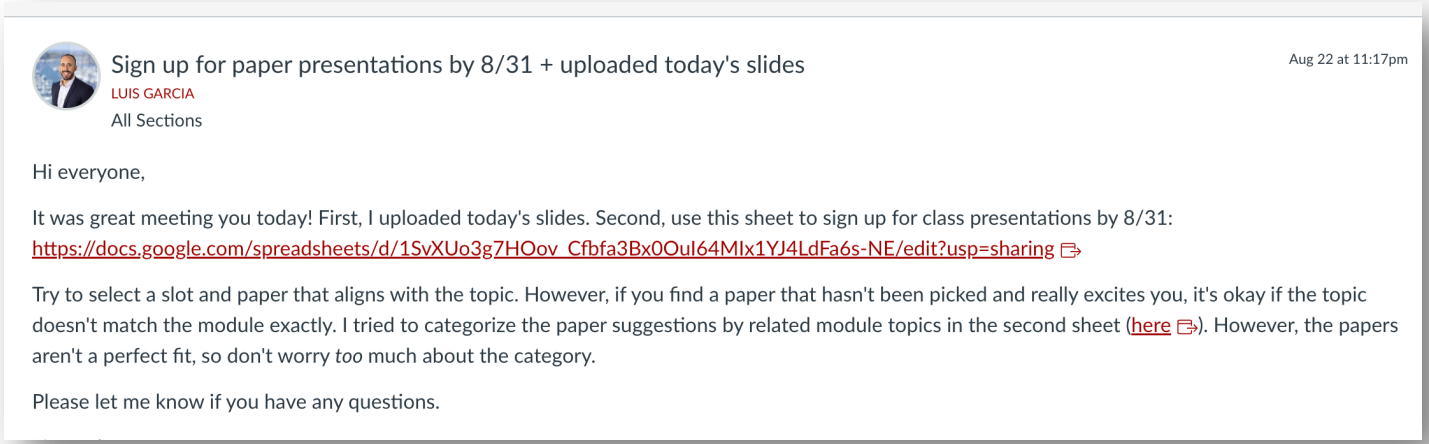
CS 6963/5963
University of Utah

Cyber-physical Systems and IoT Security

Module 1a: CPS/IoT Security Challenges

Announcements

- I requested a new room!
- Sign up for presentations by 8/31 (next week!)
  - Link is on Canvas + Piazza announcements



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.

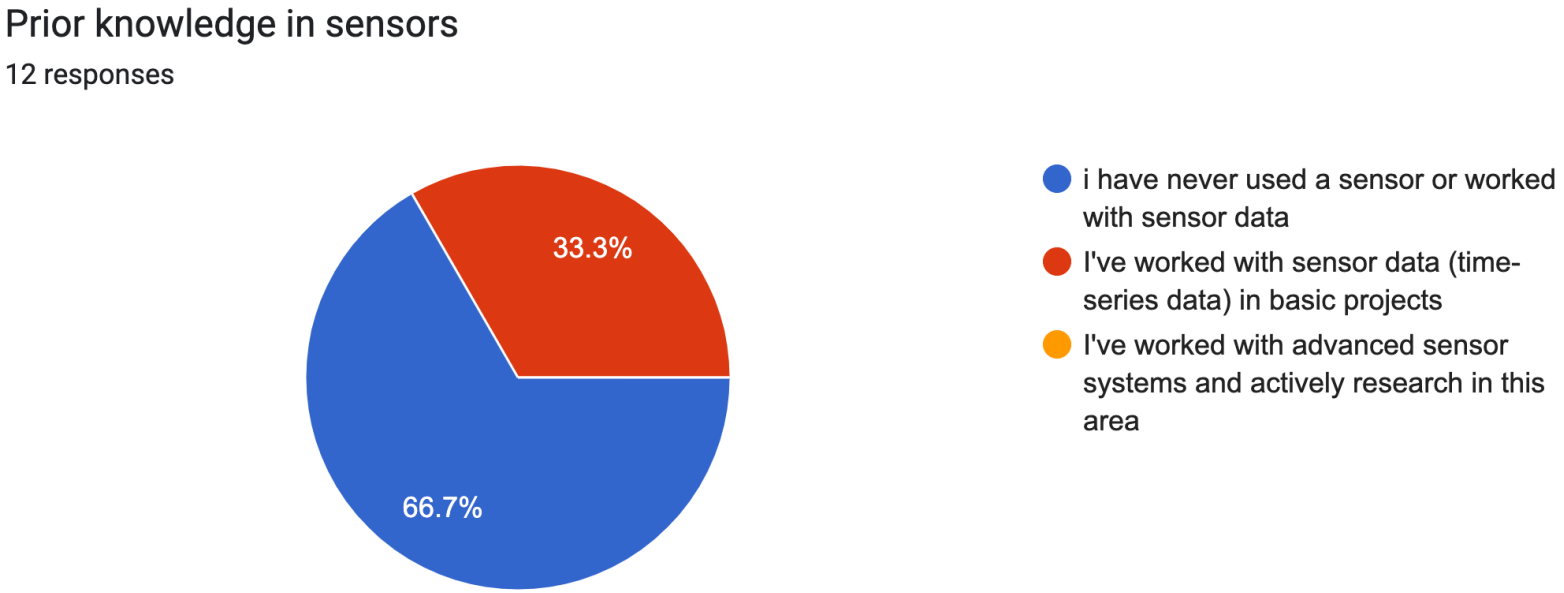

Questions?
1967 2017
AND BEYOND

Some Survey Results (in case imposter syndrome is lurking)

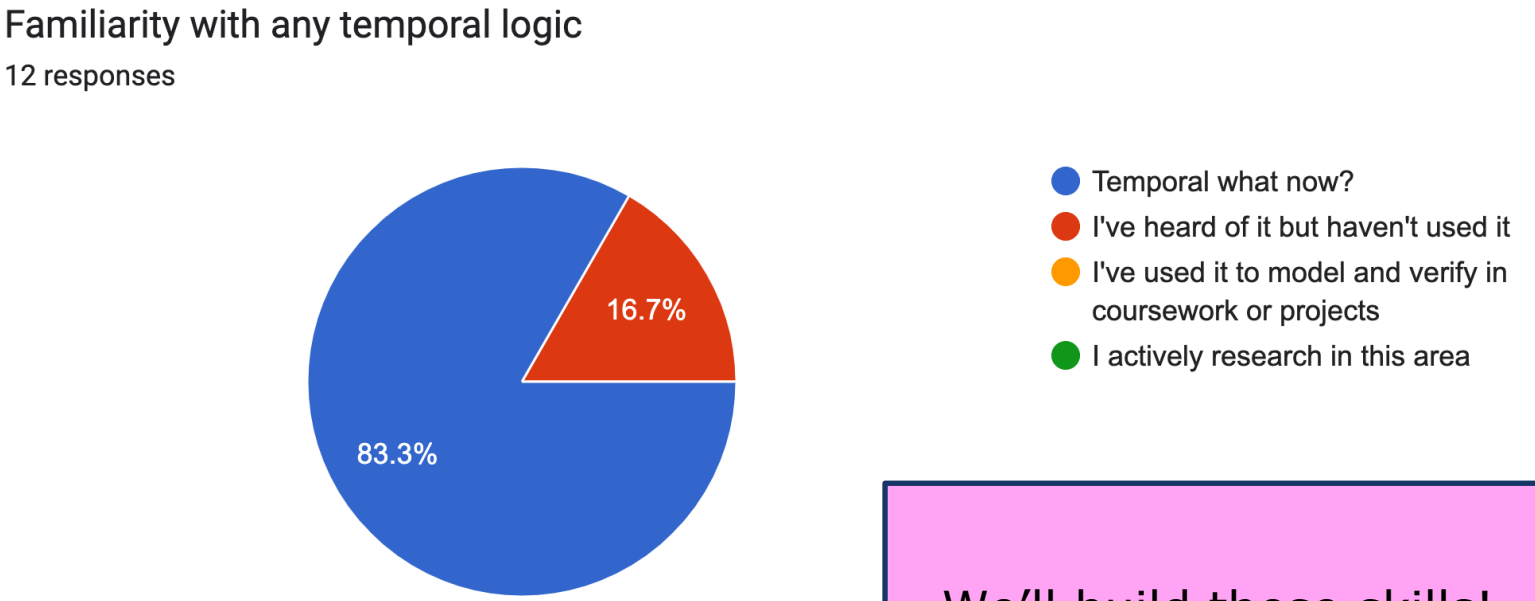
Deep Learning knowledge

12 responses

Some Survey Results (in case imposter syndrome is lurking)



Some Survey Results (in case imposter syndrome is lurking)



We'll build these skills!

Last Class: CPS/IoT are all around us!

From safety-critical infrastructure…

Is this a “CPS”?

…to making our lives more efficient…

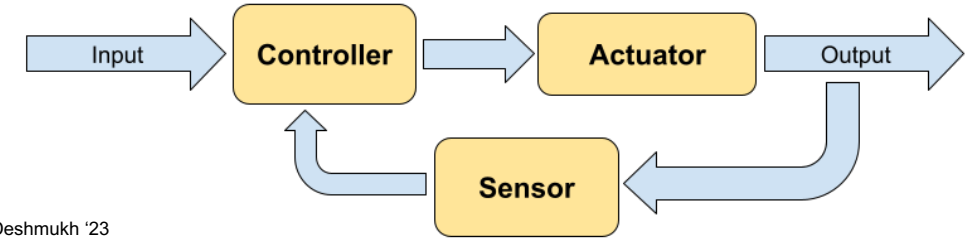
Is this “IoT”?

What is a Cyber-physical System?

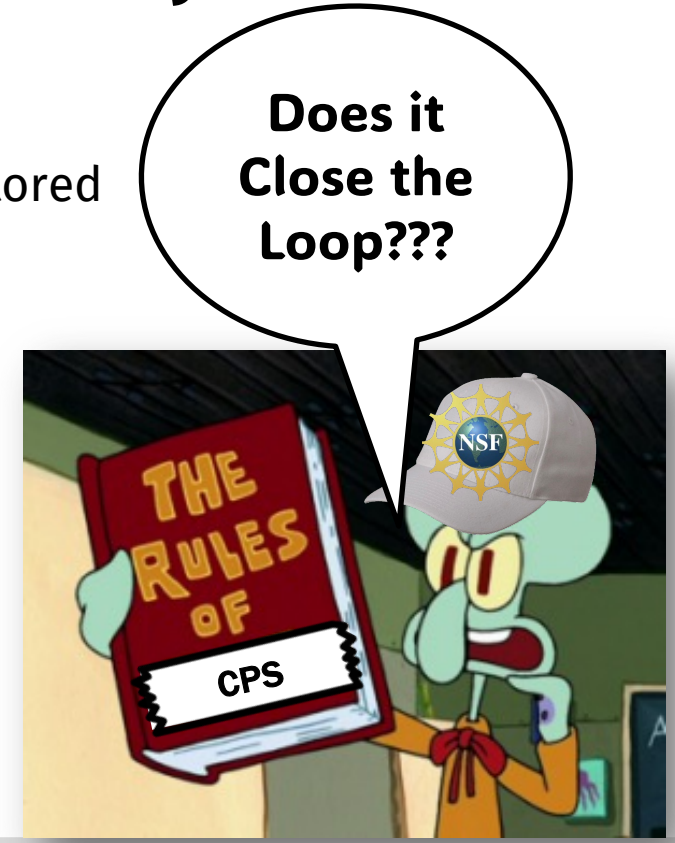
Depends on who you ask!

- **Wikipedia:** "a ***mechanism*** controlled or monitored by ***software algorithms.***

- **NSF: "**engineered systems built from, and depending upon, the ***seamless integration*** of algorithms and physical components"



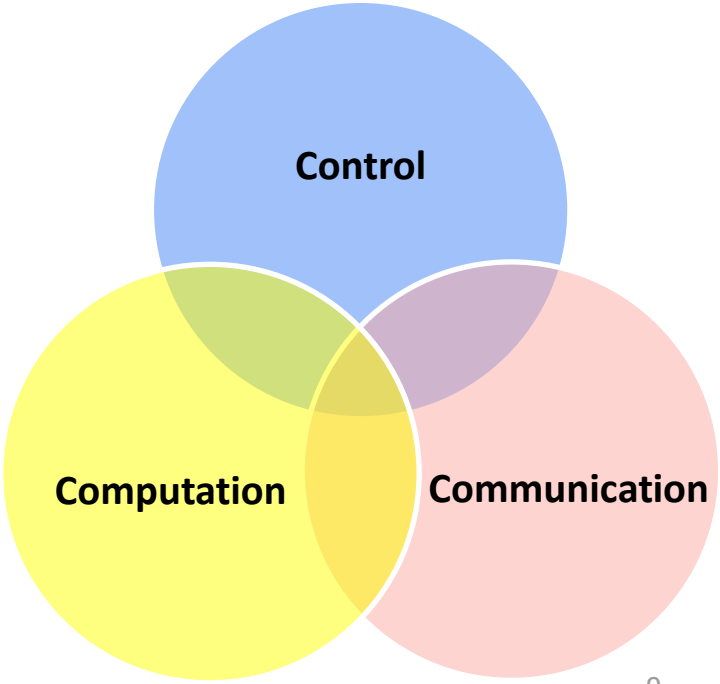
J. Deshmukh '23



What is a Cyber-physical System?

Depends on who you ask!

- **Wikipedia:** “a ***mechanism*** controlled or monitored by ***software algorithms.***
- **NSF: “**engineered systems built from, and depending upon, the ***seamless integration*** of algorithms and physical components”
- **Common saying:**
  CPS = “Control + Computation + Communication”



J. Deshmukh ‘23

What is the Internet-of-Things?

https://info.hummingbirdnetworks.com/blog/what-is-iot-and-how-it-works

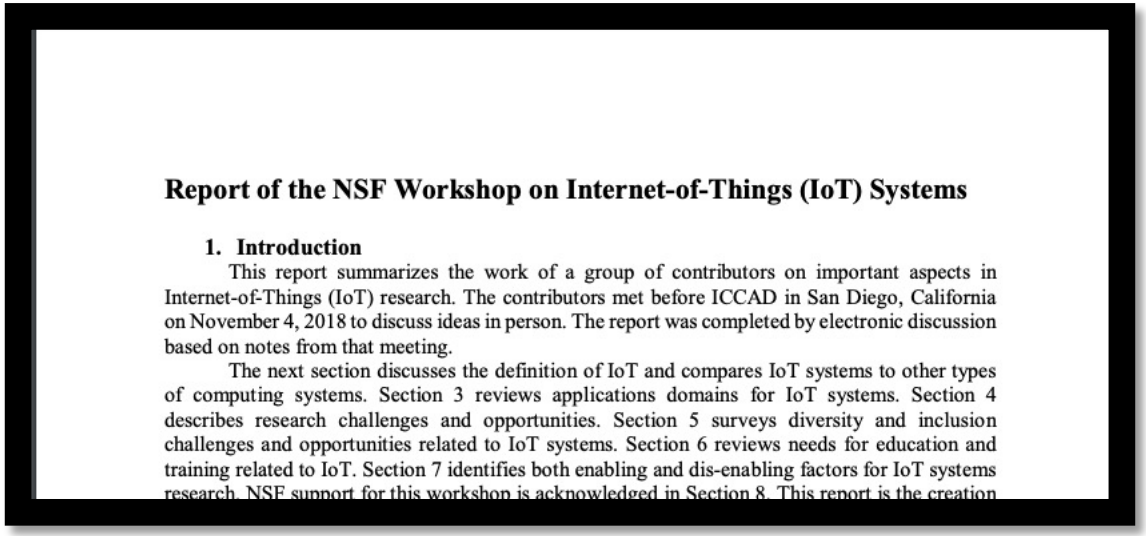
What is the ~~Internet-of-Things~~?

What is a "Thing"?

https://info.hummingbirdnetworks.com/blog/what-is-iot-and-how-it-works

What is the Internet-of-Things?

NSF Report on IoT (2019)



Report of the NSF Workshop on Internet-of-Things (IoT) Systems

1. Introduction

This report summarizes the work of a group of contributors on important aspects in Internet-of-Things (IoT) research. The contributors met before ICCAD in San Diego, California on November 4, 2018 to discuss ideas in person. The report was completed by electronic discussion based on notes from that meeting.

The next section discusses the definition of IoT and compares IoT systems to other types of computing systems. Section 3 reviews applications domains for IoT systems. Section 4 describes research challenges and opportunities. Section 5 surveys diversity and inclusion challenges and opportunities related to IoT systems. Section 6 reviews needs for education and training related to IoT. Section 7 identifies both enabling and dis-enabling factors for IoT systems research. NSF support for this workshop is acknowledged in Section 8. This report is the creation

https://mwolf.unl.edu/iot-workshop-report.pdf

NSF Report: What is an IoT System?

Two essential characteristics:

Senses physical Quantities

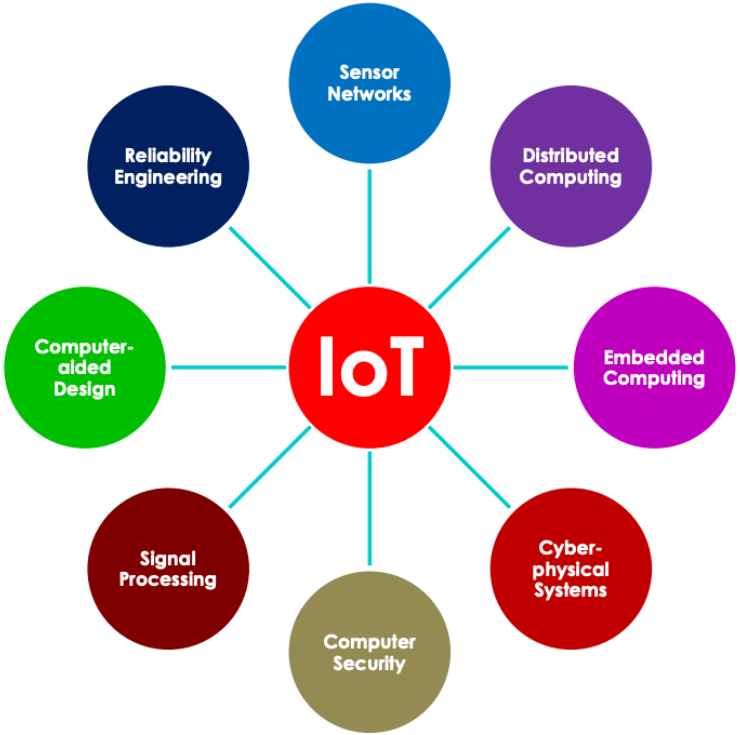
Continuous and discrete signals

Operates on Sensor data as a distributed computing system

Composed of several different types of nodes connected by wireless and/or wired networks

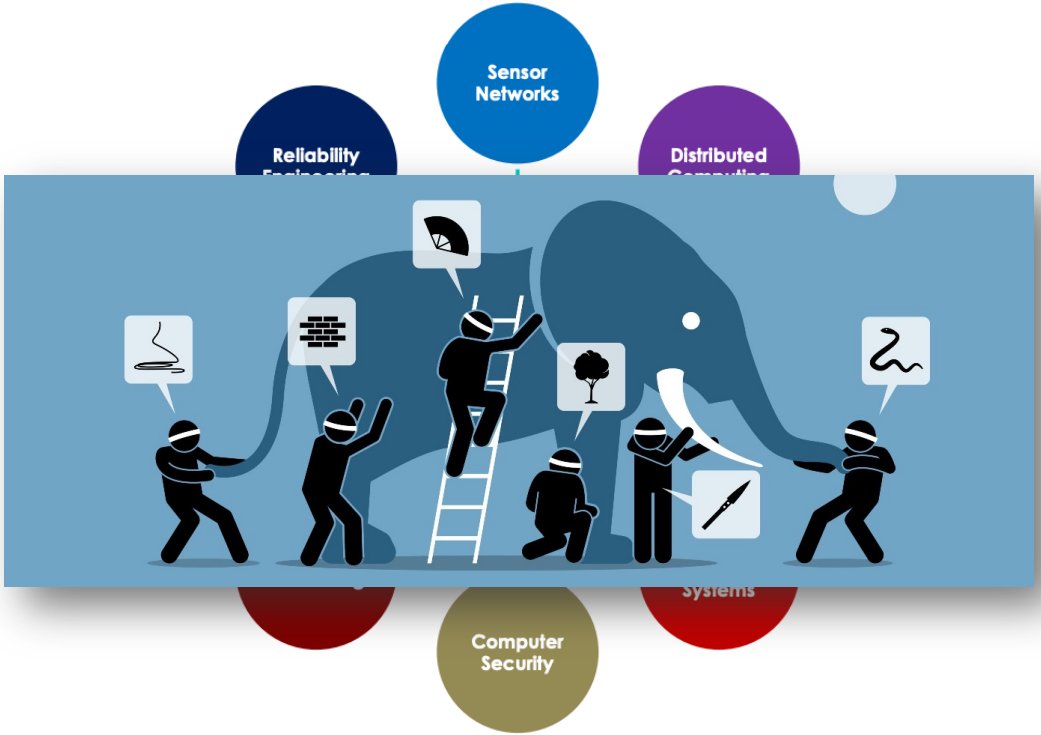
https://news.mit.edu/2020/iot-deep-learning-1113

NSF Report: What is an IoT System?



IoT Systems research draws from several communities…

NSF Report: What is an IoT System?



IoT Systems research draws from several communities…

Why Distinguish? Let's Unify!

IoT and CPS are comprised of the following components, all engineered for function through integrated logic and physics:

- Logical components (computation)
- Physical components
- Transducers (sensors/actuators)
- Humans

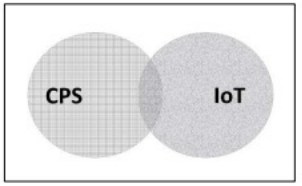


FIGURE 7A. PARTIAL OVERLAP

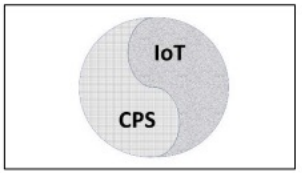


FIGURE 7B. EQUIVALENCE

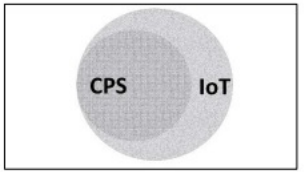


FIGURE 7C: CPS AS A SUBSET

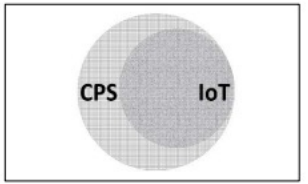


FIGURE 7D: IOT AS A SUBSET

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1900-202.pdf

What about Autonomous CPS?

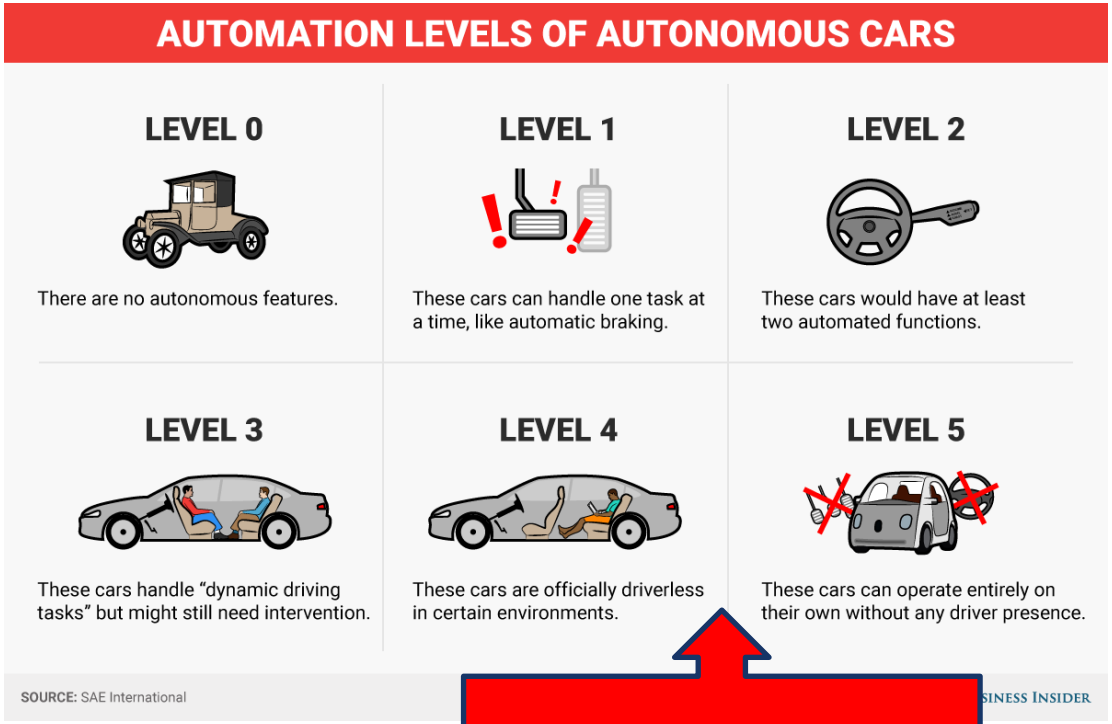
Autonomous CPS

- Autonomous: without the need for human intervention
- Autonomous CPS == CPS with no human operator
- Semi-autonomous: humans in- and on-the-loop (for control)
- All types are in scope in this course

Domain-specific Definition: Self-driving cars

J. Deshmukh ‘23

Domain-specific Taxonomies of Autonomous CPS: Self-Driving Cars

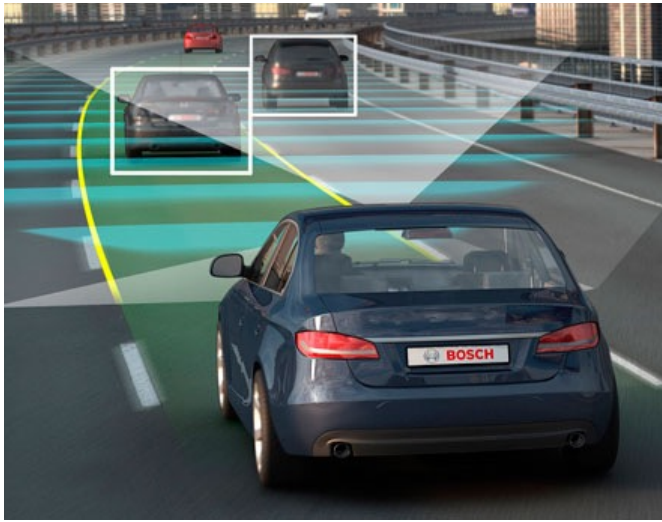


We're sort of here

Autonomous/Semi-Autonomous CPS Examples

Medical IoT

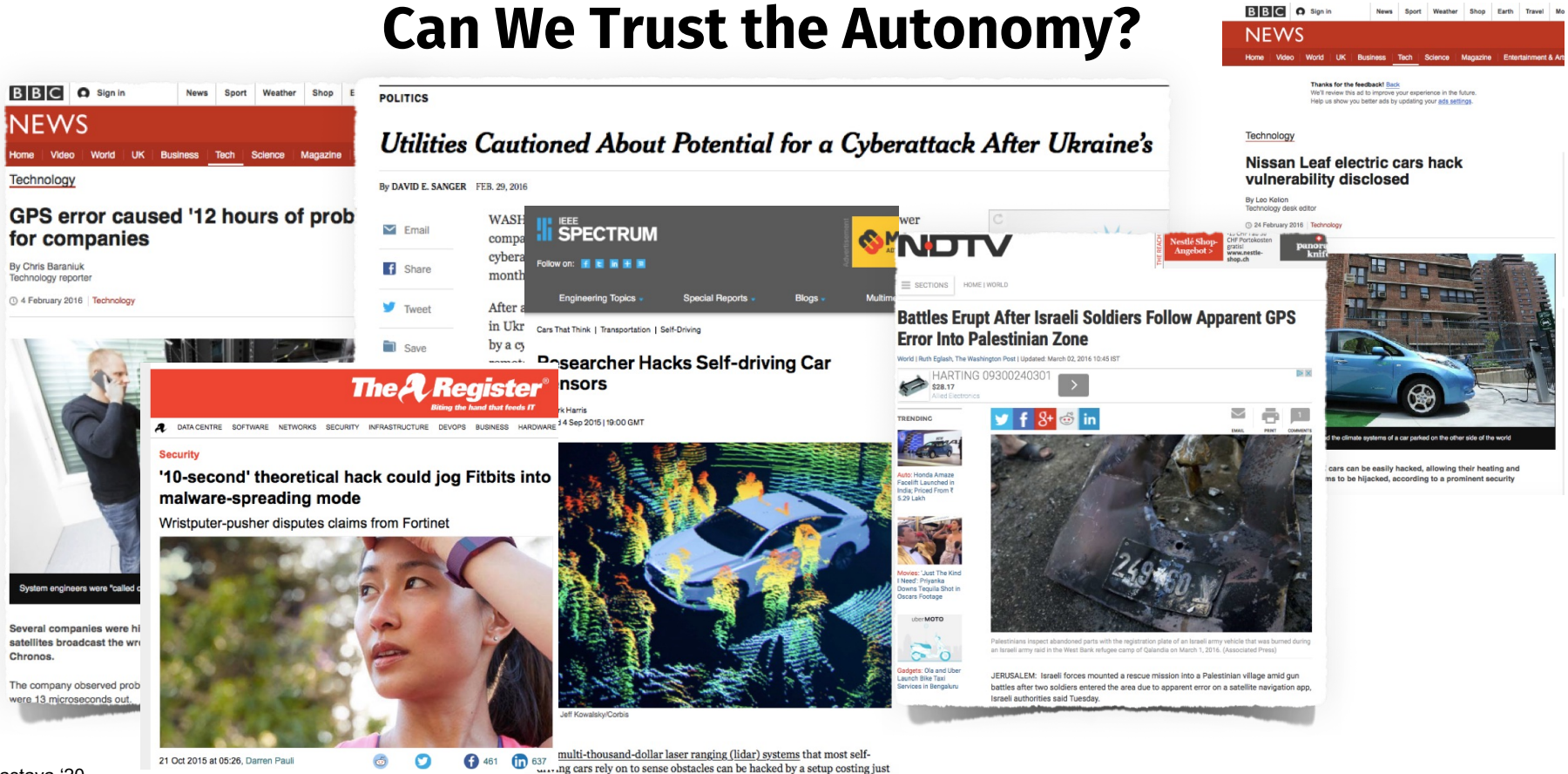
Smart Building/Cities



Transportation Systems

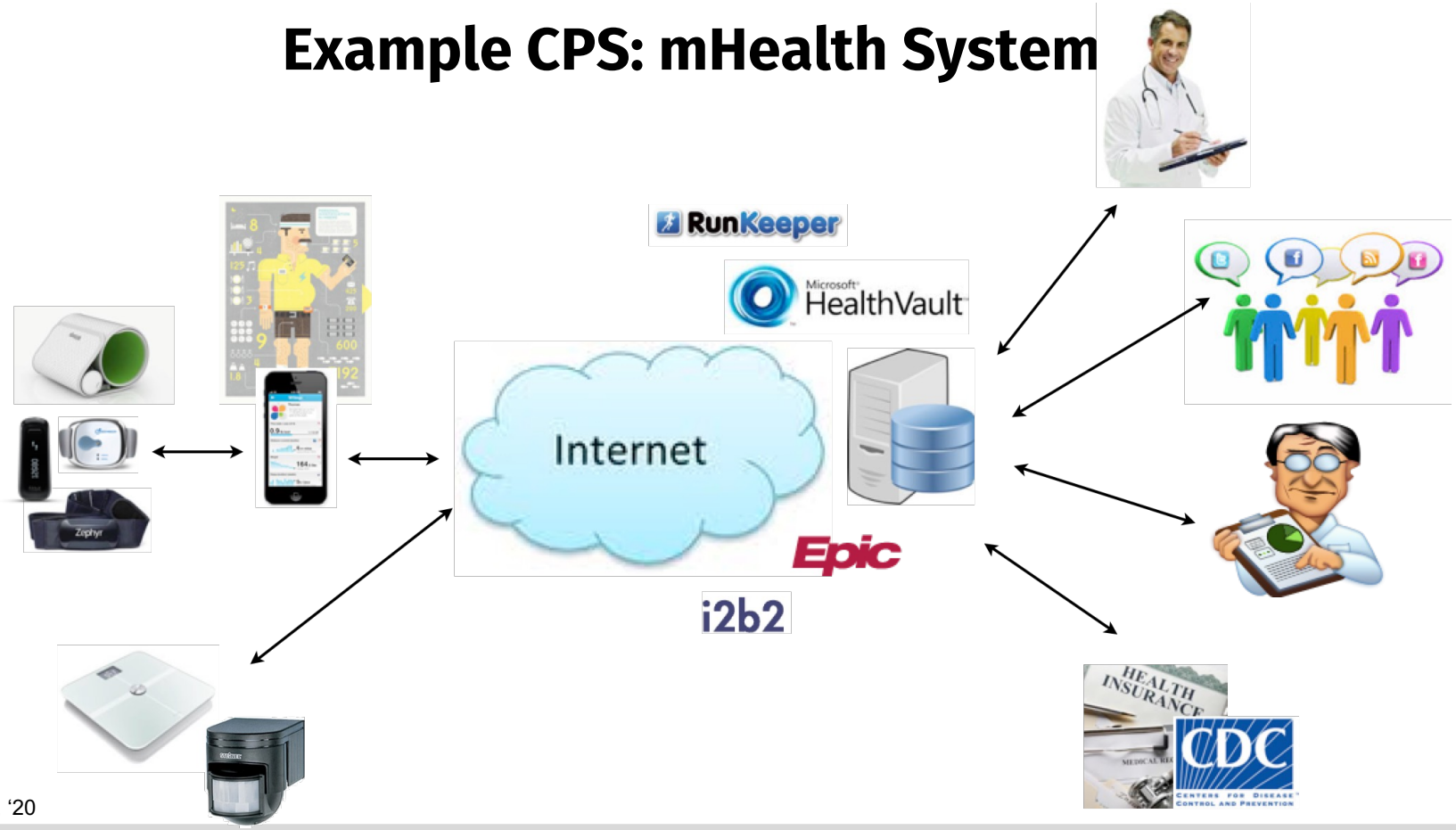
J. Deshmukh '23

Can We Trust the Autonomy?



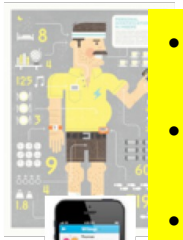
M. Srivastava '20

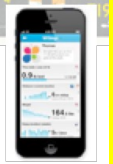
Example CPS: mHealth System



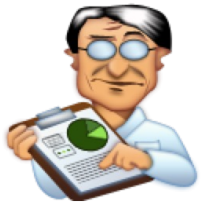
M. Srivastava, '20

Example CPS: mHealth System



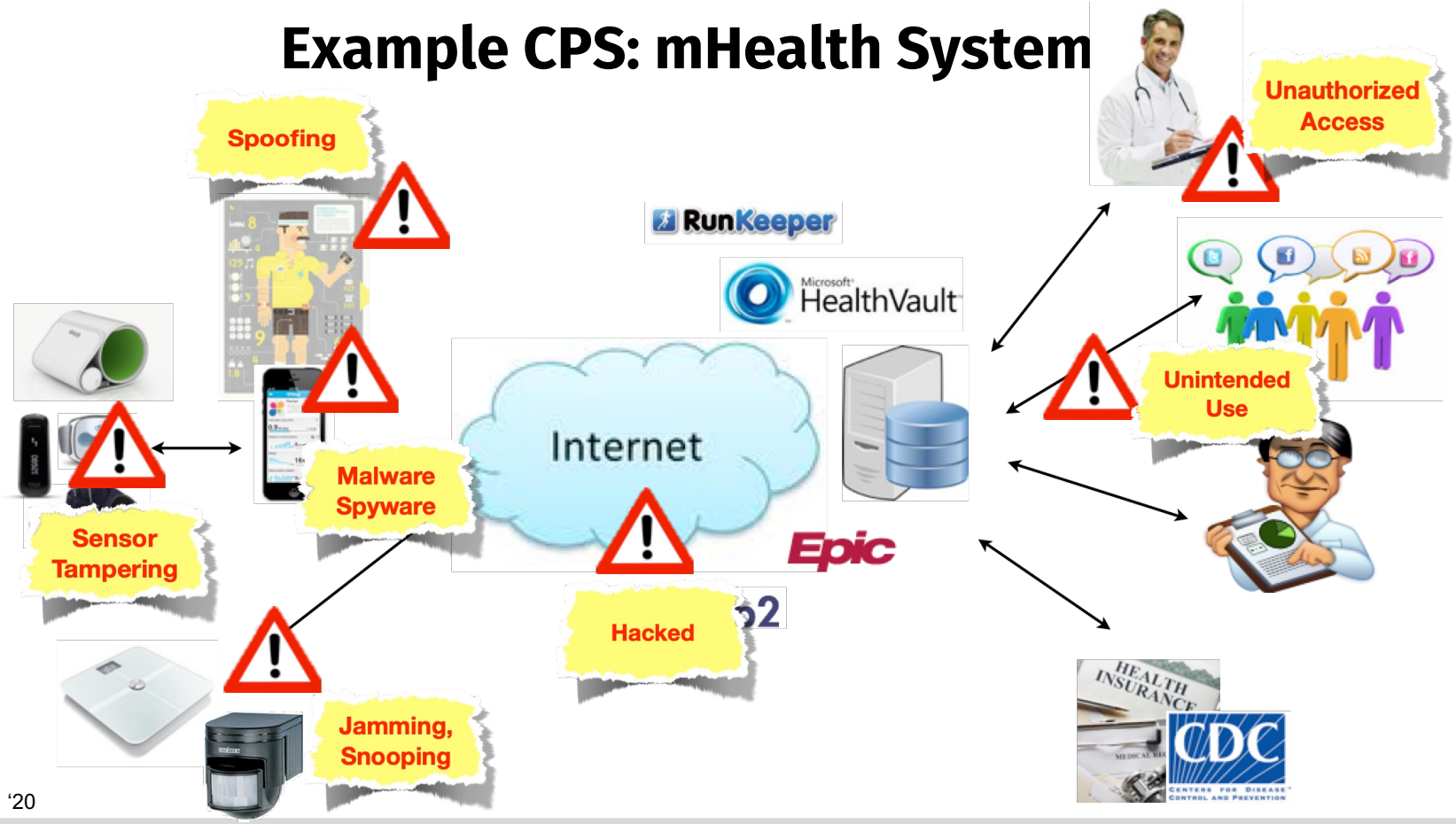


- General-purpose self-managed internet-connected mobile and wearable devices
- Rich, high-dimensional, continuously-captured sensory data
- Sensors accessible by multiple apps
- Use of 3rd party software libraries
- Data aggregated and processed by 3rd party cloud platforms and services
- Easy access to rich side information and advanced machine learning tools
- Complexity and rapid changes



M. Srivastava, ‘20

Example CPS: mHealth System



M. Srivastava, '20

Example: Smart & Automated Buildings

COMPUTERWORLD

Botnets coming soon to a smart home or automated building near you

Computerworld | Jun 4, 2014 5:16 PM PT

With the Internet of Things, smart buildings pose big risk

As buildings get more automated, they r risks

Who wants smart meter data?	How could the data be used?
Utilities	To monitor electricity usage and load; to determine bills
Electricity usage advisory companies	To promote energy conservation and awareness
Insurance companies	To determine health care premiums based on unusual behaviors that might indicate illness
Marketers	To profile customers for targeted advertisements
Law enforcers	To identify suspicious or illegal activity*
Civil litigators	To identify property boundaries and activities on premises
Landlords	To verify lease compliance
Private investigators	To monitor specific events
The press	To get information about famous people
Creditors	To determine behavior that might indicate creditworthiness
Criminals	To identify the best times for a burglary or to identify high-priced appliances to steal

Exacerbating the situation is the fact that many of the communications protocols for building automation and control networks, such as BACnet and LonTalk, are open and transparent, said Jim Sinopoli, managing principal at Smart Buildings LLC.

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY

Safari Power Saver Click to Start Flash Plug-in

THREAT LEVEL cybersecurity Hacks and Cracks

Researchers Hack Building Control System

COMPUTERWORLD

Target attack shows danger of remotely accessible HVAC systems

Qualys says about 55,000 Internet-connected heating systems, including one at the Sochi Olympic arena, lack adequate security

MORE LIKE THIS

Target breach happened because of a basic network segmentation error

Investigations

Tridium's Niagara Framework: Marvel of connectivity illustrates new cyber risks

M. Srivastava, '20

Example: Smart & Automated Buildings

Attack Scenarios

(from "Alice's Adventures in Smart Building Land" by Wendzel et. al., 2014)

- An attacker could **disable fire alarms and then set the building on fire**, or set off the fire alarm at the airport as an evacuation would cause chaos.
- Coordinated attacks on smart appliances as well as turning up the heat or air conditioning levels at night could **increase energy consumption sales over an entire region**.
- **Excessive heating** affects people's efficiency and capability to work, so an attack on a Stock Exchange building could include increasing the temperature to **slow down a trader's reaction time**.
- A BAS botnet could simultaneously **crank up the heat** to a high number of server rooms, which would **cause denial of service due to server failures**.
- BAS integration can be part of ambient assisted living (AAL) for the elderly, so "an assailant could try to **blackmail inhabitants** of a high number of buildings by attacking these buildings. Elders, handicapped and weak people could be **locked inside buildings** (by closing windows and doors automatically) if they do not transfer an amount of money to a given bank account."
- **Entire smart cities or even economies could theoretically become part of a smart building botnet**

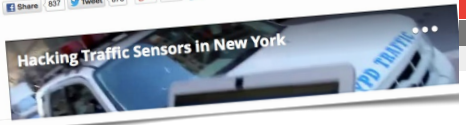
Example: Transportation Systems

WIRED GEAR SCIENCE ENTERTAINMENT BUSINESS SECURITY DESIGN OPINION MAGAZINE VIDEO

THREAT LEVEL

Hackers Can Mess With Traffic Lights to Jam Roads and Reroute Cars

BY KIM ZETTER 04.30.14 | 6:30 AM | PERMALINK



FBI investigating hacked NCDOT digital road signs

Submitted by WWAY on Sat, 05/31/2014 - 8:55am.

The Register®

Data Center Software Networks Security Business Hardware Science Bootnotes Video

SECURITY

Polish teen derails tram after hacking train ...work

...city network into Hornby set

...Leyden, 11 Ja...

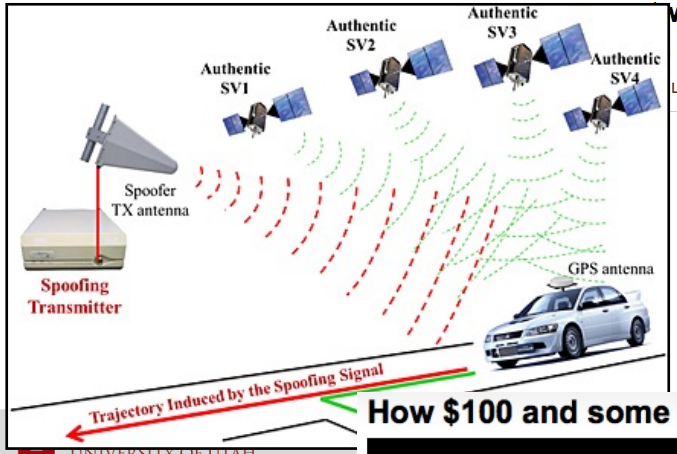
WIRED.CO.UK

NEWS Topics / TECHNOLOGY WAZE HACKING

6 issues for £9 + FREE iPad & iPhone editions SUBSCRI

Students hack Waze, send in army of traffic bots

TECHNOLOGY / 25 MARCH 14 / by NICHOLAS TUFNELL

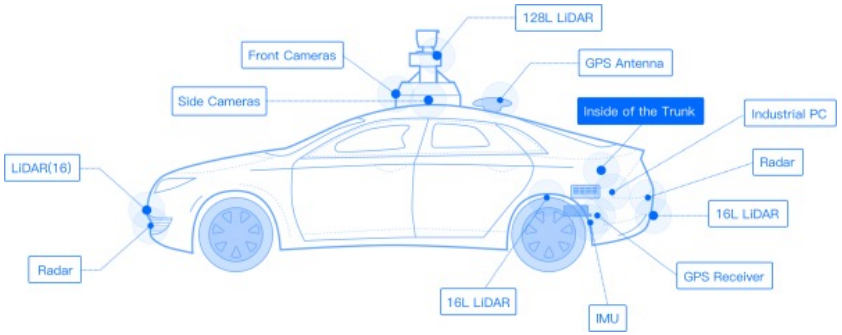


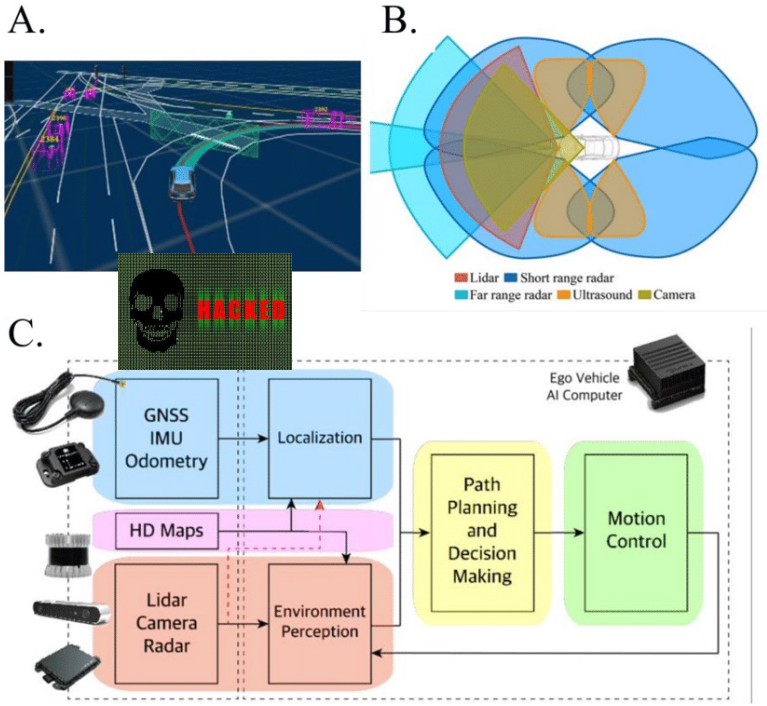
How $100 and some spare time is enough to hack traffic lights

Canada AM: Hacki...

Example: Transportation Systems

Typical Self-driving Car Vehicle Pipeline (perception-planning-control)





Sensor Spoofing

More on this in Module 6!

Information System Security: Traditional Goals

Goal	What does it mean?	How to achieve it?
Confidentiality	Keep your secrets secret	Physical isolation, cryptography, background checks on people
Integrity	Prevent others from modifying your code/data	TPM, Checksums & digital signatures, redundancy, backups
Availability	Make sure you can use your system	Hardening, redundancy, reference checks on people

CIA Triad

Information System Security: Traditional Goals

Goal	What does it mean?	How to achieve it?
Confidentiality	Keep your secrets secret	Physical isolation, cryptography, background checks on people
Integrity	Prevent others from modifying your code/data	TPM, Checksums & digital signatures, redundancy, backups
Availability	Make sure you can use your system	Hardening, redundancy, reference checks on people
Authentication	Person or entity is really who it claims to be	Cryptography with public key infrastructure
Control	Regulate the use of your system	Access control lists, physical security
Audit	What happened? How do we undo it?	Log files, provenance info, human auditors, expert systems
Nonrepudiation	Sender / Receiver can't deny sending / receiving	Cryptography with public key infrastructure

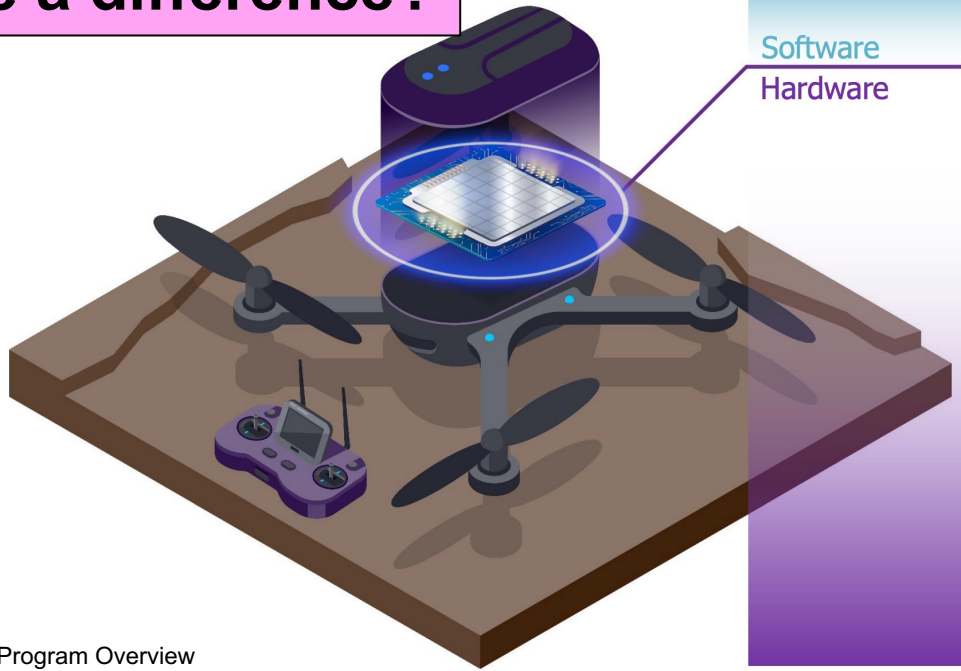
http

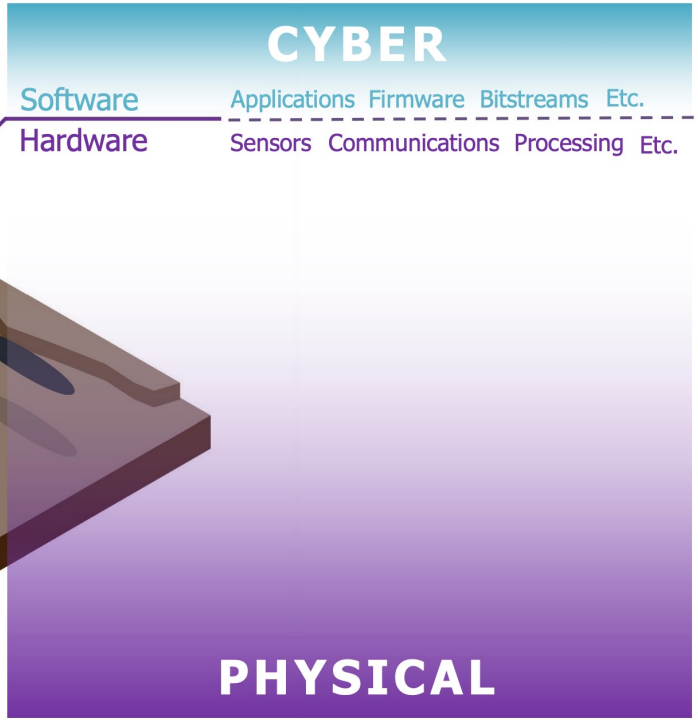
Basic Terminology

- **Vulnerability:** A flaw or weakness in a system's design, implementation, operation, or management that could be exploited to violate the system's confidentiality, integrity, or availability.
- **Threat:** Any circumstance or event with the potential to exploit a vulnerability and adversely affect a system through unauthorized access, destruction, disclosure, or modification of data, or denial of service.
- **Attack:** An intentional assault on system security that derives from an intelligent threat. An active attack is one that attempts to alter system resources or affect their operation, while a passive attack is one that attempts to learn or make use of information from a system but does not affect that system.
- **Adversary**: An entity that attacks a system or is a threat to a system. The terms "intruder," "attacker," "cyber attacker," "cracker," and "hacker" can also be used.
- **Countermeasure:** An action, device, procedure, or technique that meets or opposes (i.e., counters) a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Cyber Threats vs. Cyber-physical Threats

Is there a difference?





L. Yan, DAPRA FIRE Program Overview

Cyber Threats in CPS/IoT

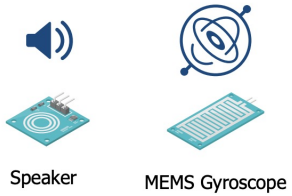
- Security or Privacy Failures that may ***intentionally lead to physical threats***
- For instance, a cyber threat in a smart home may lead to
  - *physical harm to things, environments, or occupants*
  - *Financial harm to owners of environments*
  - *Reputational or financial harm to owner or occupants through exposure of personal information*

Cyber-physical Threats

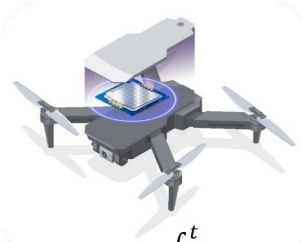
DARPA FIRE Program:

"Vulnerabilities that arise from the composition of hardware, software, and physical sub-systems where each component may not be vulnerable in-and-of itself."

0. Wait until quadcopter is in flight



1. Use speaker to inject false readings in Z-axis



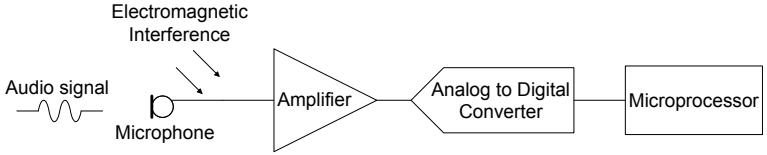
$$u(t) = K_p e(t) + K_i \int_0^t e(\tau)d\tau + K_d \frac{de(t)}{dt}$$

2. Errant readings lead to wild swings in error $e(t)$ causing wild swings in output $u(t)$

3. Crash

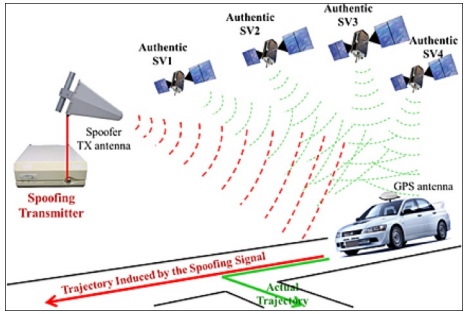
Cyber-physical Threats: Attacks from the Physical / Analog Domain Spoofing the Sensor Signals

EMI Injection Attack [Kune]

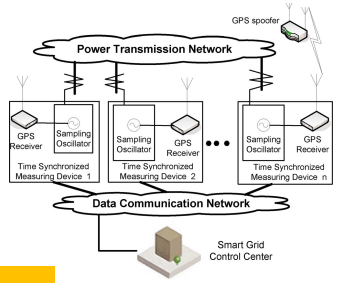


Attacking Light Rays (Mission Impossible)

Spoofing & Meaconing Attacks on GPS Signals (transportation, PMUs in smart grids)



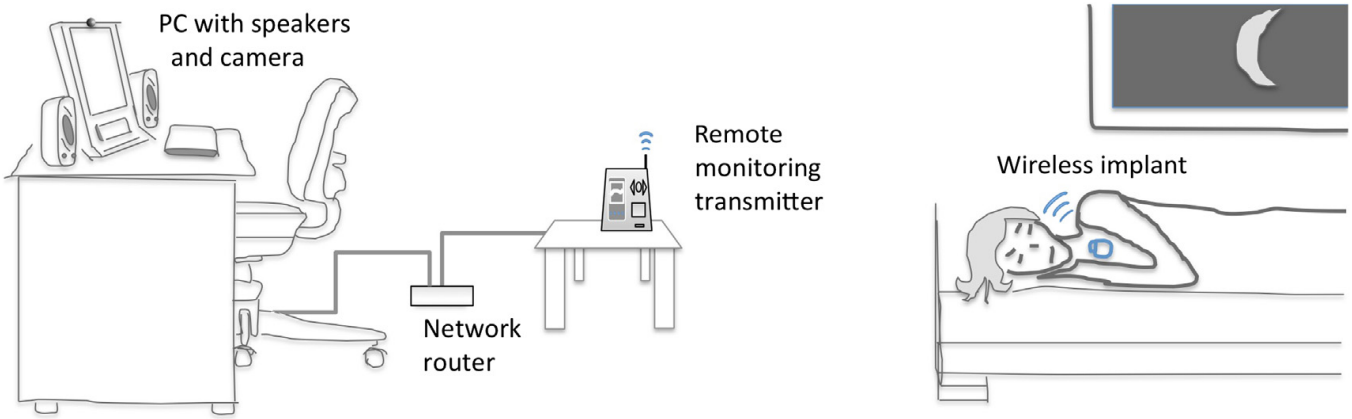
More on this in Module 6!



Traditional security mechanisms don't help

In this class: we care about both! Attacks that Bridge Cyber and Physical Spaces

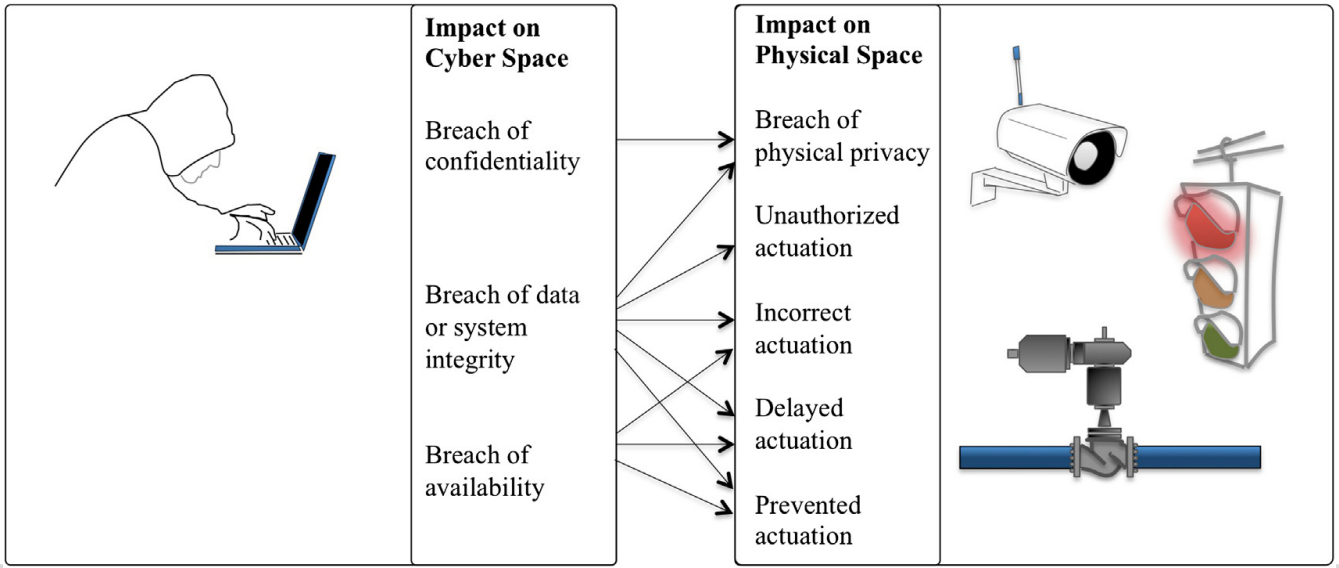
- Security breach in cyberspace adversely affecting physical space, and vice versa



The politician is sleeping at night, with her computer left on and a remote monitoring device collecting real-time data on the operation of her heart from the sensor of her implantable cardioverter defibrillator.

In this class: we care about both!
Attacks that Bridge Cyber and Physical Spaces

- Security breach in cyberspace adversely affecting physical space, and vice versa



CPS/IoT Vulnerabilities and Where to Find Them

- Research conferences
- BlackHat Briefings
  - https://www.blackhat.com/us-23/briefings/schedule/index.html#track/cyber-physical-systems--iot
  - Easier to navigate than DEFCON content (and probably safer)
- Vulnerability Databases
  - E.g., NIST National Vulnerabilitity Database, Common Vulnerabilities and Exposures (CVE), ICS-CERT Advisories,...
- Exploit Databases
  - E.g., exploit-db
- Shodan
  - Search engine for internet-connected devices: https://www.shodan.io/search?query=screenshot.label%3Aics
- Security Blogs
  - Security Weekly, The Hacker News, Krebs on Security, Dark Reading, ...

Wrapping Up

- Brief Overview of IoT vs. CPS
- Basic Terminology
- From Cyber to Cyber-physical Threats

Reminders

Start looking for teammates!
Don’t be shy on Piazza!

(and don’t forget to sign up for presentations by 8/31)

Next Week:
Real World Attacks and Defenses

Attacks on Industrial Control Systems

Attacks on Medical Implants

Attacks on Autonomous Vehicles

Goal: Inspire More Project Ideas


Questions?
1967-2017
AND BEYOND