Overview of Security in IoT

Gabe Parmer

Perspective on Liability

Who is to blame if it goes wrong?

- Computer Science
  - Users = Lusers
  - They use our service
    ...and should be
    thankful

Perspective on Liability

Who is to blame if it goes wrong?

- Computer Science
  - Users = Lusers
- Mechanical/civil:
  - You build it, you can be sued

Perspective on Liability

Who is to blame if it goes wrong?

- Computer Science
  - Autonomous Vehicles
  - Pervasive surveillance
  - City-level control

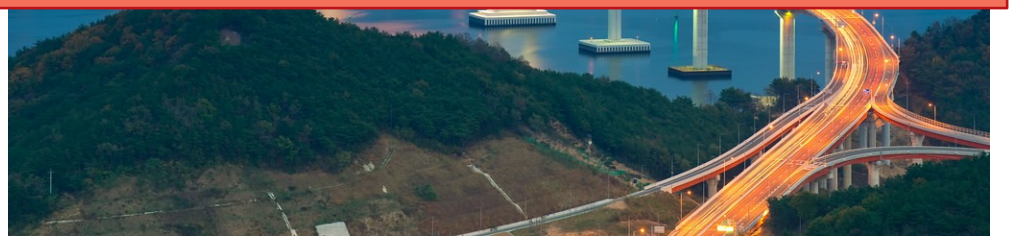
Now who's to blame?

Perspective on Liability

Who is to blame
goes wrong?

- Computer Sci
  - Autonomous
  - Pervasive surveillance
  - City-level control

Goal: Can we *understand* the risk of the system, to explicitly *analyze* it?



Now who's to blame?

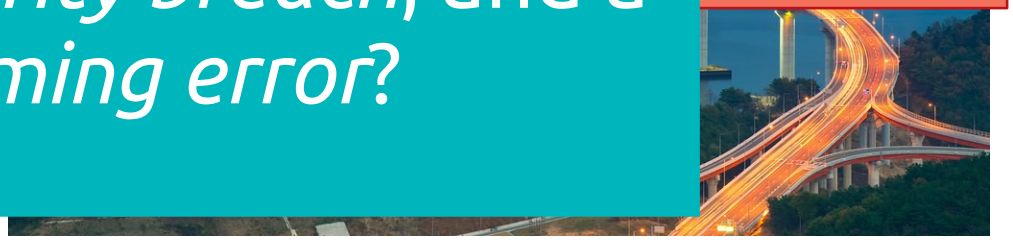
Perspective on Liability

Who is to blame
goes wrong?

- Comp
  - Aut
  - Per
  - City

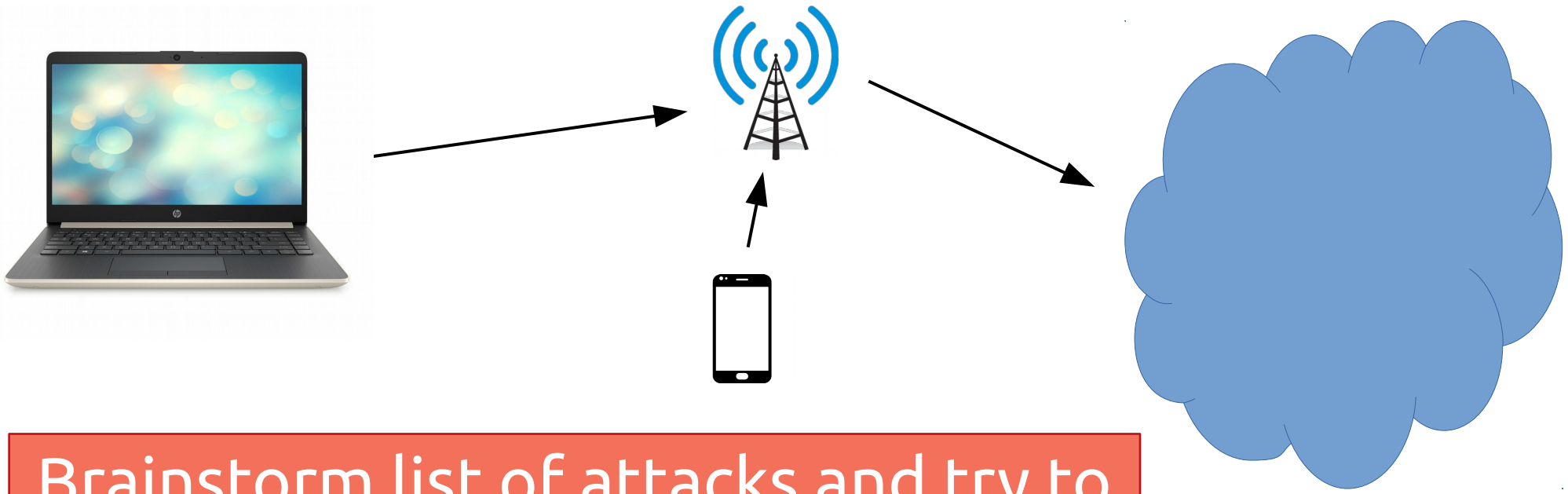
Goal: Can we *understand* the risk
citly

Really hard: Can we differentiate between a *security breach*, and a *programming error*?



Now who's to blame?

Vectors for Traditional Attacks?



Brainstorm list of attacks and try to make a taxonomy (abstract them)

Vectors for Traditional Attacks?

- *Man in the middle* – spoofing, eavesdropping, connection hijacking
- *Privilege escalation* –
  - Client: malware, ransomware
  - Server: infiltration, exfiltration
- *Service unavailability* – DoS, DDoS attacks
- …

Security: traditional view

- **C**onfidentiality
  - Only appropriate principles can access information
- **I**ntegrity
  - Data and computation cannot be interfered with
- **A**vailability
  - Requests can be processed within expected span

Security: traditional view

- **C**onfidentiality
  - Only appropriate principles can access information
  - *Mitigation*: Controlling the *flow of information*
- Tools
  - *Limit access to information* – encryption
    - Have key? Can access information
  - *Limit access to data* – Access Control, limit comm.
    - Limit and manage data-flow, and access (POLP)

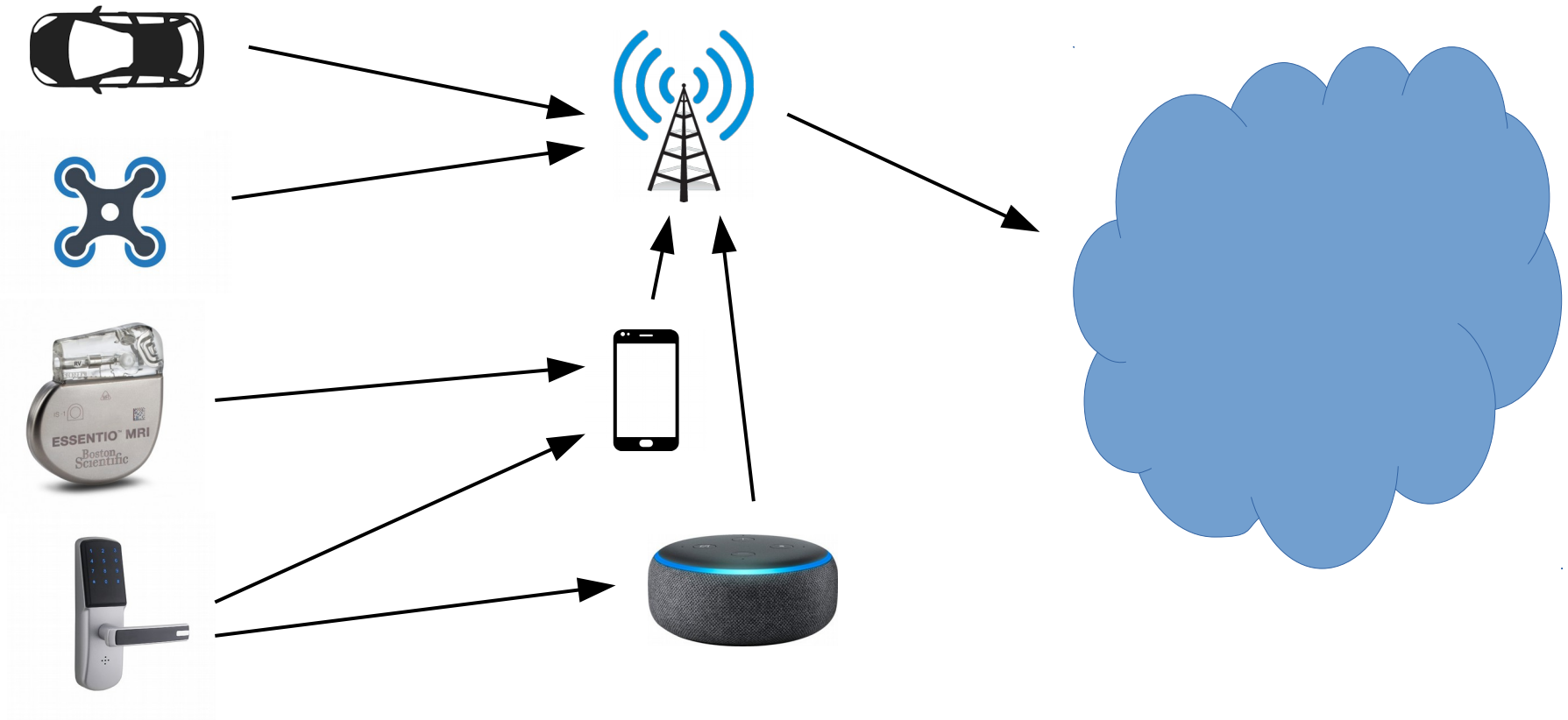
Security: traditional view

- **I**ntegrity
  - Data and computation cannot be interfered with
  - *Mitigation*: Isolation and “many walls”
- Tools
  - *Detect corruption* – HW for tagging, Hashchains
  - *Prevent corruption* – Constrain mods via isolation

Security: traditional view

- **A**vailability
  - Requests can be processed w/i an expected span
  - *Mitigation*: Distribution, scale, and rate-limiting
- Tools
  - *Constrain request rate* – rate-limiting
  - *Moar resources* – parallelism and scaling

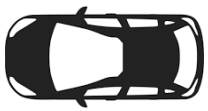
Vectors for IoT/CPS Attacks?



Vectors for IoT/CPS Attacks?

Brainstorm list of attacks and try to make a taxonomy (abstract them)

Vectors for Attack

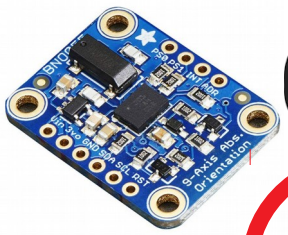


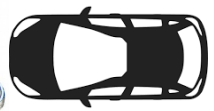
Limited resources

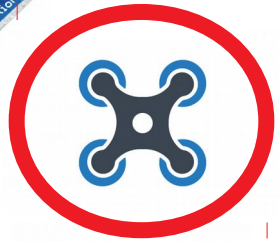
Typical solutions to security no longer work

- Protection domains
  - no isolation between system/tasks nor tasks/tasks
- Address-Space Layout Randomization (ASLR)
  - probabilistic defense against control-flow hijacking attacks (ROP attacks)
  - IoT scale + physical addresses
- Crypto-based communication
  - crypto vs. power, crypto vs. time

Vectors for Attack



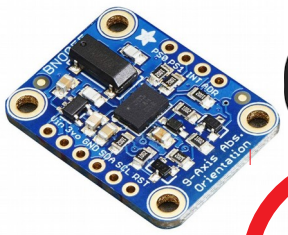


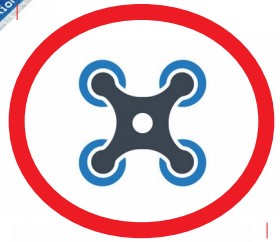


GPS

How is GPS implemented?

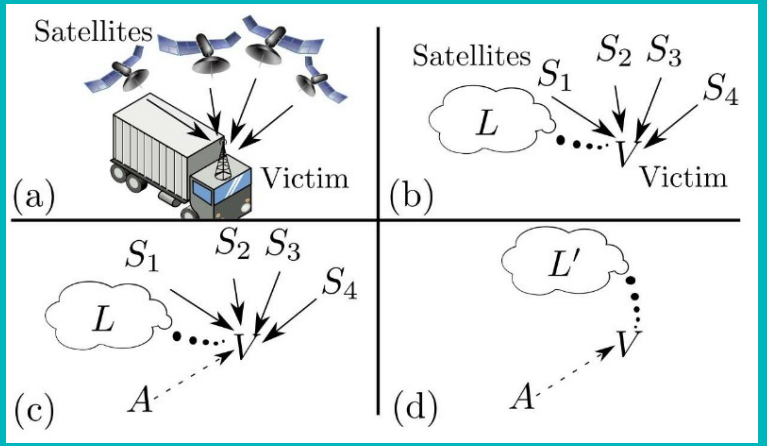
Vectors for Attack





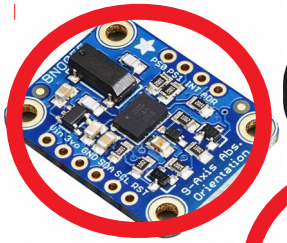
GPS

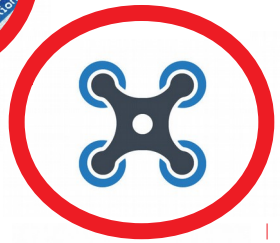
- Civilian GPS signals are *not* authenticated
- Can be jammed, or spoofed



”On the Requirements for Successful GPS Spoofing Attacks” by Tippenhauer et al.
”A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing“ by Warner et al.

Vectors for Attack



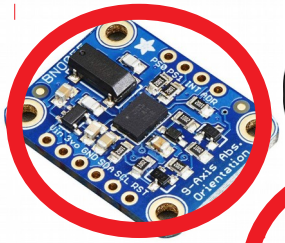


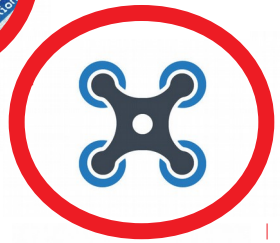
Inertial Measurement Unit

- *Accelerometer* – Measures change in velocity
- *Gyroscope* – Measures angular rotation
- *Magnetometer* – Orientation WRT earth's magnetic field

How are these implemented?

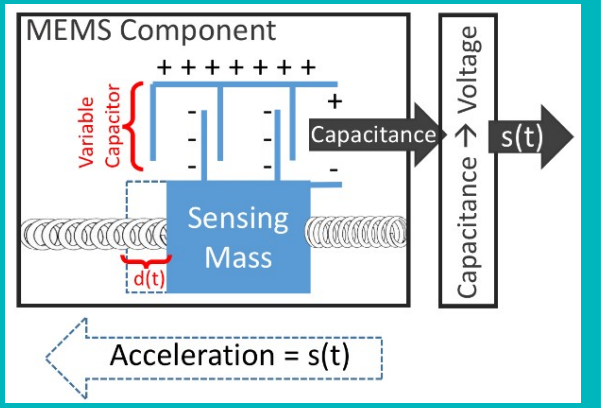
Vectors for Attack



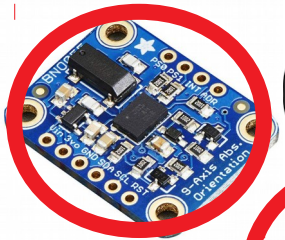


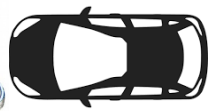
Inertial Measurement Unit

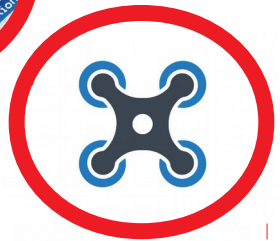
- ***Accelerometer & Gyroscope*** **– Micro-Electro-Mechanical System (MEMS)**
- *Magnetometer* – Hall effect → measure voltage disparity across a plate

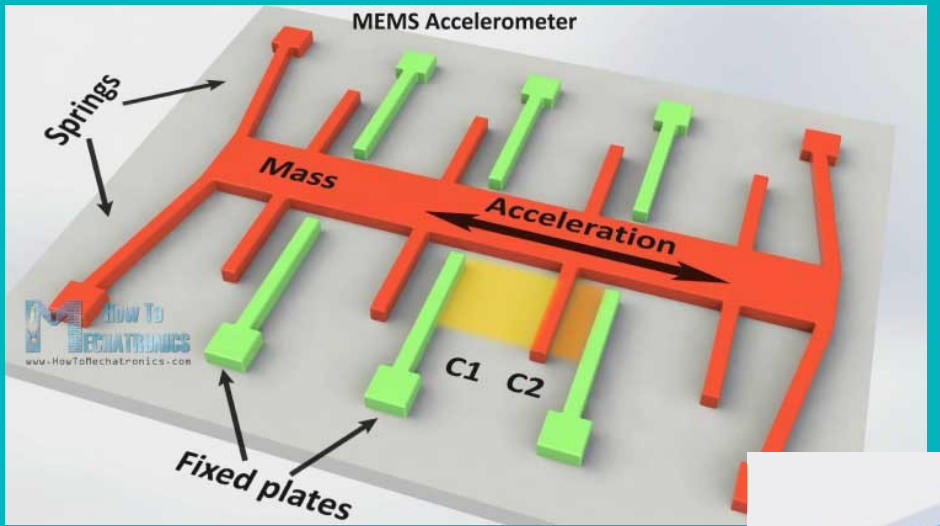


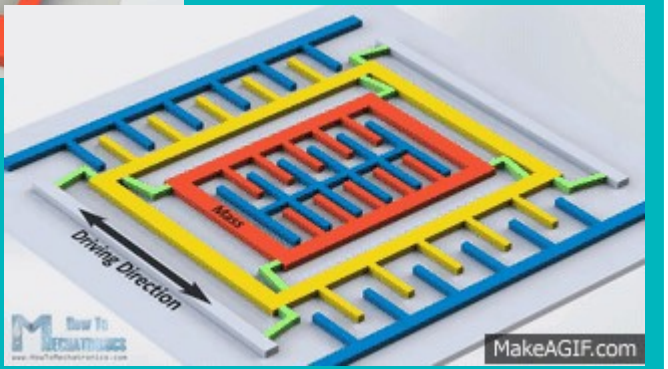
Vectors for Attack



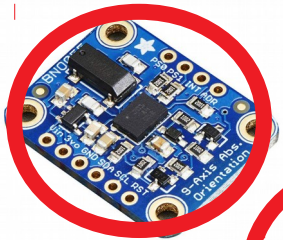


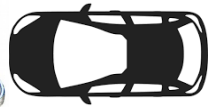


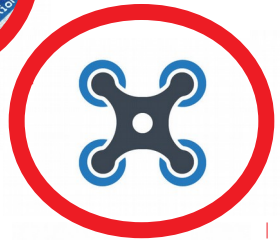


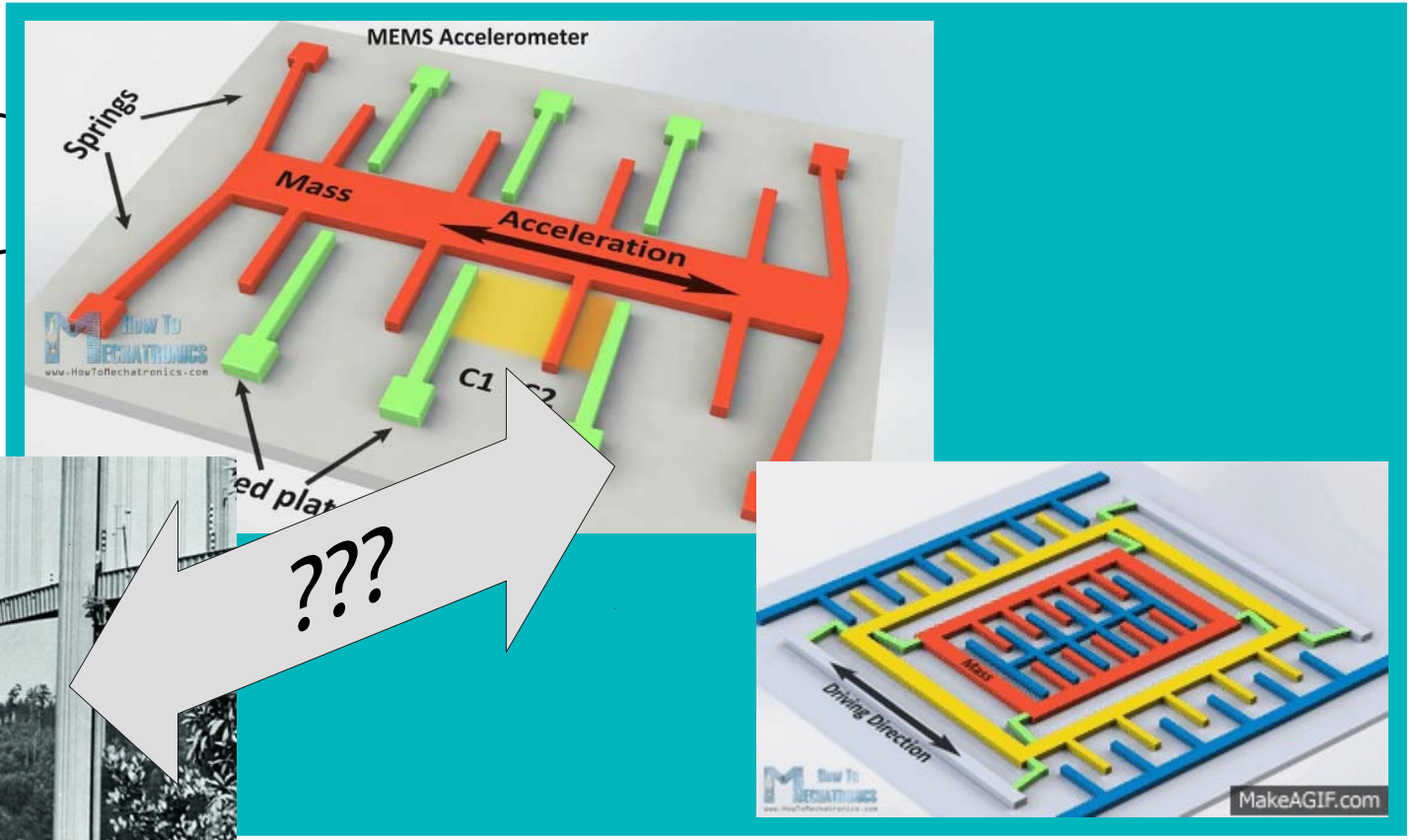


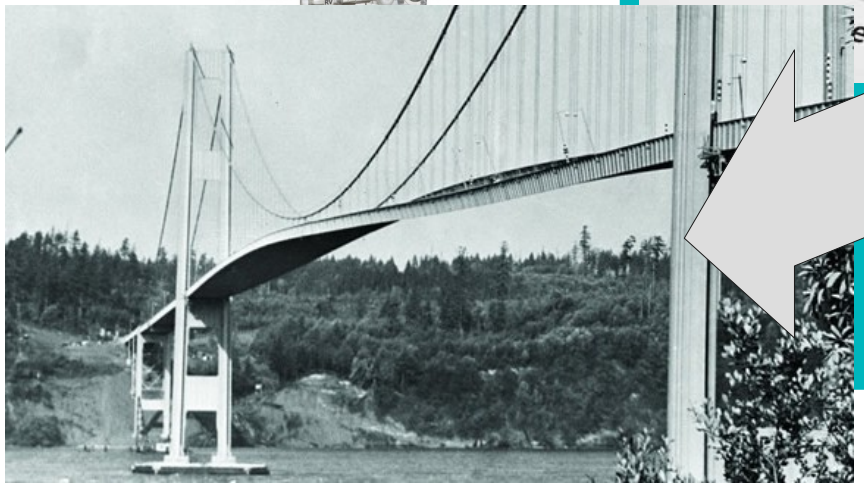
Vectors for Attack



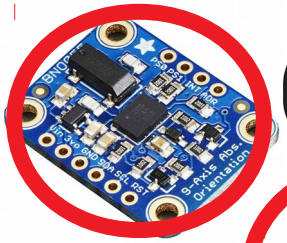


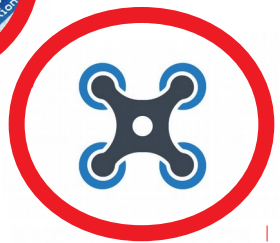






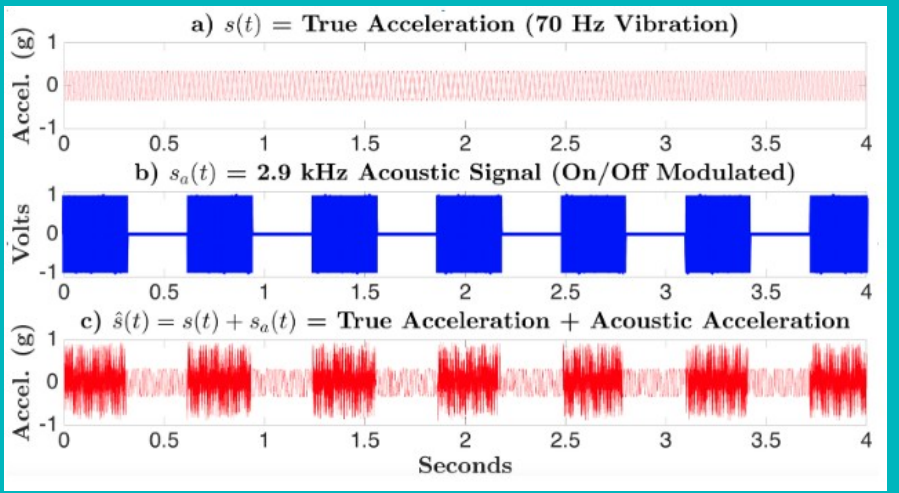
Vectors for Attack





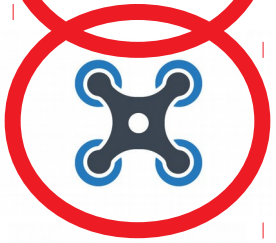
Inertial Measurement Unit

- MEMS are physical structures
- Use sound waves at resonant frequency to disrupt



"Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors" by Son et al.
"WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks" by Trippel et al.

Vectors for Attack

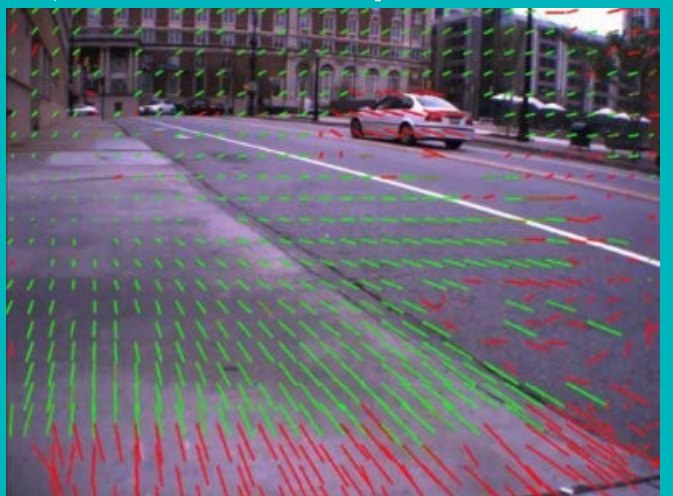


Video Cameras

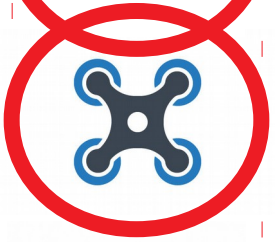
- Common, important sensor
- Detect features (corners) and track px motion
- Use cameras to build 3d-maps
  - Stereo cameras
  - Mobile cameras

  → **Optical flow**

How can we attack this sensor?



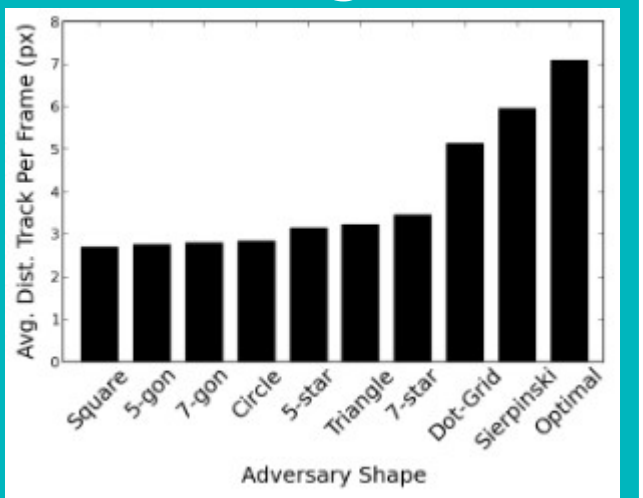
Vectors for Attack



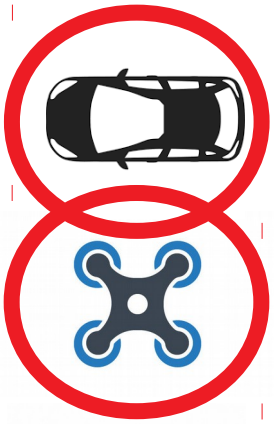
Video Cameras

- Use a projector to 1. cast a feature rich image on the ground, and 2. move that image.
- Use a laser to do the same with a sharp pattern

"Controlling UAVs with Sensor Input Spoofing Attacks" by Davidson et al.



Vectors for Attack



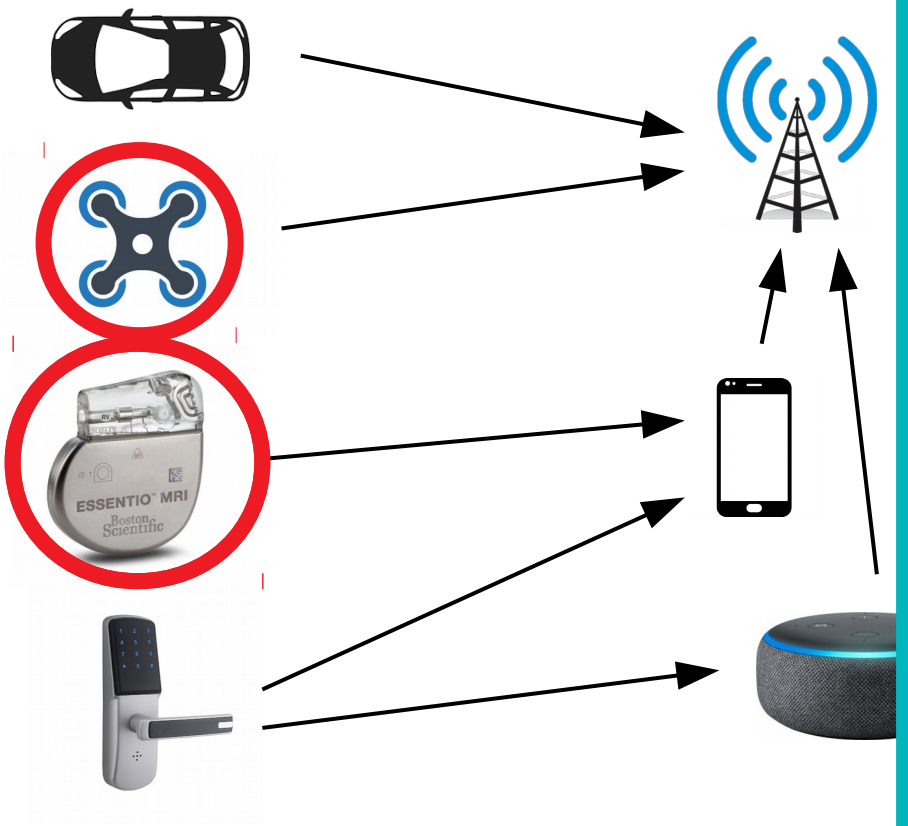
Perspective on Sensor Attacks

- AV's sensor processing stack is complex:

  s = kalman_filter(read_sensors([audio, GPS, IMU, …]))
  write_actuators(pid(s, plan))

- How do we design systems to be resilient to attacks?
  - Better sensors
  - Redundant sensors
  - …

Vectors for Attack

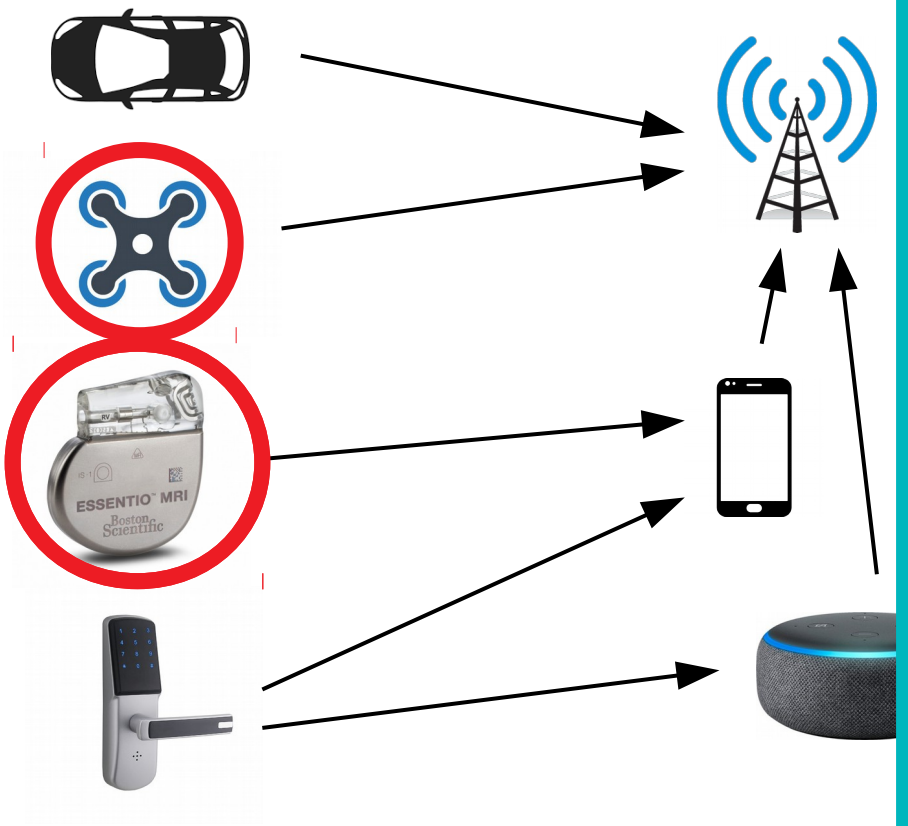


Actuator Attacks

- StuxNet:
  - gain control of PLCs
  - send erratic commands to centrifuges
  - mask disruption
- Pacemaker: change timing of electrical signals
- Quadcopter: cause instability

How can we try and prevent these types of attacks?

Vectors for Attack



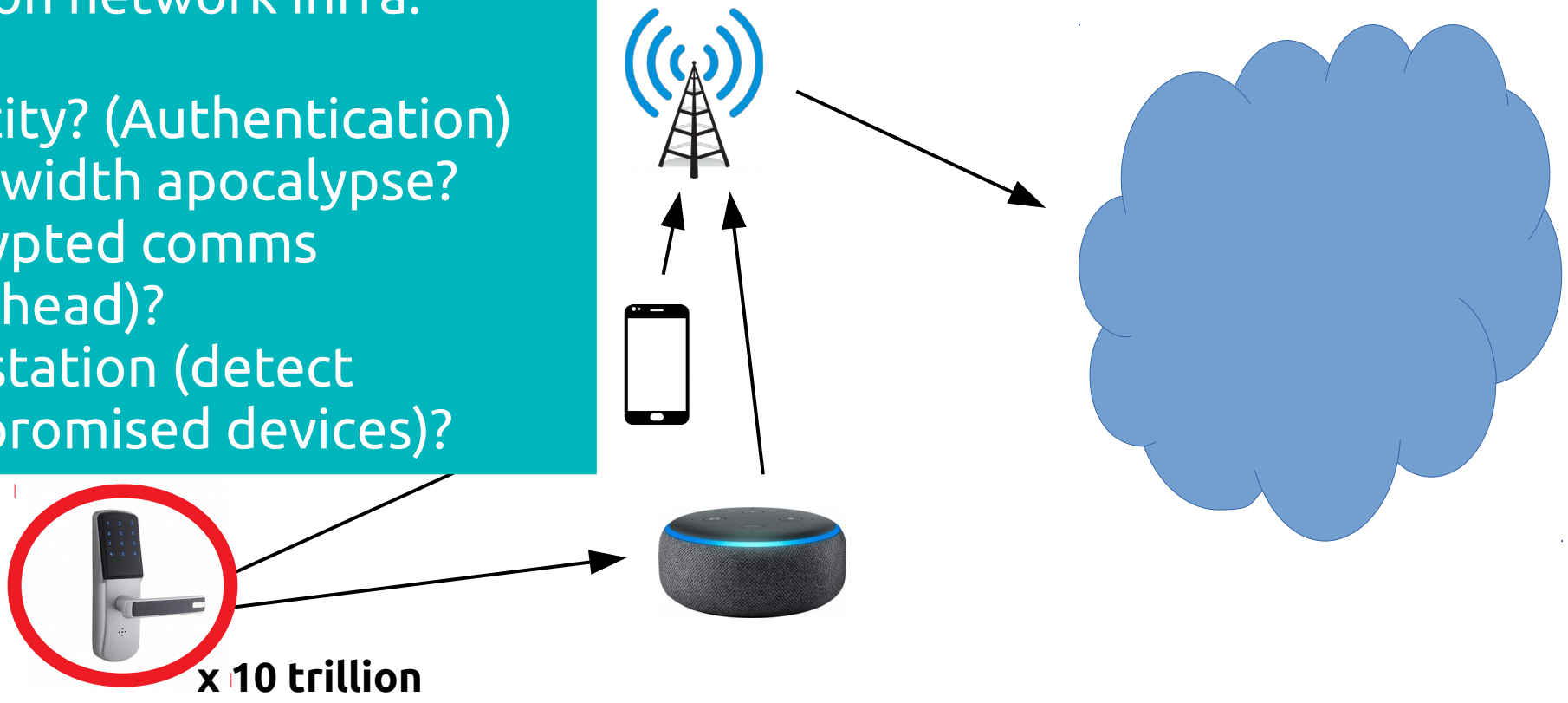
Actuator Attacks

- Rely on system model:
  - Mathematical description of system dynamics
  - Updated with new sensor information
- Predictive: used for planning/ control
- Detecting: are system dynamics deviating from expected?
  - *Challenges?*

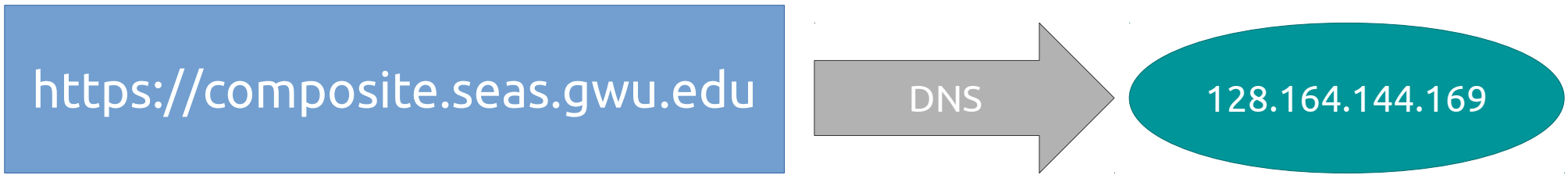
Vectors for Attack

Impact of Trillions of devices on network infra.

- Identity? (Authentication)
- Bandwidth apocalypse?
- Encrypted comms (overhead)?
- Attestation (detect compromised devices)?



[Sec] IIoT: Naming & Identification



✓ Business

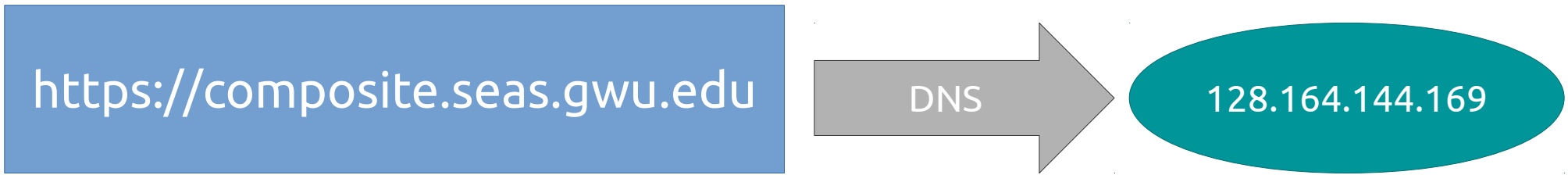
✓ Server

✗ IoT device

✗ IoT dev

- Billions of devs, humans → device & dev → dev

Authentication Challenges



✓ Business ✓ Server

Solutions? Options?

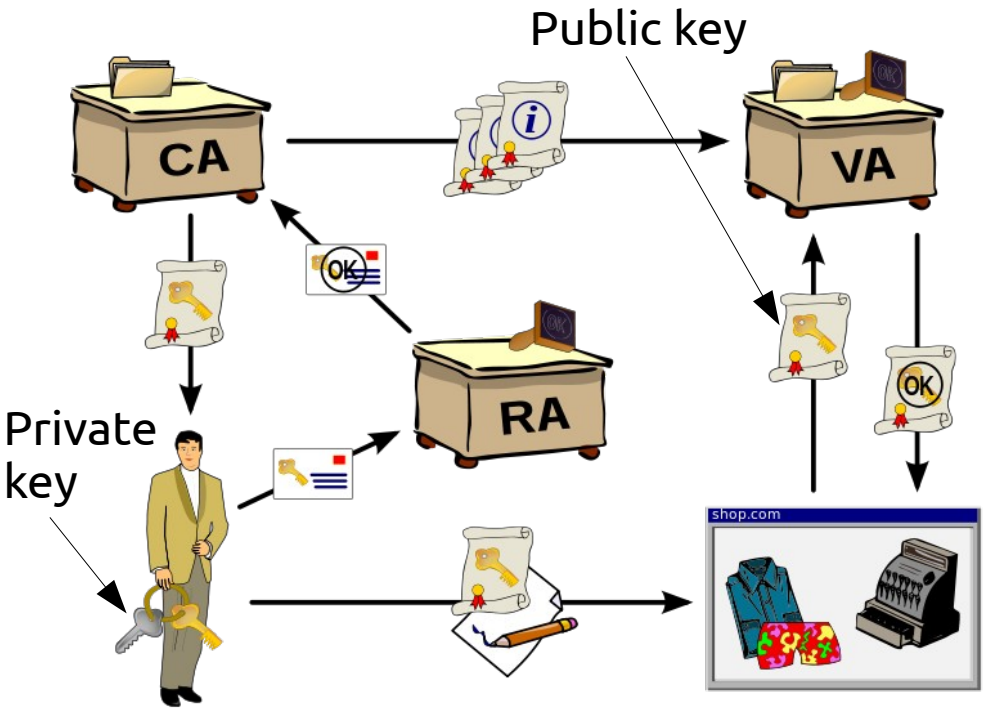
✗ IoT device ✗ IoT dev

- Billions of devs, humans → device & dev → dev

Authentication Challenges II

Solving:
Am I talking to X?

- X = business/org
- SSL/TLS
  (used in http**s**://...)



CA/RA/VA =
Certificate/Registration/Validation Authority

Image: Thanks Wikipedia!

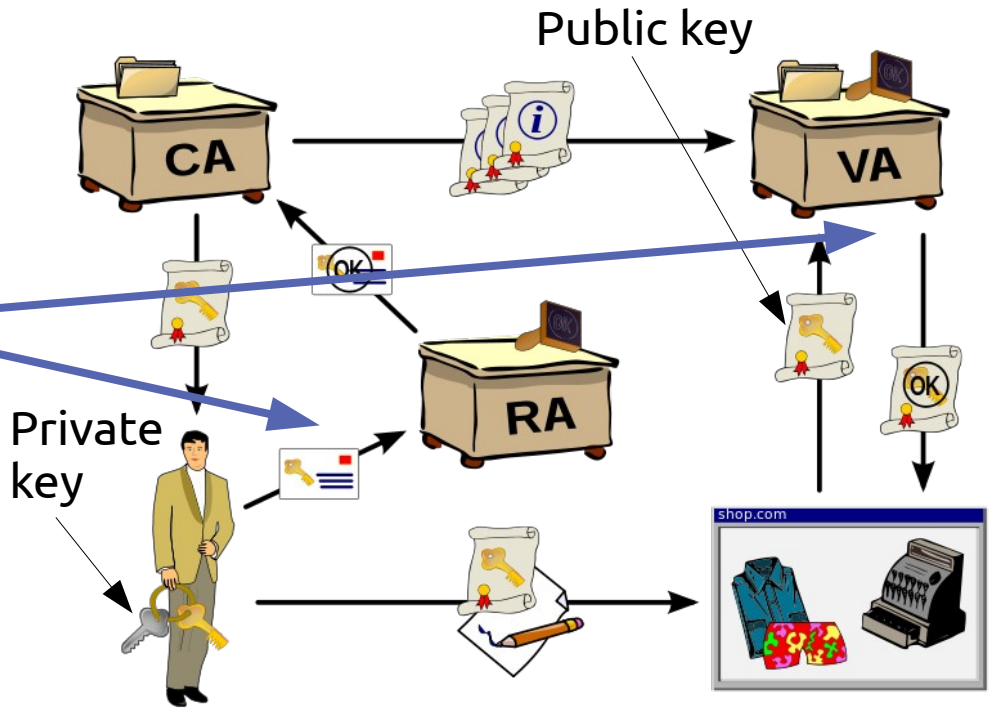
Authentication Challenges III

Solving:

IoT: Trillions of devices

Will this scale to billions of devices?

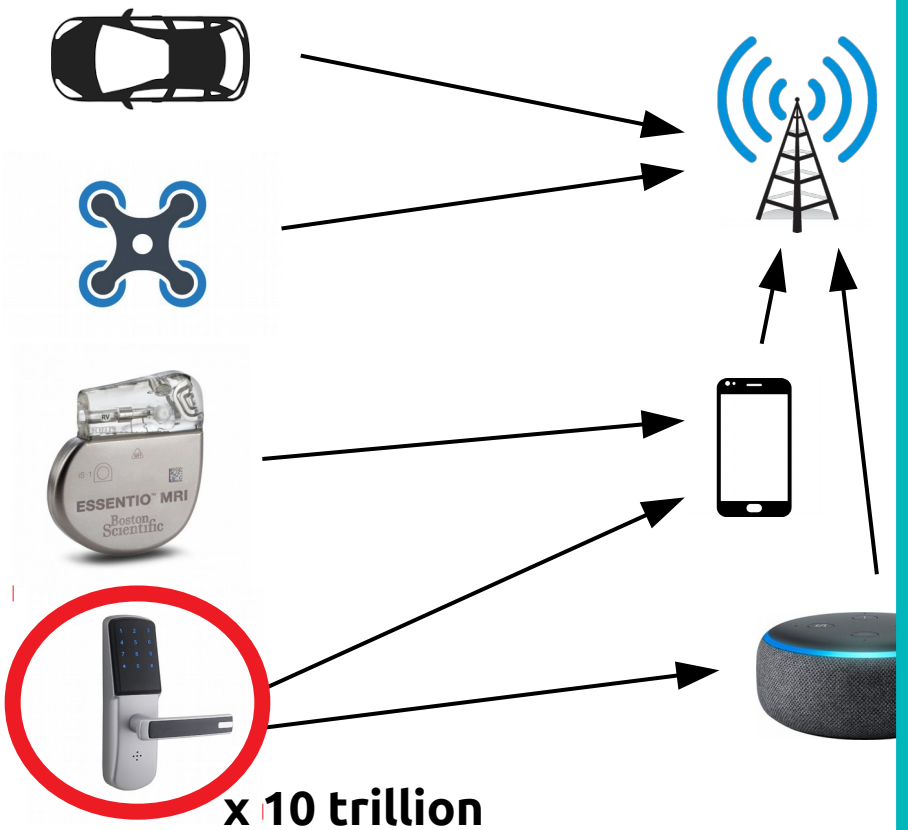
SSL/TLS (used in https://...)



CA/RA/VA = Certificate/Registration/Validation Authority

Image: Thanks Wikipedia!

Vectors for Attack



Impact of Trillions of devices

- Software update
  - Without physical access
  - With low power/intermittent net.
- Secret dissemination
  - RSA keys, passwords in plaintext in binaries
- Attestation
  - Know we're talking to a trusted program? TPM/root of trust
- "Get things done" mentality
  - Telnet accessible
  - Backdoors

Conclusions

- CS is going in the direction of Civil/Mechanical
  - Physical safety determined by software
  - The future of liability for errors is unclear
- IoT poses new security challenges, requires new techniques
  - Scale, lack of physical access, sensors/actuators