromised vehicle software (ECU firmware)
  - Injecting corrupted signals
  - Physical alteration

Use Case: Wireless Tire Pressure Monitoring System

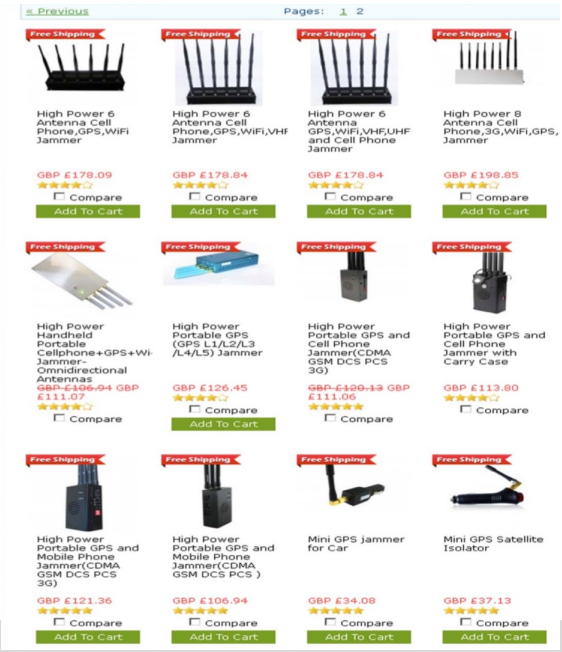
- Communications based on standard modulation schemes/protocols
  - Spoofing, battery drain attacks easily mounted
- Significant communication range
  - Attacker can overhear or spoof transmissions from the road-side
- Vehicle tracking using the unique identifier for each sensor
  - Privacy, targeted roadside attacks, etc.



Rouf, Ishtiaq, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. "Security and privacy vulnerabilities of {In-Car} wireless networks: A tire pressure monitoring system case study." In *19th USENIX Security Symposium (USENIX Security 10)*. 2010.

Attack Vector: GPS Jamming

- Jamming: Cheap and Easy
  - Jam GPS signals within a certain surrounding area
  - Marketed as a “personal privacy device”
  - Used to cheat toll/insurance, evade tracking, bypass drone flying restrictions,…



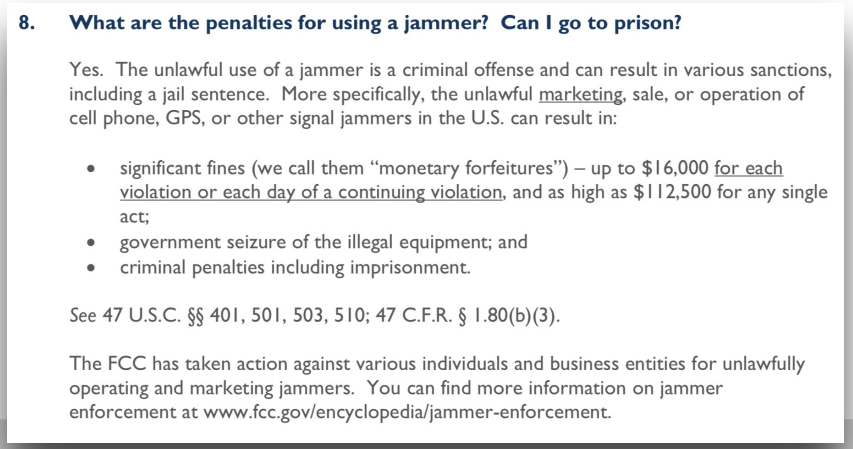
Attack Vector: GPS Jamming

- Jamming: Cheap and Easy**... but illegal and dangerous**
  - Many safety-critical systems use GPS for navigation (airplane landing, 911 response, drones, ...)

- Illegal to market, sell, buy, or use

In June 2015, planes flying into Northeast Philadelphia Airport kept reporting that they were losing the GPS signal on the last mile of their approach.

In June 2015, planes flying into Northeast Philadelphia Airport kept reporting that they were losing the GPS signal on the last mile of their approach. An agent from the Federal Communications Commission (FCC), which enforces prohibitions against jammers, came to investigate and discovered a truck in a nearby parking lot. The driver said that he was using a jammer to disable a tracking device in his vehicle, and that he hadn't realized the jammer was illegal. According to a governmental aviation safety report, the agent "confiscated the jamming unit and destroyed it with a sledge hammer."



8. What are the penalties for using a jammer? Can I go to prison?

Yes. The unlawful use of a jammer is a criminal offense and can result in various sanctions, including a jail sentence. More specifically, the unlawful marketing, sale, or operation of cell phone, GPS, or other signal jammers in the U.S. can result in:

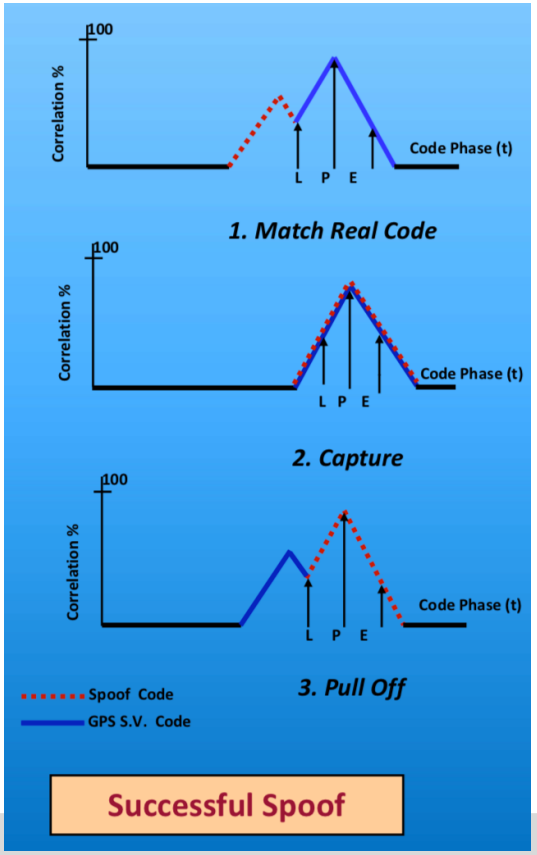
- significant fines (we call them "monetary forfeitures") – up to $16,000 for each violation or each day of a continuing violation, and as high as $112,500 for any single act;
- government seizure of the illegal equipment; and
- criminal penalties including imprisonment.

See 47 U.S.C. §§ 401, 501, 503, 510; 47 C.F.R. § 1.80(b)(3).

The FCC has taken action against various individuals and business entities for unlawfully operating and marketing jammers. You can find more information on jammer enforcement at www.fcc.gov/encyclopedia/jammer-enforcement.

Attack Vector: GPS Spoofing

- Easy to generate counterfeit signals
- Widely available signal generators



http://www.atis.org/01_news_events/webinar-pptslides/IsGPSMoreVulnerable_Webinar_3082017.pdf

Attack Vector: GPS Spoofing

SCIENCE & TECHNOLOGY

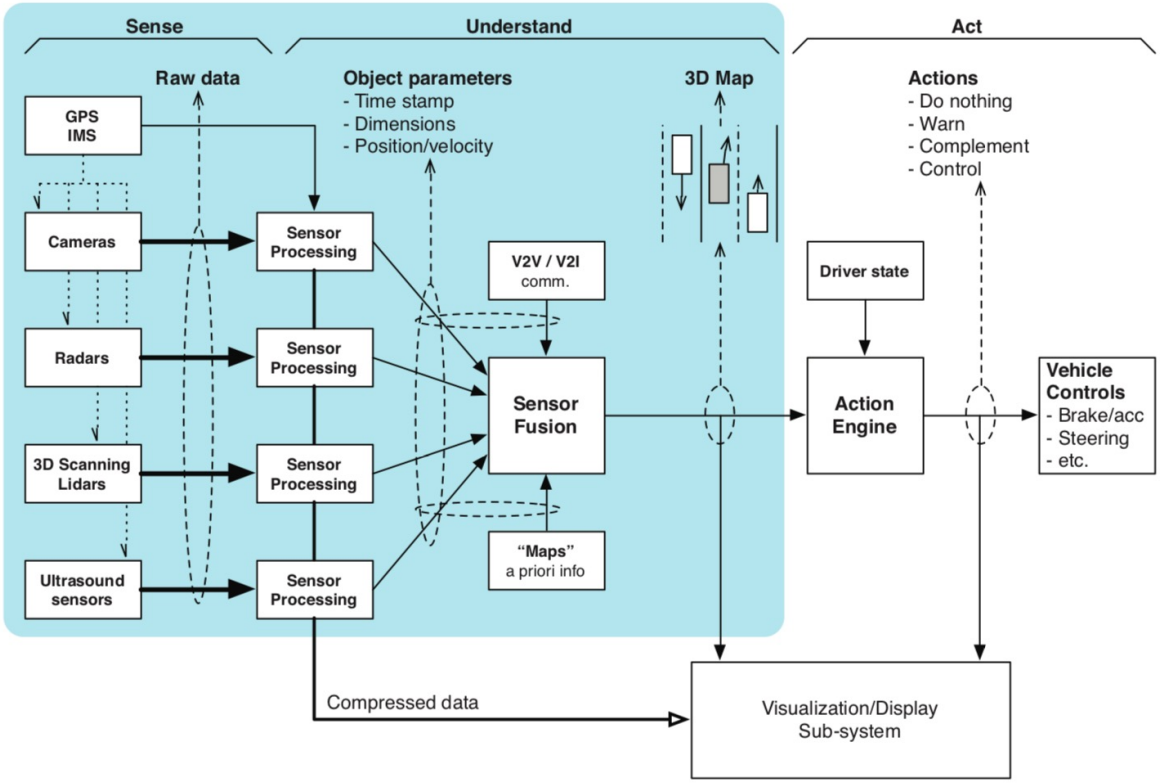
Jul 29, 2013

UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea

This summer, a radio navigation research team from The University of Texas at Austin set out to discover whether they could subtly coerce a 213-foot yacht off its course, using a custom-made GPS device.

Attack Vector: Car Sensors

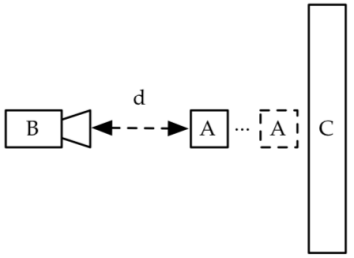
- Front/rear/side attack
- Roadside attack
- Evil mechanic attack

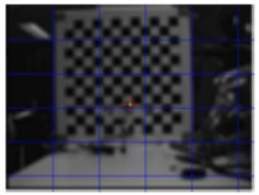


https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

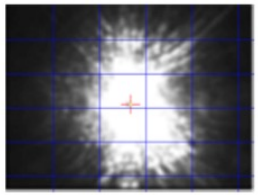
Attacking Cameras in Cars: Blinding

MobilEye C2-270

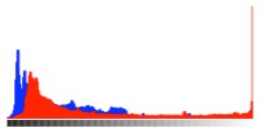




(a) Laser off



(b) Laser on



(c) Tonal distribution

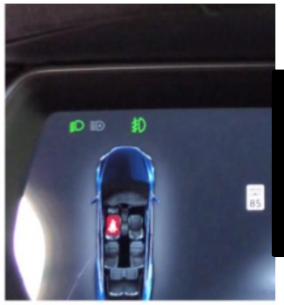
https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf

Attacking Cameras: Fooling Perception

Hackers can trick a Tesla into accelerating by 50 miles per hour

A two inch piece of tape fooled the Tesla's cameras and made the car quickly and mistakenly speed up.

By Patrick Howell O'Neill February 19, 2020

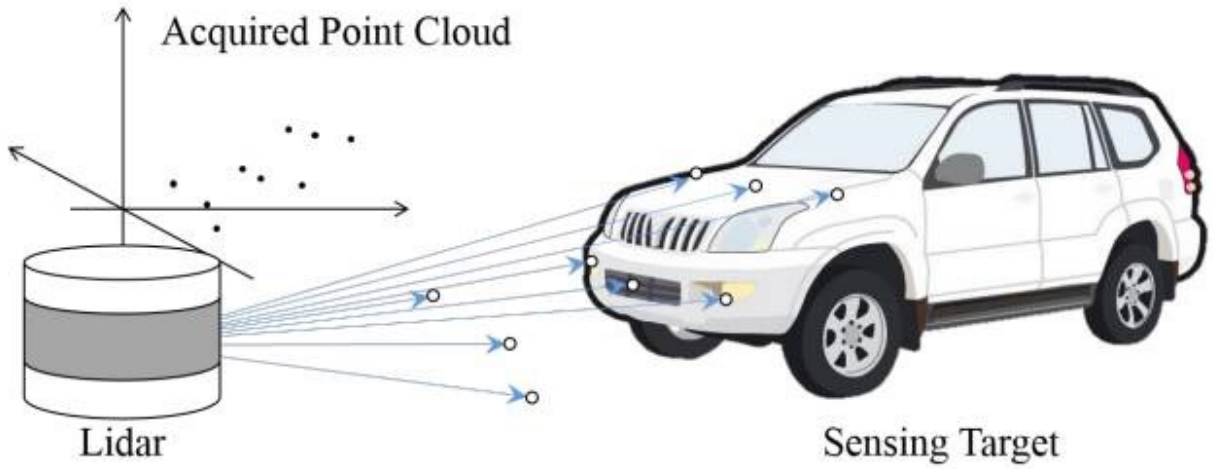


Human sees this as "35"
Car sees this "85"

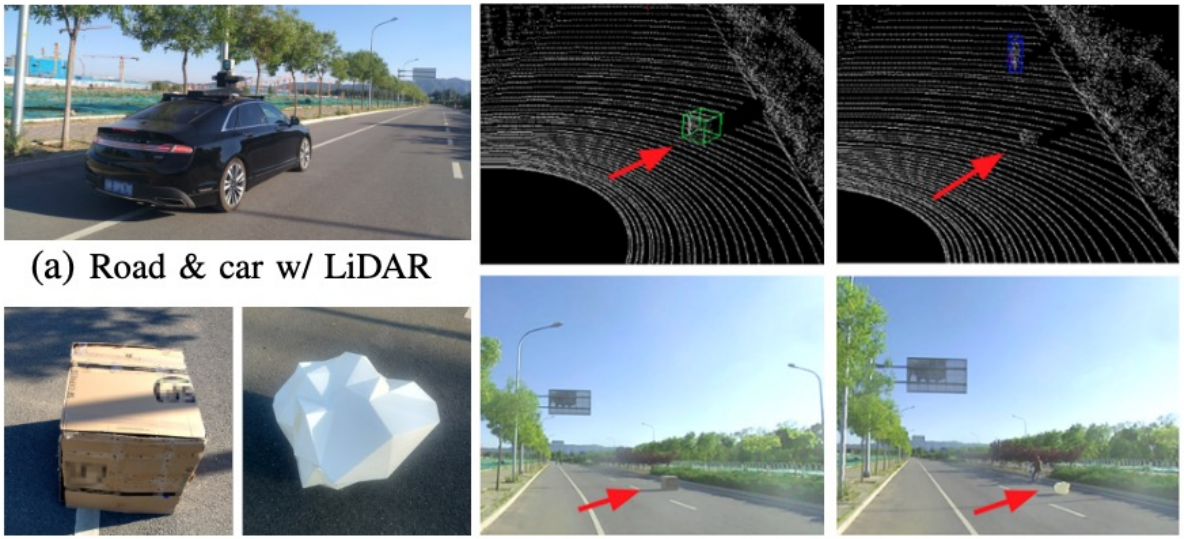
More on adversarial machine learning in the sensor perception security lecture!

Is the answer LIDAR?

- LIDAR gather distances to objects by firing a pulsed laser at them and collating reflections



LIDAR has also been attacked in many different ways!



(a) Road & car w/ LiDAR

(b) Benign and adv. cubes (c) Benign case (d) Adversarial case

https://arxiv.org/pdf/2106.09249.pdf

We'll cover
physical adversarial machine learning
attacks later

So Many Ways a Vehicle Interacts with an Environment

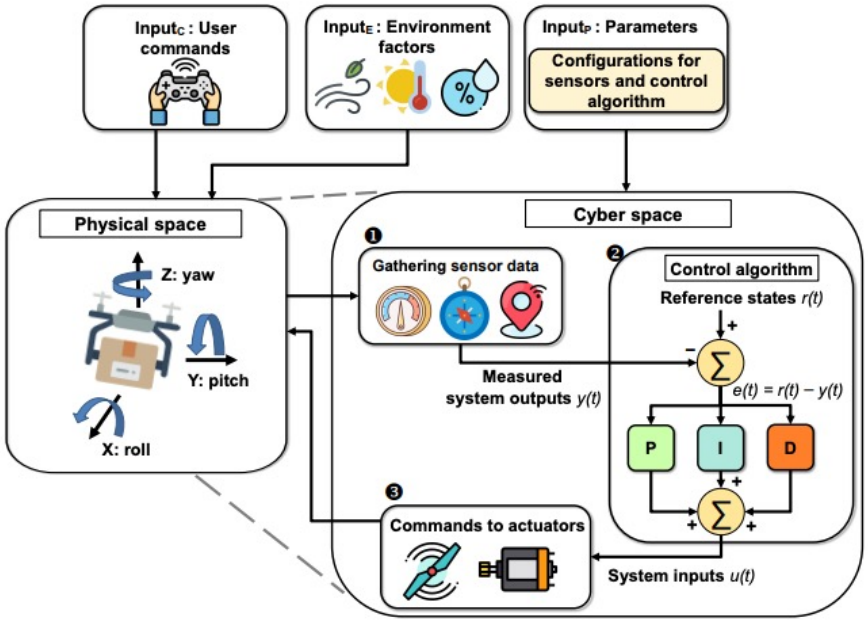


Fig. 1: Workflow of RV's control software.

https://www.ndss-symposium.org/wp-content/uploads/ndss2021_6A-1_24096_paper.pdf

Attacks on Sensors: Knocking Drones Out of the Sky with Sound Waves

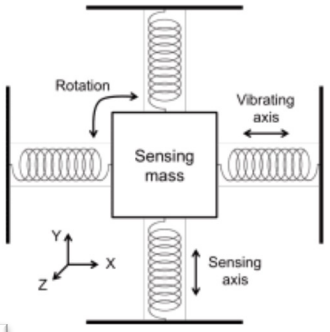


Table 4: Result of attacking two target drones

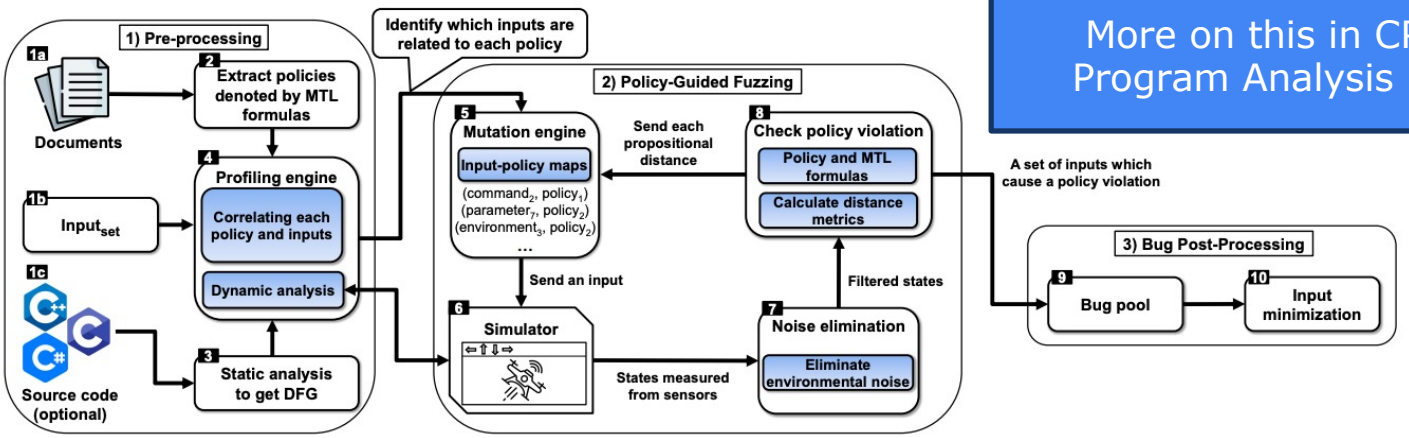
Item	Target Drone A	Target Drone B
Resonant Freq. (Gyroscope)	8,200 Hz (L3G4200D)	26,200 Hz (MPU6000)
SPL at Resonant Freq.	97 dB	95 dB
Affected Axes	X, Y, Z	Z
Attack Result	Fall down	Not affected

https://www.usenix.org/node/190941

- Drones use MEMS gyroscopes for sensing orientation
- Resonant frequencies of gyros used in drones are in audible range
- Experiments with speakers attached to drones
  - Loud enough, directional speakers could disable a drone

Fuzzing How a Vehicle Interacts with an Environment

- One approach:
  - Based on safety specifications, use simulators to test out different interactions
  - See if any simulated environmental conditions cause a violation of safety



More on this in CPS/IoT Program Analysis Module

https://www.ndss-symposium.org/wp-content/uploads/ndss2021_6A-1_24096_paper.pdf

How to do CPS research in this space: Target Devices

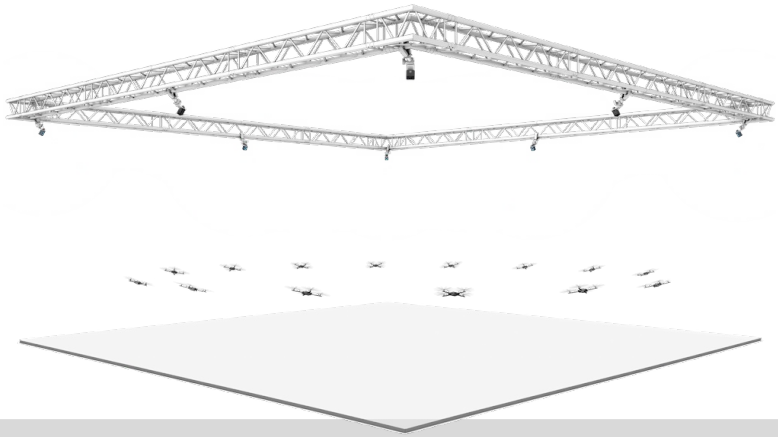
- Use simulators when possible, add fidelity when necessary
  - Be mindful of resource requirements!
- Validate on real hardware
  - We can purchase devices if justified
  - Sometimes smaller/cheaper devices are sufficient for a proof-of-concept

Crazyflie AI bundle

Amazon Deepracer

How to do CPS research in this space?

- Be resourceful!
  - Lots of robotics, autonomous vehicles, and AI folks on campus
  - Lots of computational and expensive infrastructure exists on campus
  - Example: validating attacks on localization: use an existing Optitrack camera setup on campus to give yourself ground truth data!



How to do CPS research in this space?

- Large (but incomplete!) list of simulators:
  - Drone models for Gazebo simulator: https://github.com/ethz-asl/rotors_simulator
  - Gazebo Tutorial: http://gazebosim.org/tutorials
    - Maybe skim the beginner tutorials
  - AirSim: simulator for drones and cars
    - https://microsoft.github.io/AirSim/
    - Sensors: https://microsoft.github.io/AirSim/
  - Baidu Apollo simulator: simulator for Baidu's open-source Apollo autonomous vehicle:
    - https://github.com/ApolloAuto/apollo/blob/master/docs/specs/Dreamland_introduction.md
    - https://apollo.auto/gamesim.html
  - CARLA simulator: open-source simulator for autonomous driving research
    - Main page: https://carla.org/
    - Sensor API reference: https://carla.readthedocs.io/en/latest/ref_sensors/
  - SVL simulator for autonomous vehicles: https://www.svlsimulator.com/
  - Smart home simulator:
    - https://realgames.co/home-io/
  - Other IoT device simulators:
    - https://www.microsoft.com/en-us/p/iot-simulator/9nwh3926zt2r?SilentAuth=1&activetab=pivot:overviewtab
    - https://aws.amazon.com/solutions/implementations/iot-device-simulator/
- Programming language for simulators: https://scenic-lang.readthedocs.io/en/latest/simulators.html
  - We'll discuss this more in Module 3

How to do CPS research in this space?

- **Legal issues**
  - Signal injection (e.g., GPS spoofing) can be illegal and lead to severe penalties
    - You may accidentally tamper with safety-critical operations!
  - Domain-specific regulations, e.g., flying drones within 5 miles of an airport
  - Research permissions: may require IRB approval **(when in doubt, ask me!)**
- **Safety Concerns**
  - Any attacks on real devices can lead to safety issues, and may violate campus policies
  - Some projects may require official safety training
- **Ethical Considerations**
  - **Responsible disclosure:** we can work together on a responsible disclosure process if vulnerabilities are discovered
  - **Potential misuse:** understand how your research findings can lead to misuse and cause harm to society
- **Reproducibility**
  - Ensure the experiments can be reproducible without compromising safety or legality
  - Be transparent about the conditions and limitations of the research

Wrapping up: Common Themes for ICS and Medical IoT

- Retrofit security
  - CPS systems are often hard to ”patch” simply, especially if system cannot be taken offline
  - We often need to have workaround solutions
  - Security is often an afterthought in these systems
  - Vulnerabilities amplified when everything is “internetified”
- Weak communication protocols are often the guilty party
- Relatively easy exploits can have dire consequences

Next Class

- Wrapping up Real World Attacks: Autonomous Vehicles
- Start “Security in a Nutshell” Module

- **Reminder:**
  - Sign up for presentations!!!
  - Discuss teams on Piazza

Please reach out to me if you’re struggling with ideas!


Questions?