

# Security and Privacy Issues in IoT Applications

CSIE5292 Systems and Network Security Laboratory, Spring 2019

<https://cool.ntu.edu.tw/courses/309>

[seclab-ta@csie.ntu.edu.tw](mailto:seclab-ta@csie.ntu.edu.tw)

Hsu-Chun Hsiao

# Warm up: new security/privacy Issues in each application?



Smart Home



Automotive



Drone



Voice-controlled Device



Smart Factory

# Smart Home Security

# Smart Home

- A residence where **internet-connected devices** cooperate **automatically** and are **managed by houseowners** via various user-friendly interfaces
- Popular providers
  - Samsung SmartThings
  - Google Home
  - Apple HomeKit
  - D-Link Connect home



# Smart Appliances



Smart pan: *Pantelligent*



Smart coffee machine: *Behmor Coffee Maker*

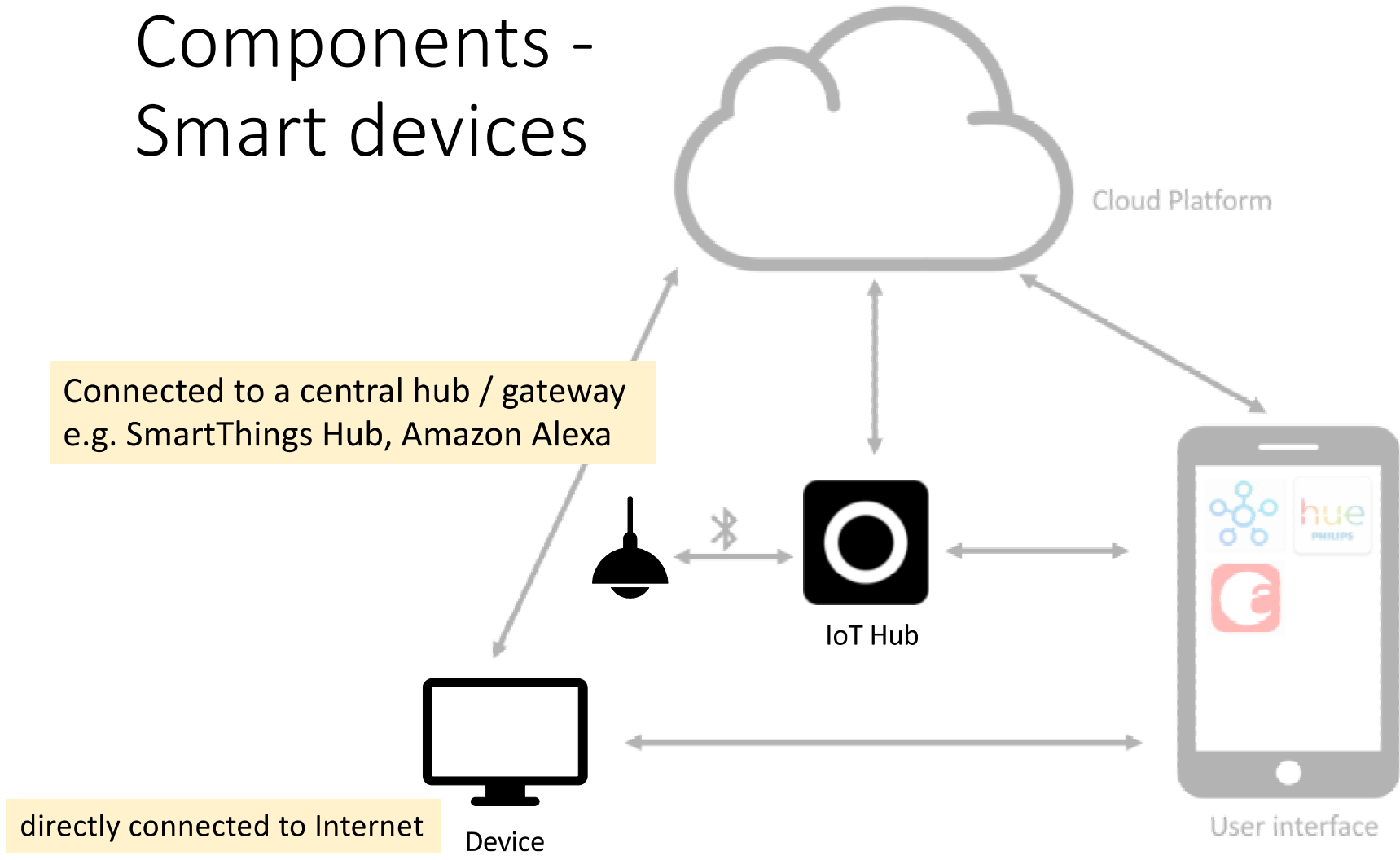
# Smart Appliances

Type	Example
Heating, ventilation, air conditioning	Thermostat, air purifier
Lighting control system	Smart lighting, smart switch
Energy monitoring	Smart plug, smart meter
Leak detection	Water sensor, CO sensor
Security system	Door & window sensor, motion sensor Surveillance camera Smart lock, smart alarm
Assistive domotics	Designed for the elderly and disabled Home robotics Emergency assistance Smart medical devices

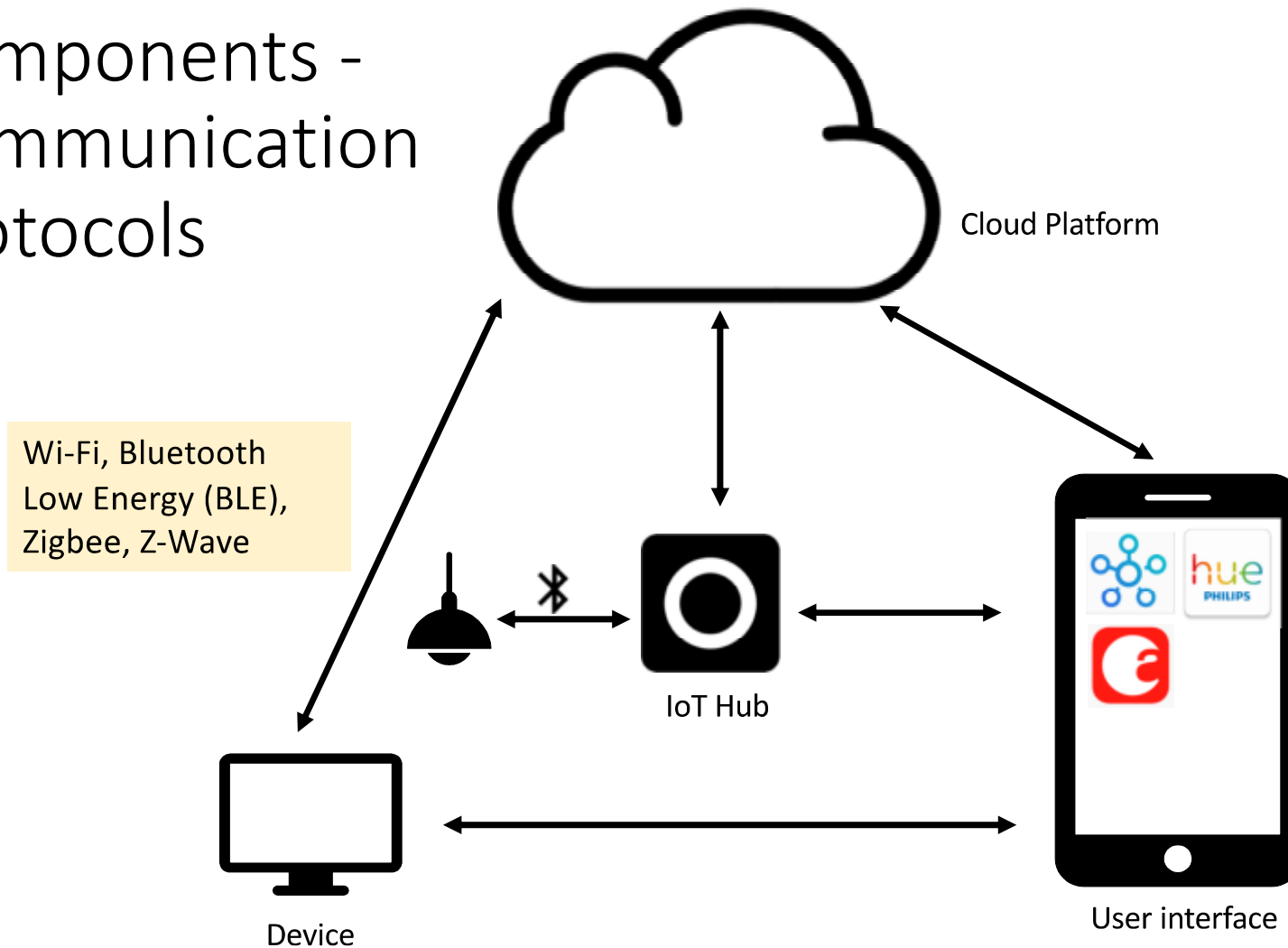


*Nest Thermostat, Philip Hue  
D-Link Water Sensor & Smart Plug*

# Components - Smart devices



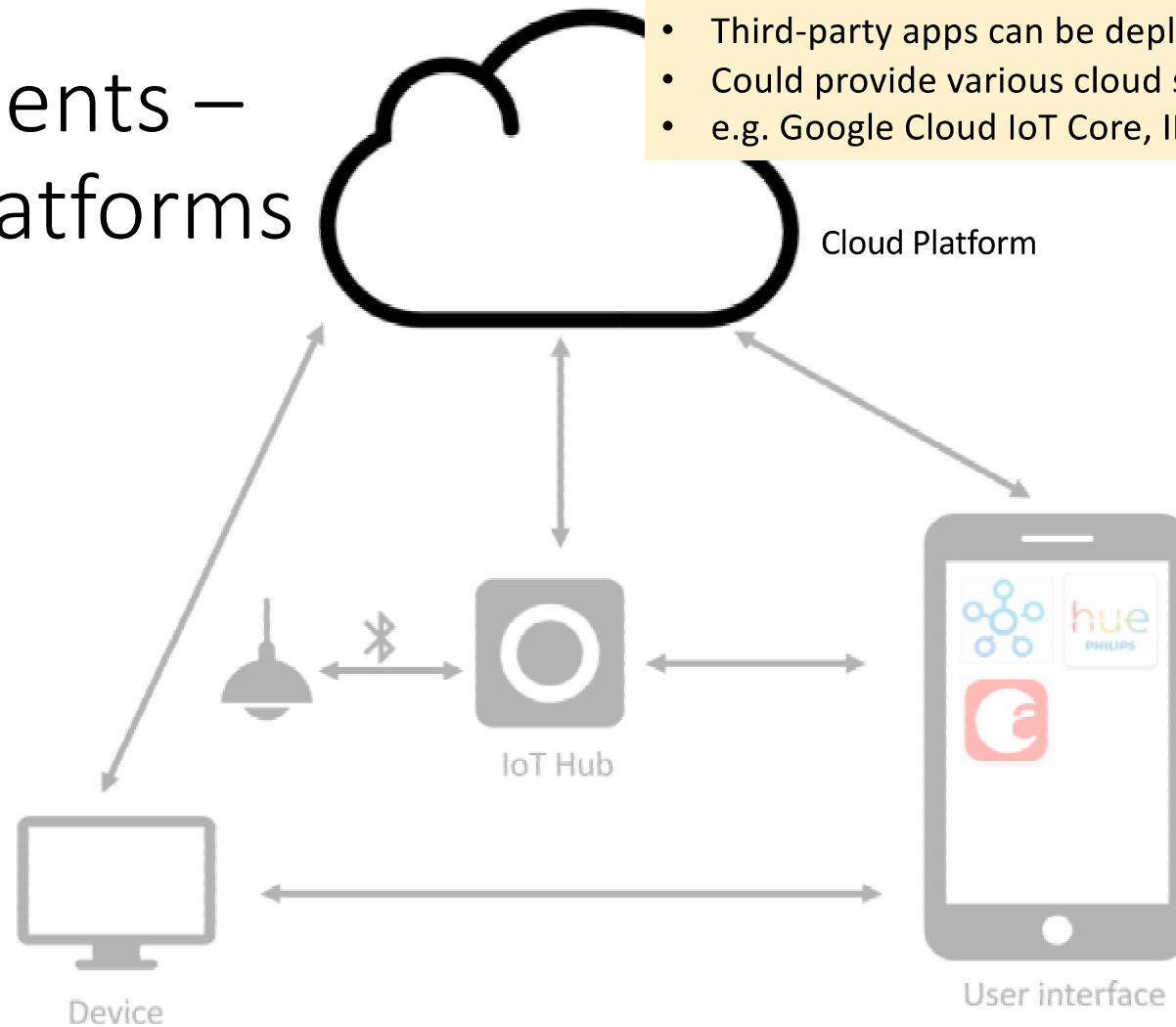
# Components - Communication protocols



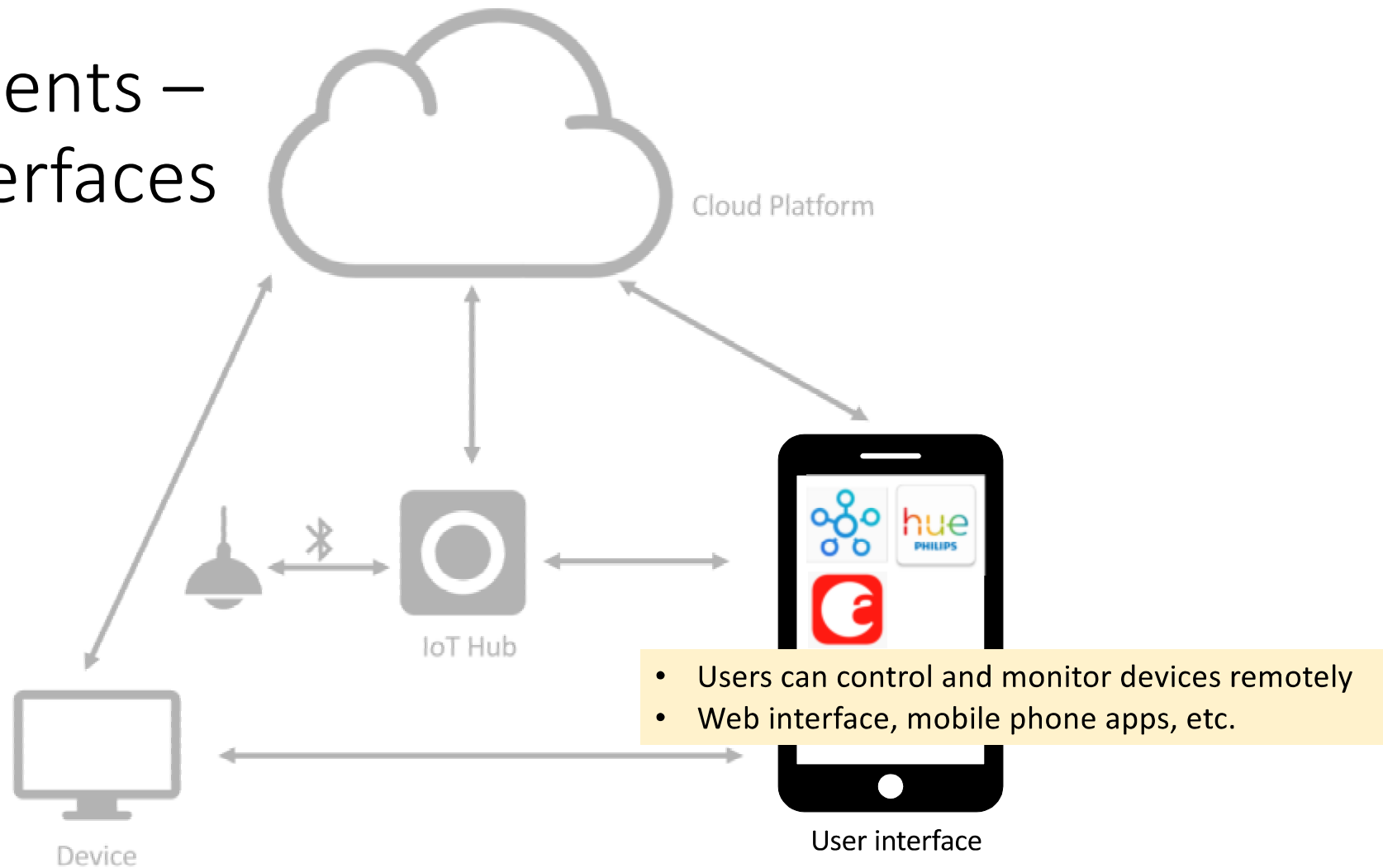


# Components – Cloud Platforms

- Third-party apps can be deployed on cloud platforms
- Could provide various cloud services
- e.g. Google Cloud IoT Core, IFTTT, Zapier



# Components – User interfaces



# Smart Home Case Study - Samsung SmartThings

# SmartThings

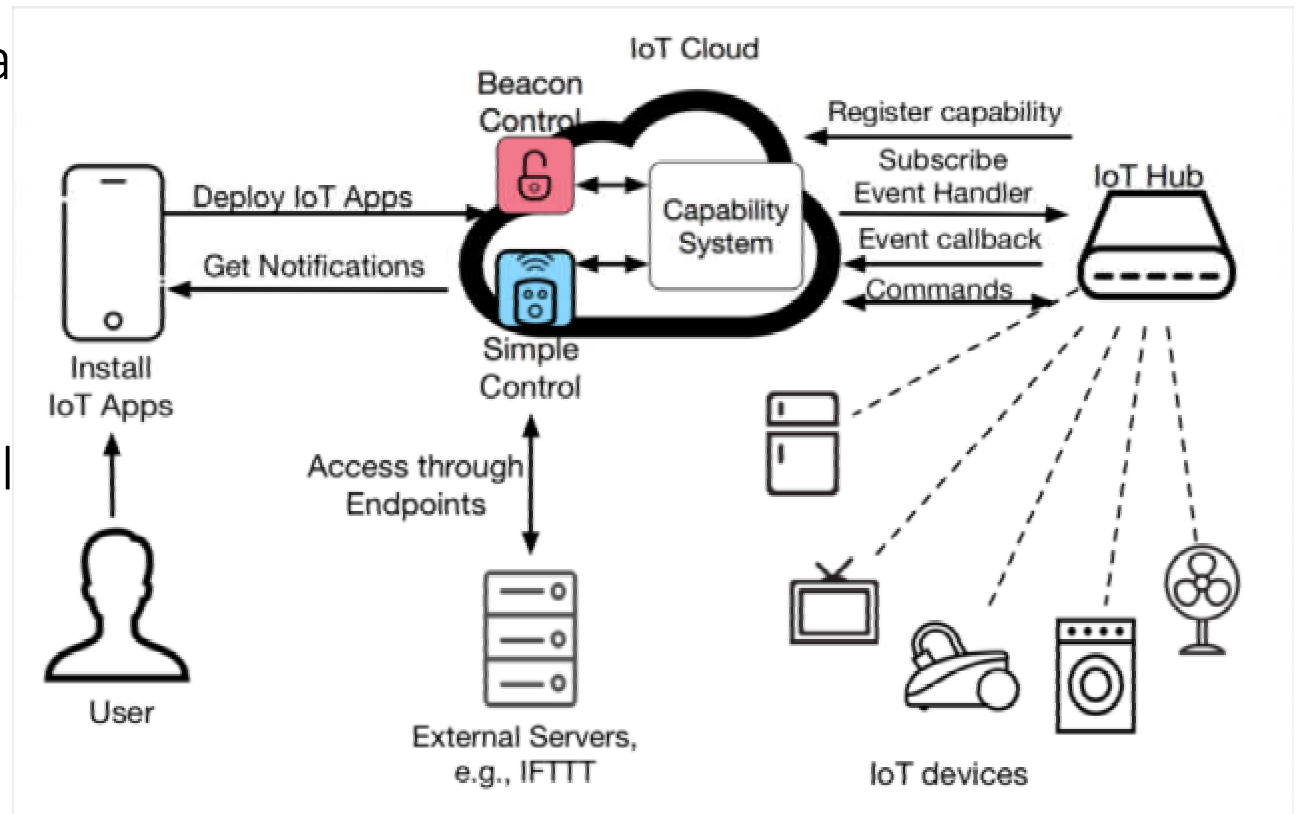
*“Add a little smartness to yours things.”*

- A commercial IoT framework that integrates heterogeneous IoT ecosystems
- Support around 170 IoT devices
- Support diverse communication protocols
- Provides a web-based programming environment



# SmartThings Architecture

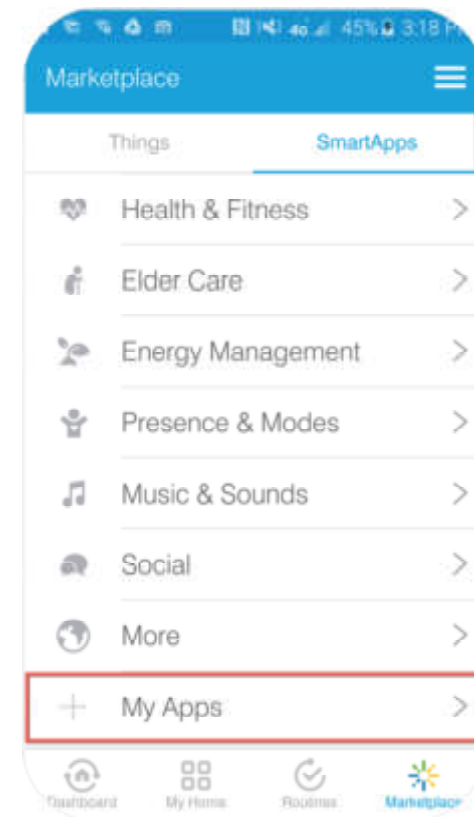
- User installs IoT apps via mobile devices
- IoT apps pair **event handlers** to IoT devices
- Cloud interacts with user's devices
- IoT apps enable external interaction via the web



*“SmartAuth: User-Centered Authorization for the Internet of Things”, USENIX Security ‘17*

# SmartApp

- Users can install/deploy apps from *Marketplace*
- Developers can write and publish apps
- SmartApp APIs
  - Provide access and control for external systems
  - Authenticated by OAuth 2.0



# SmartApp Authorization

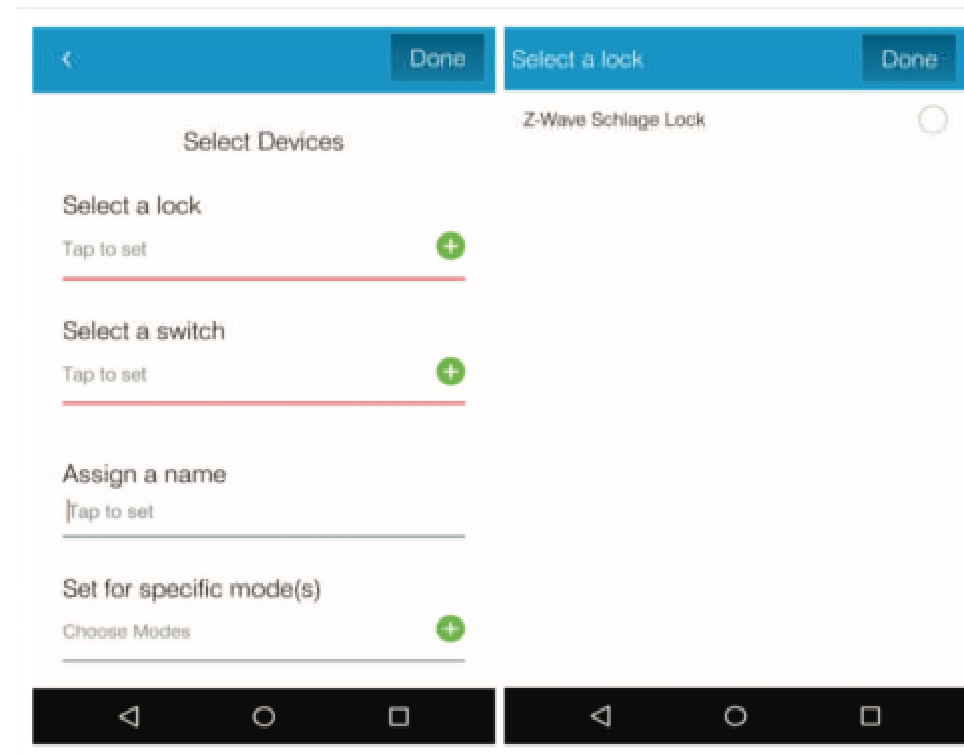
- **Capability:** The basic unit of authorization
  - **Attributes:** Properties of a device
  - **Commands:** Ways to control a device

<b>Capability</b>	<b>Commands</b>	<b>Attributes</b>
<code>capability.lock</code>	<code>lock()</code> , <code>unlock()</code>	<code>lock (lock status)</code>
<code>capability.battery</code>	N/A	<code>battery (battery status)</code>
<code>capability.switch</code>	<code>on()</code> , <code>off()</code>	<code>switch (switch status)</code>
<code>capability.alarm</code>	<code>off()</code> , <code>strobe()</code> , <code>siren()</code> , <code>both()</code>	<code>alarm (alarm status)</code>
<code>capability.refresh</code>	<code>refresh()</code>	N/A

# SmartApp Authorization

## → Example

1. Capability request
  - *capability.lock* and *capability.switch*
2. Scanned devices
  - Z-Wave Schlage Lock, ...
3. Selected devices
  - Select Z-Wave Schlage Lock
4. Successfully authorized
  - App is able to lock/unlock the smart lock





# Security flaws in SmartThings: Overprivileged Apps

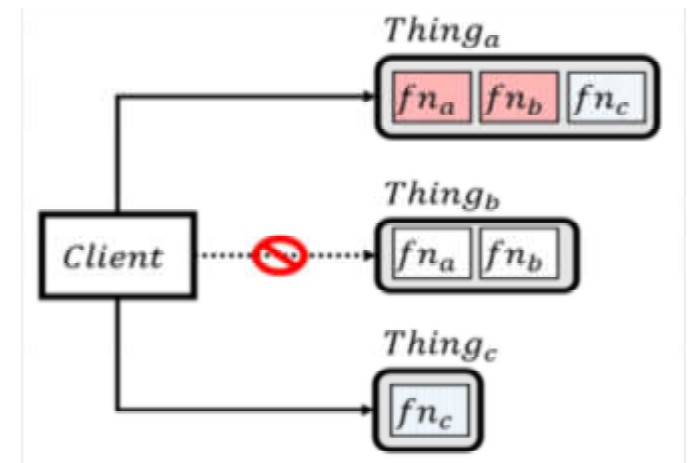
- **Overprivileged:** An app gains access to more operations on protected resources than it requires to complete its claimed functionality
- Root causes
  - Coarse-grained capability
  - Coarse device-app binding

# Security flaws in SmartThings: Overprivileged Apps

- Coarse-grained capabilities
  - Capability is the **basic unit** of authorization
  - An app is allowed to perform unneeded operations
  - *capability.lock* can do both *lock()* and *unlock()*
- Asymmetry in risk of commands
  - e.g. *switch.off()* v.s. *switch.on()*
  - Not appropriate to grant an app access to an unsafe command when it only needs to access a safe command

# Security flaws in SmartThings: Overprivileged Apps

- Coarse device-app binding
  - Device-centric approach
  - All-or-nothing approach
  - An app given **any** capability of a device is implicitly granted unlimited access to the **whole** device



# Example: *Auto-lock*

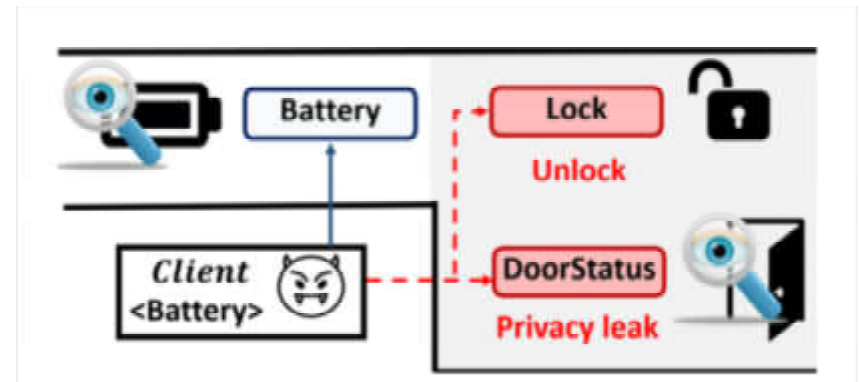
- App 1: *Auto-lock*
  - App description: *“Locks the door when nobody is at home.”*
  - Requested capability: *capability.lock*
  - User selected device: *Z-Wave Schlage Lock*
- Why over-privileged?

# Example: *Auto-lock*

- Reason: Coarse-grained capability
  - Though only *lock()* is needed
  - The app is able to lock **and unlock** the door lock

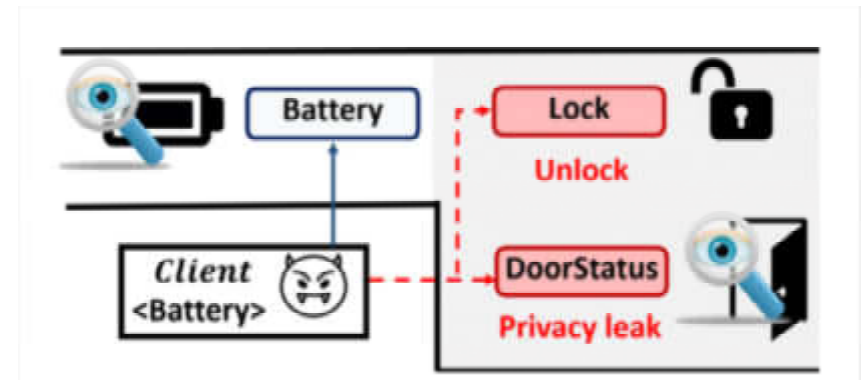
# Example: *Battery Monitor*

- App 2: *Battery Monitor*
  - App description: “*Monitor the battery status of your devices*”
  - Requested capability: *capability.battery*
  - User selected device: *Z-Wave Schlage Lock*
- Why over-privileged?



# Example: *Battery Monitor*

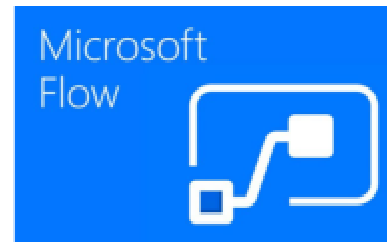
- Reason: Coarse device-app binding
  - Though only *capability.battery* is requested
  - The app is granted to access all capabilities of the device, including *capability.lock*



# Smart Home Case Study - IFTTT



# Automation Service Providers Connect Devices via Automation Rules



# Automation Service Providers Connect Devices via Automation Rules



IF-This-Then-That: "A free platform that helps you do more with all your apps and devices"

- Over **400** applications and devices are supported
- Over **19** millions rules are created
- Around **600 million** rules executed monthly

**Record Arlo clip when your door is opened**

When an abode door or window equipped with a sensor is opened, Arlo will record a video clip.

by **abode** ✓

Turn on

16 works with

**When it's steaming hot outside, switch the air conditioner on using Sensibo**

When the temperature outside is boiling hot, it's time to start cooling your house using Sensibo.

by **Sensibo** ✓

Turn on

300 works with

**Turn off WiFi when you leave home to save power**

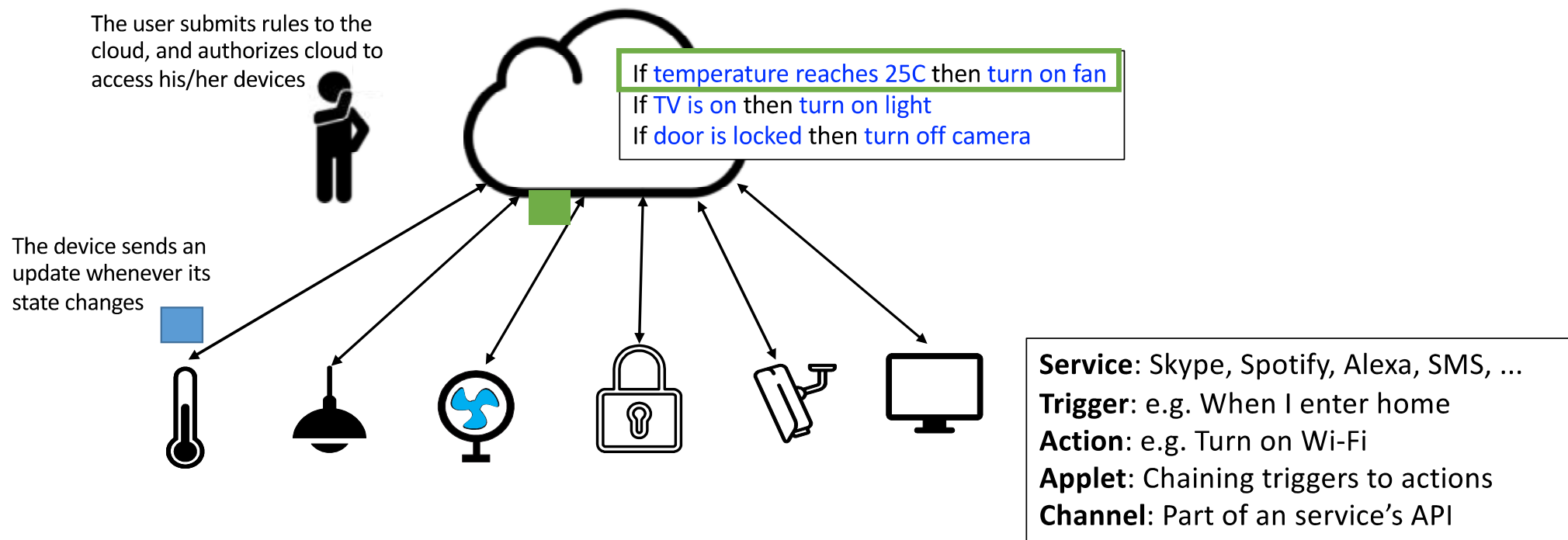
If you don't normally use WiFi when you're not at home, this Applet will help you save power throughout the day by turning off WiFi when you leave home.

by **IFTTT** ✓

Get Started

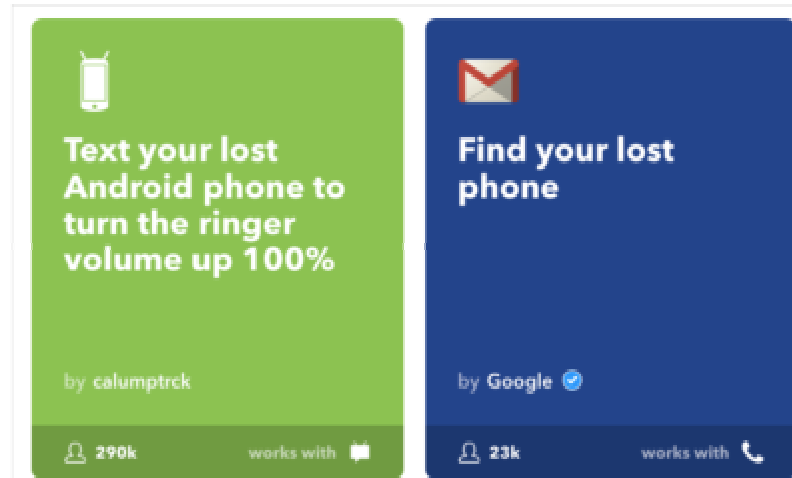
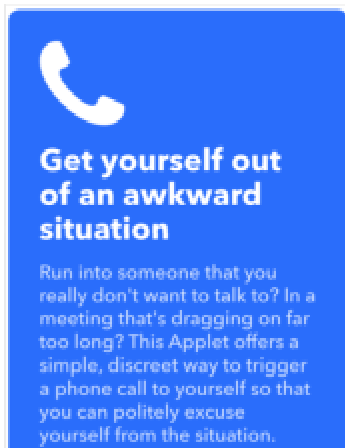
210k works with

# Automation Service Providers Connect Devices via Automation Rules



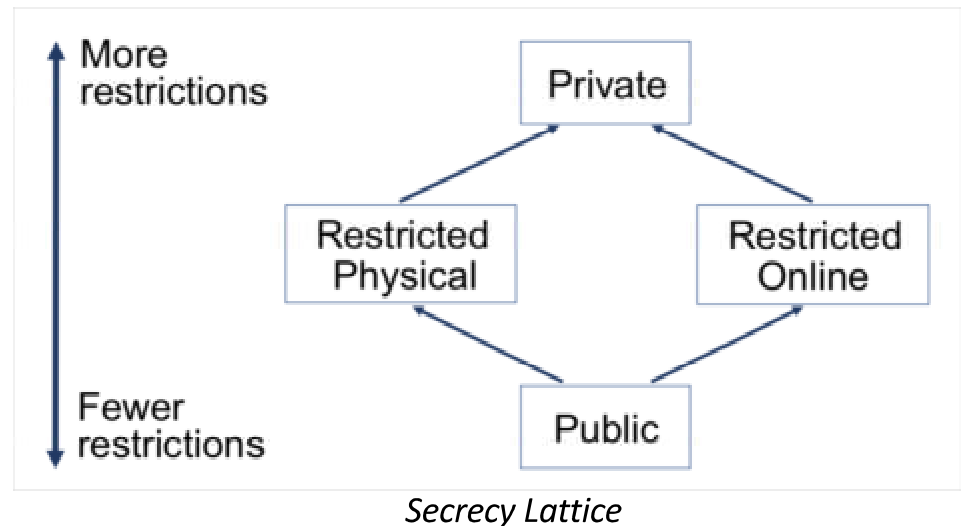
# Exercise

- 前往 <https://ifttt.com>
- 找一條你想使用的規則
- 找一條你可以用來惡作劇/做壞事的規則
- Can it be worse?



# IFTTT Security Issues

- Receipts could be “unsafe”
- Secrecy violation
  - If I take a new photo  
→ Add photo to Flickr
- Integrity violation
  - If I am tagged in a photo  
→ Create a Facebook status
- Chaining recipes
  - A → B & B → C
  - Exploit condition A to execute C



# IFTTT Security Issues

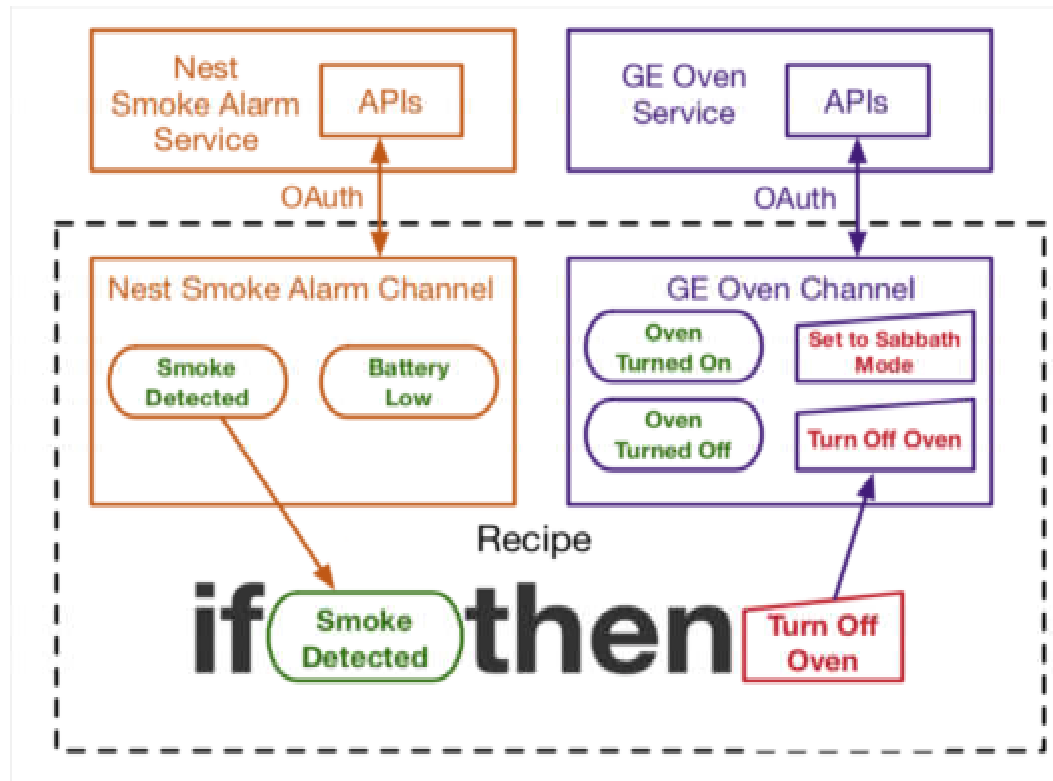
- *Chaining recipes* may cause unintended consequences

Chain	Recipe 1	Recipe 2	Type
C1	Convert an e-mail to event in Google Calendar	Send recurring Square Cash payments with Google Calendar & Gmail	privilege
C2	Disconnect from home Wi-Fi, start recording on Manything	When Manything detects motion, scare the intruder.	privilege
C3	Turn off sprinklers when I arrive home	If irrigation stopped, then blink lights	privacy
C4	When your nest thermostat is set to away then put your water heater in vacation mode	If water heater enters vacation mode, then turn off the lights	privacy

“SAFECHAIN: Securing Trigger-Action Programming from Attack Chains,” *Transactions on Information Forensics and Security*, 2019.

# IFTTT Security Issues

- OAuth 2.0
  - Allow IFTTT to access APIs to get or manipulate user's data on other services
- Security risks
  - Platform compromise
  - Over-privileged access tokens



*"Decentralized Action Integrity for Trigger-Action IoT Platforms"*

# IFTTT Security Issues

- Over-privileged access tokens
  - Online services are not designed to support only trigger-action platforms
  - Coarse-grained OAuth scopes
- What privileges will this applet request to access your twitter account?



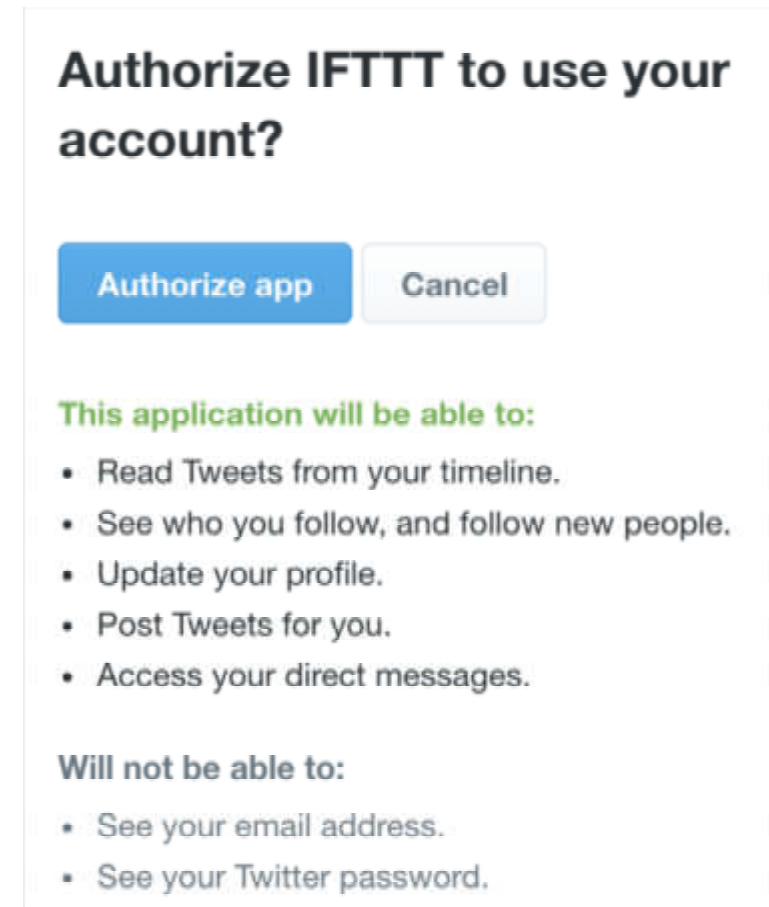
The image shows a dark blue IFTTT applet card. At the top left is a white icon of a document with three horizontal lines. To the right of the icon, the text reads: **Save tweets to a doc when you use a specific hashtag**. Below this, in a lighter blue font, it says: "When you use the hashtag you specify in the Applet, this will save your Tweet text and a link to them in a Google doc – easy to go back later and organize them or review!". At the bottom left, it says "by Google" followed by a blue checkmark icon.

*“Decentralized Action Integrity for Trigger-Action IoT Platforms”*



# IFTTT Security Issues

- Many of them are not necessary to complete the task
- User is only given an all-or-nothing choice



*"Decentralized Action Integrity for Trigger-Action IoT Platforms"*

# IFTTT Security Issues

What can IFTTT see?

If **phone's location** is near home, then **unlock door**



Phone's location is sent to the cloud for checking whether this trigger is satisfied.

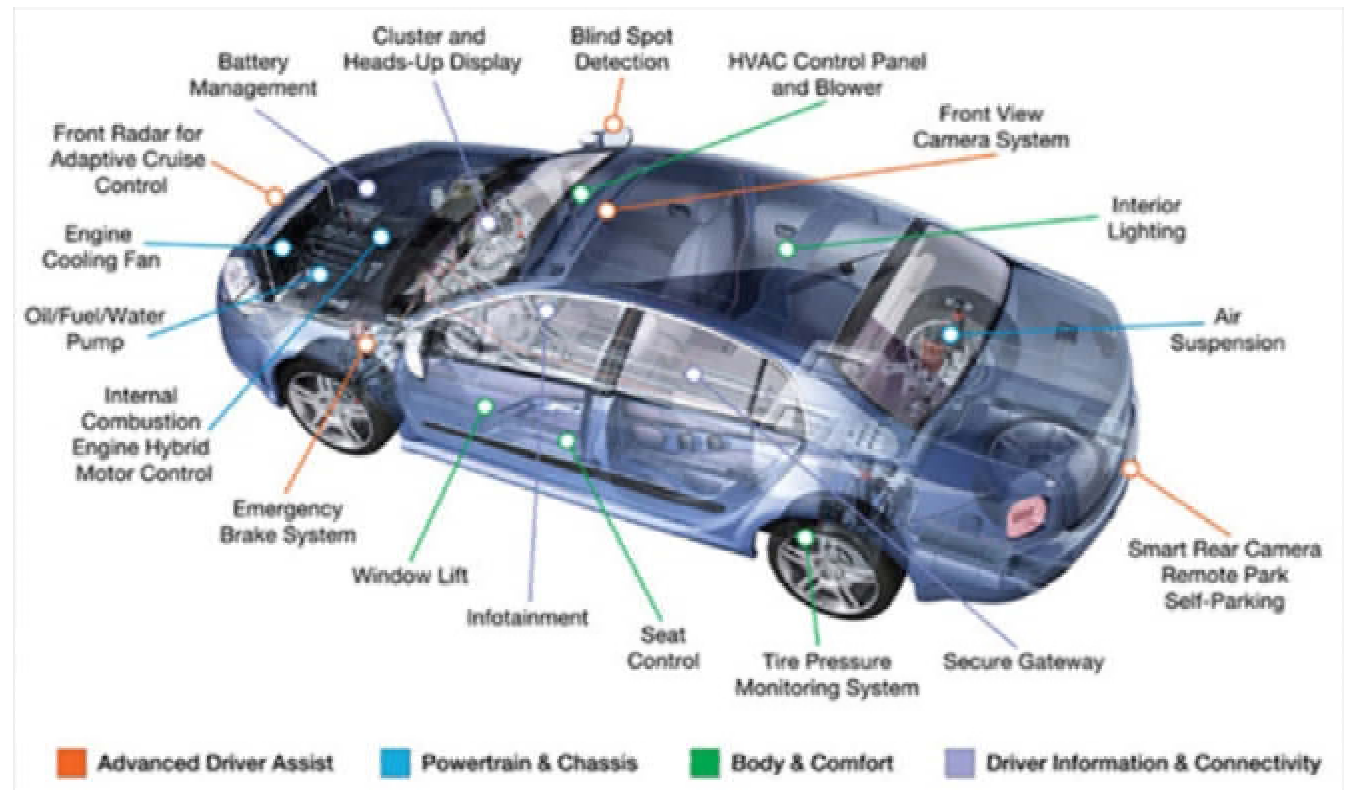
Once the trigger is satisfied, the cloud performs this action — sending an unlock command to the door.

- Data – trigger device's *state* and *associated data*
- Access pattern – *when* an action is performed over *whose* device

# Automotive Security

# Modern Cars

- Many subsystems
  - Emergency break
  - Blind spot detection
  - HVAC control panel
  - Smart rear camera
  - Secure gateway
  - ....



# Car Hacking

- Why hacking cars?
- What will happen if a car is hacked?
- Is the current design of cars secure enough?



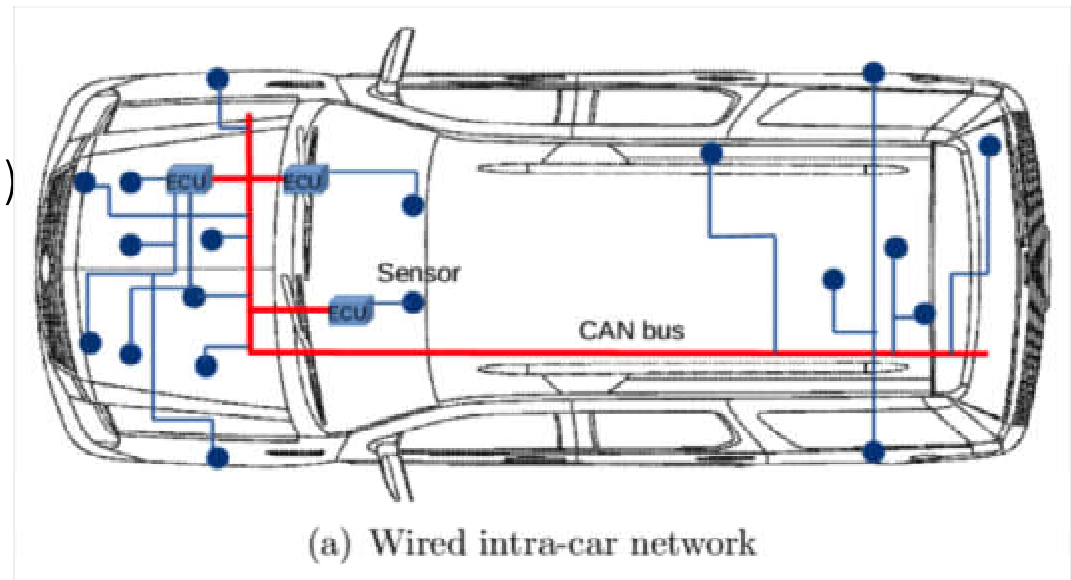
# Attack Vectors of a Car

- Car sensors and actuators
- In-vehicle network
- Control unit of cars
- Driving assistance systems
- AI models used in car system
- Software of car system
- Communication between cars
- ...

# Automotive Security: In-vehicle network

# Controller Area Network (CAN)

- “A vehicle bus standard designed to allow microcontrollers and devices to communicate with each other without a host computer”
- Features
  - Multicast
  - No node configuration (address)
  - Deterministic

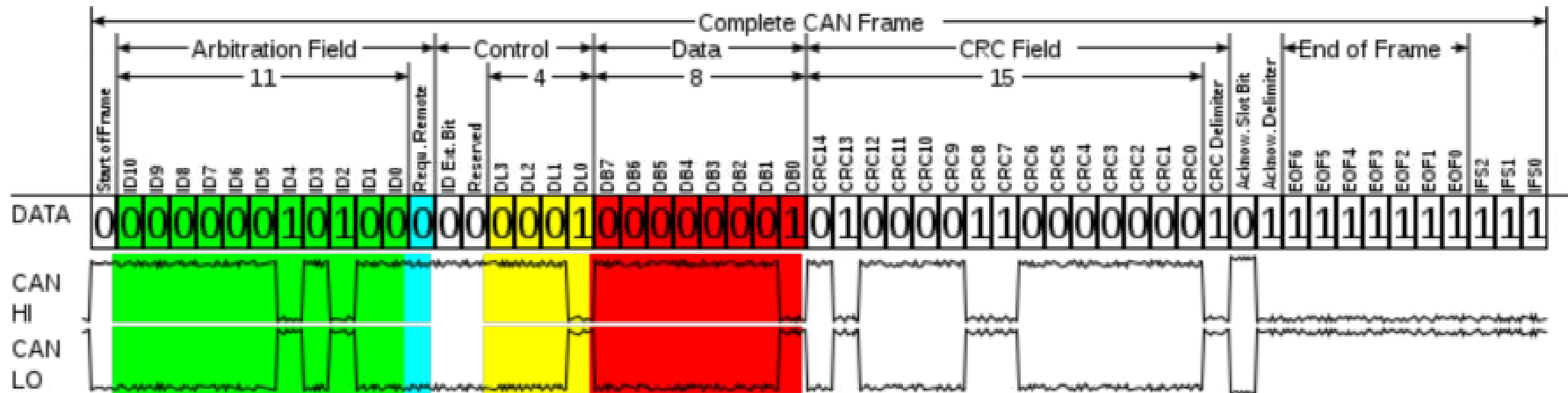


*“On feedback-based rateless codes for data collection in vehicular networks”*



# Controller Area Network

- Base frame format
  - Green - Message identifier (11 bits)
  - Red - Data field (at most 64 bits)



[https://en.wikipedia.org/wiki/CAN\\_bus](https://en.wikipedia.org/wiki/CAN_bus)

# Hacking CAN Bus

- CAN protocol is not designed to be secure
  - No encryption
  - No authentication mechanism
- If an attacker can access CAN bus, ...
  - Sniffing messages
  - Replay attack
  - Jamming attack

# Hacking CAN Bus

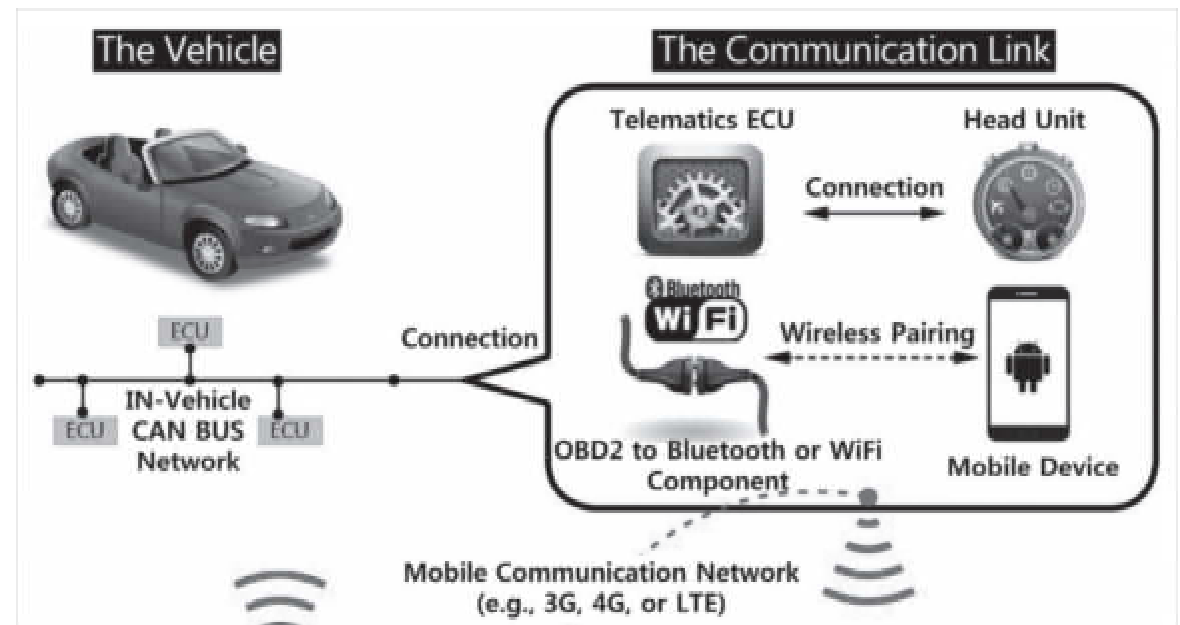
- Onboard Diagnostic port (OBD2)
  - Direct interface to a vehicle's CAN bus
- Reverse engineering CAN bus communications
  - Analyze the message IDs and payloads
  - Inject fake messages to control the car



*OBD2 Port on 2005 Nissan Titan*

# Hacking CAN Bus

- Connecting CAN bus to the world
- Attacker controls the car by a malicious self-diagnostic app connected to OBD2



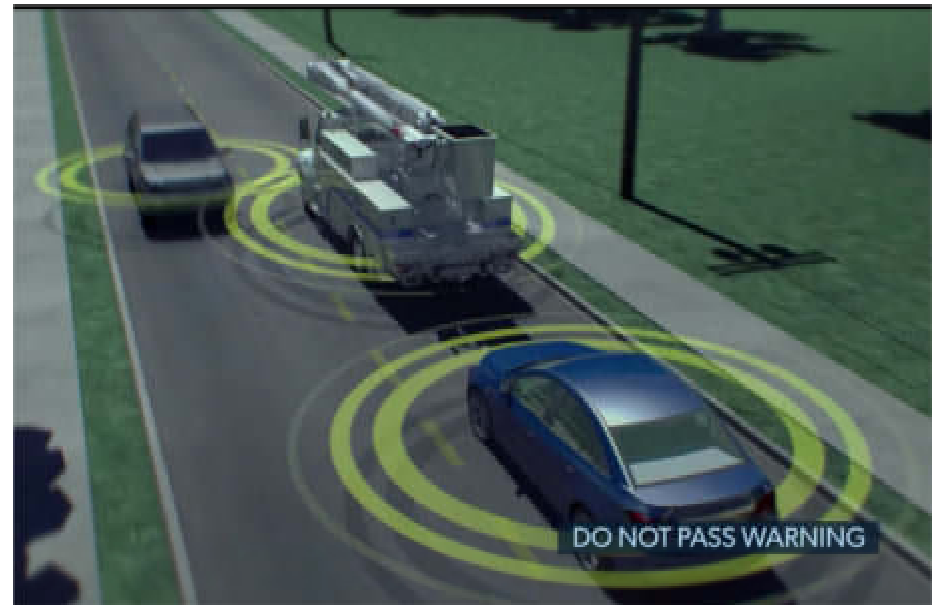
# Automotive Security: VANETs

# Intelligent Vehicles

- **Connected** and **autonomous** vehicles
- Connectivity
  - The ability of communicating to others
  - Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I)
- Autonomy
  - The ability of “self-governing”
  - Environment sensing, steering control, ...
- Example - Passing through an intersection

# Vehicular Ad-Hoc Network

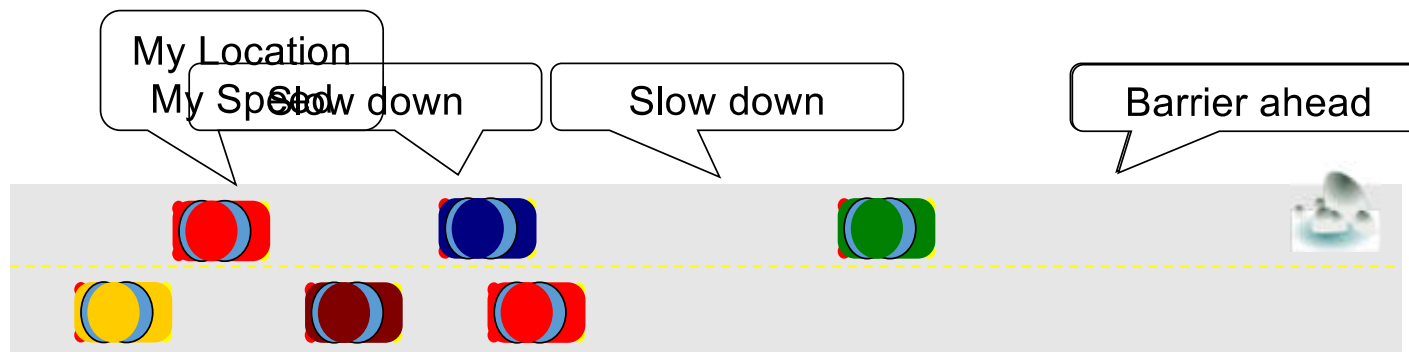
- Vehicle-to-vehicle communication (V2V)
  - GPS, speed, heading, break status, ...
  - Path history, path prediction
- Applications
  - Vehicle collision avoidance
  - Blind spot warning



U.S. department of transportation, "Connected Vehicle: The Future of Transportation", [Video](#)

# Vehicular Ad-Hoc Network (VANET)

- Each vehicle possesses an On Board Unit (OBU)
  - Broadcasts info for safety & convenience





# Vehicular Ad-Hoc Network

- Vehicle-to-infrastructure communication (V2I)
  - Railroad crossing, traffic lights
- Applications
  - Traffic monitor
  - Dynamically adjust driving speed
  - Travel information



U.S. department of transportation, "Connected Vehicle: The Future of Transportation", [Video](#)

# VANET Safety Messages

- SAE Basic Safety Message (U.S.)
- Properties
  - Periodically broadcast (100ms ~ 1s)
  - Must be authenticated
  - Encryption not recommended

Item
Time
3D Position
Position Accuracy
Speed
Heading
Steering Wheel Angle
Acceleration
Brake Status
Vehicle Size
Event Flags
Path History
Path Prediction
Other optional fields

# VANET Security Issues

- Can messages from others be trusted?
  - A car lying about its position, speed, route
- Is communication between cars secured?
  - Confidentiality, authenticated, ...
  - MitM attack
- Would there be selfish or malicious drivers?
  - Aim to jam the traffic or cause a car accident

# VANET Security Issues

- Lack of privacy protection
  - Wireless medium
  - Can be easily eavesdropped by passive adversaries
- Location privacy
  - What can an adversary do with your location information?
  - How “valuable” is your location information?
  - Location tracking

# Security Requirements of VANET

- Message authentication
  - Authenticate the origin of message
- Network availability
  - Real-time applications
- Non-repudiation
  - Identify the attackers after the attack happens
- Privacy
  - Anonymization services

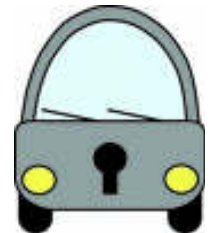
# Current Standard for Securing VANETs

- IEEE 1609.2 VANET security standard:
  - Vehicles digitally sign every broadcast message using *ECDSA*
    - ECDSA = Elliptic Curve Digital Signature Algorithm
  - Vehicles change public keys periodically
- Digital signatures provides **origin authentication, message authentication, non-repudiation**
- Changing public keys improves **privacy**



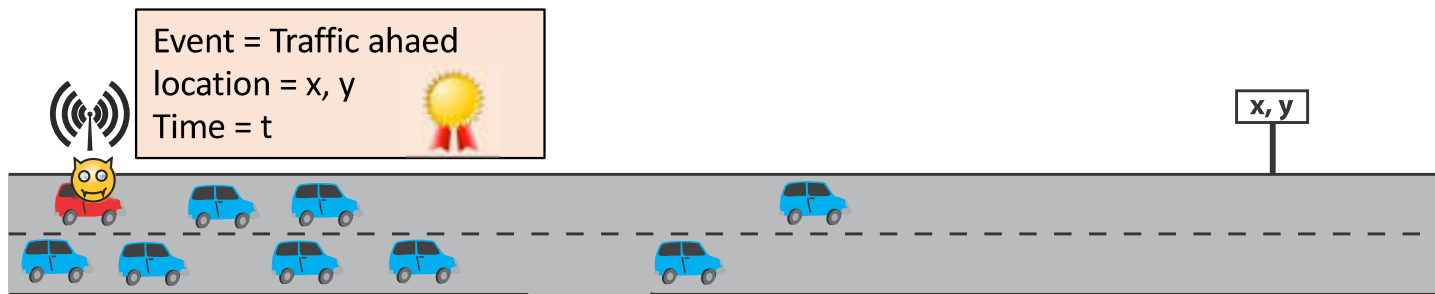
# Current Standard for Securing VANETs

- Current standard using digital signatures & public key certificates alone is not enough
  - ✓ Prevent impersonation
  - ✓ Prevent a vehicle from posing as multiple vehicles (Sybil attack)
  - Improve privacy (but still a big problem)
  - ✗ Address event falsification
  - ✗ Address signature flooding
  - ✗ Address jamming
  - ✗ Address message suppression

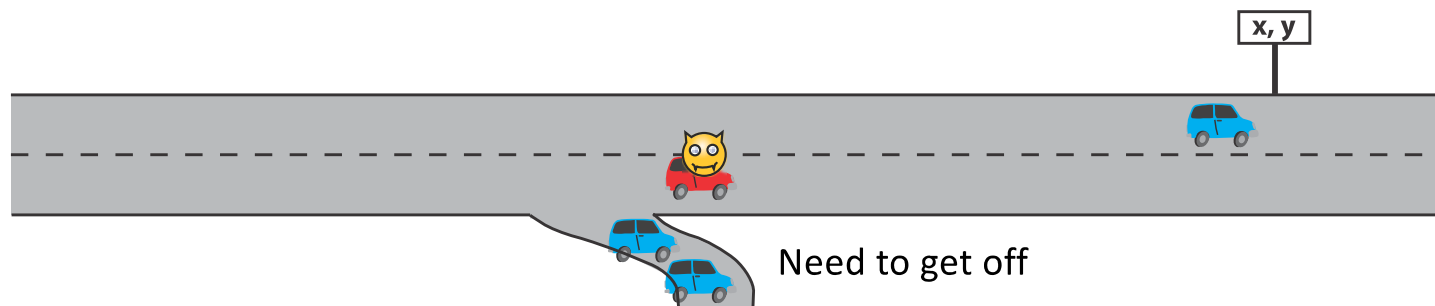


# Event Falsification

1. 自私的用路人送出假情報

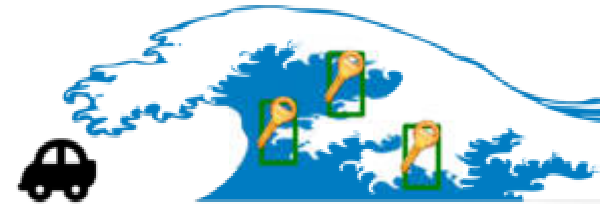



2. 其他用路人都被騙，自私的用路人繼續留在路上





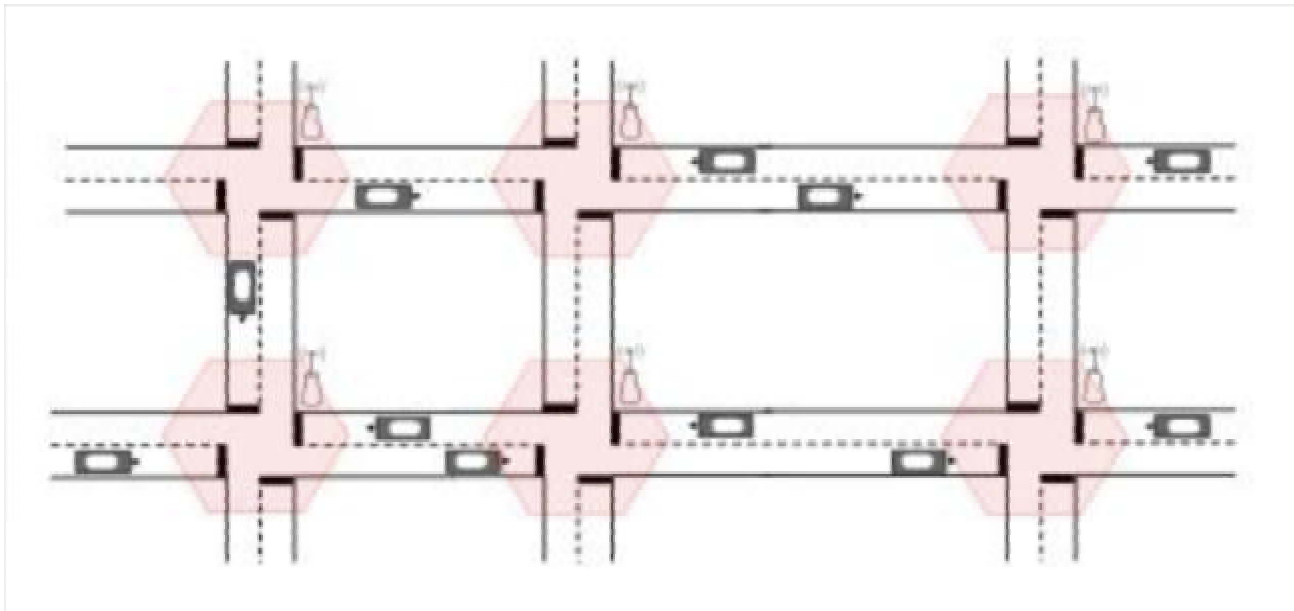
# Signature Flooding



- Expensive verification
  - 22 ms to verify ECDSA signature  on 400MHz processor
- Many messages may arrive in a short time period
  - Every vehicle broadcasts location every 100ms
  - 5 neighbors → 50 updates/s → >100% saturated
- Severely limits effectiveness of VANET applications

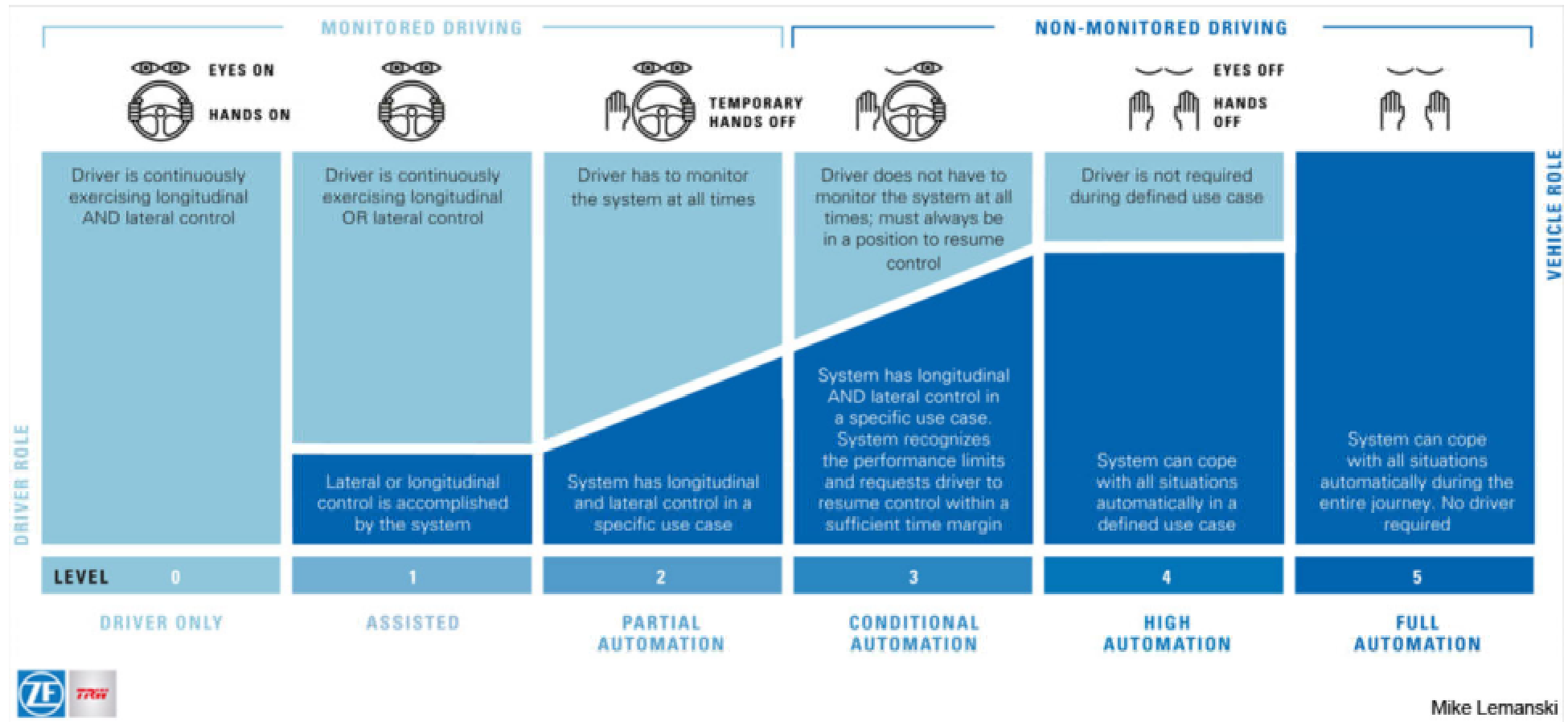
# Privacy

- Changing public keys periodically
  - Still linkable via timing analysis



# Automotive Security: Autonomous Cars

# SAE Level 0-5



<https://www.birmingham.ac.uk/news/thebirminghambrief/items/2016/11/driving-the-revolution.aspx>

# SAE Level 0-5

- Level 0 - Driver Only
- Level 1 - Driver Assistance
  - Driver and automated system share control of vehicle
  - e.g. Parking Assistance, Lane Keeping Assistance
- Level 2 - Partial Automation
  - Automated system takes full control of accelerating, breaking, steering
  - Drivers must monitor the driving

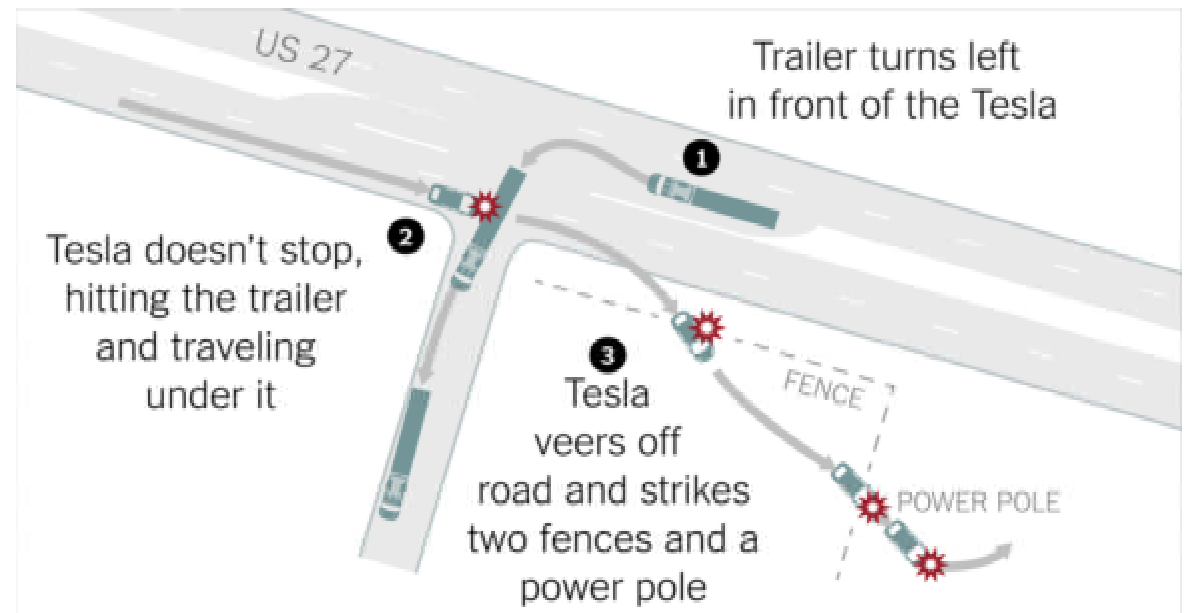
*[https://en.wikipedia.org/wiki/Self-driving\\_car](https://en.wikipedia.org/wiki/Self-driving_car)*

# SAE Level 0-5

- Level 3: Conditional Automation
  - Driver can turn their attention away from driving tasks
  - Driver must respond to a request intervene by the system
- Level 4: High Automation
  - No driver attention is required for safety
  - Self-driving is supported in limited areas or under special circumstances
- Level 5: Full Automation
  - No human intervention is required

# News

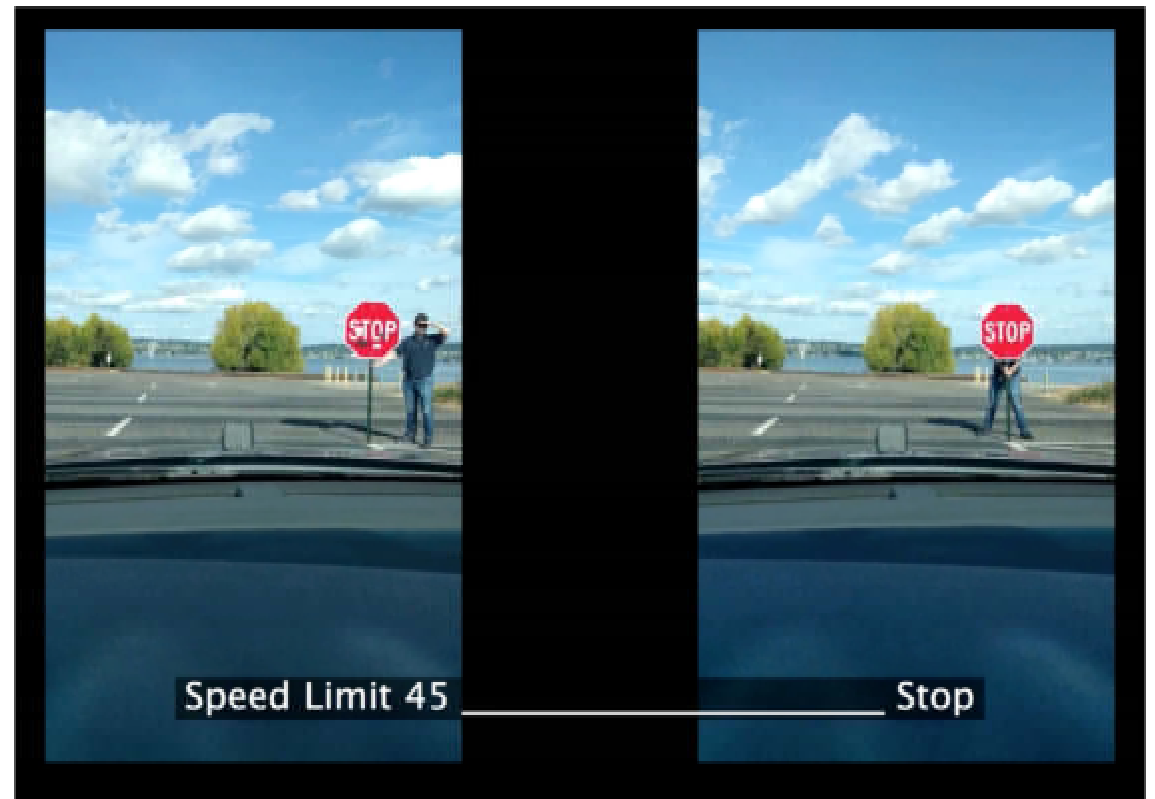
- March 2018
- Tesla Model S car accident
- Crashed in “Autopilot mode”
- Obstacle detection system



*<https://www.nytimes.com/interactive/2016/07/01/business/inside-tesla-accident.html>*, [Video](#)

# Autonomous Car Security

*“Can real physical objects be manipulated in ways that cause DNN-based classifiers to misclassify them?”*



*“Robust Physical-World Attacks on Deep Learning Visual Classification”, [Video](#)*



# Autonomous Car Security

- Physical attacks on classifiers / object detectors
- A stop sign is detected only when the camera is very close to the sign
- Too late for the car to stop or react

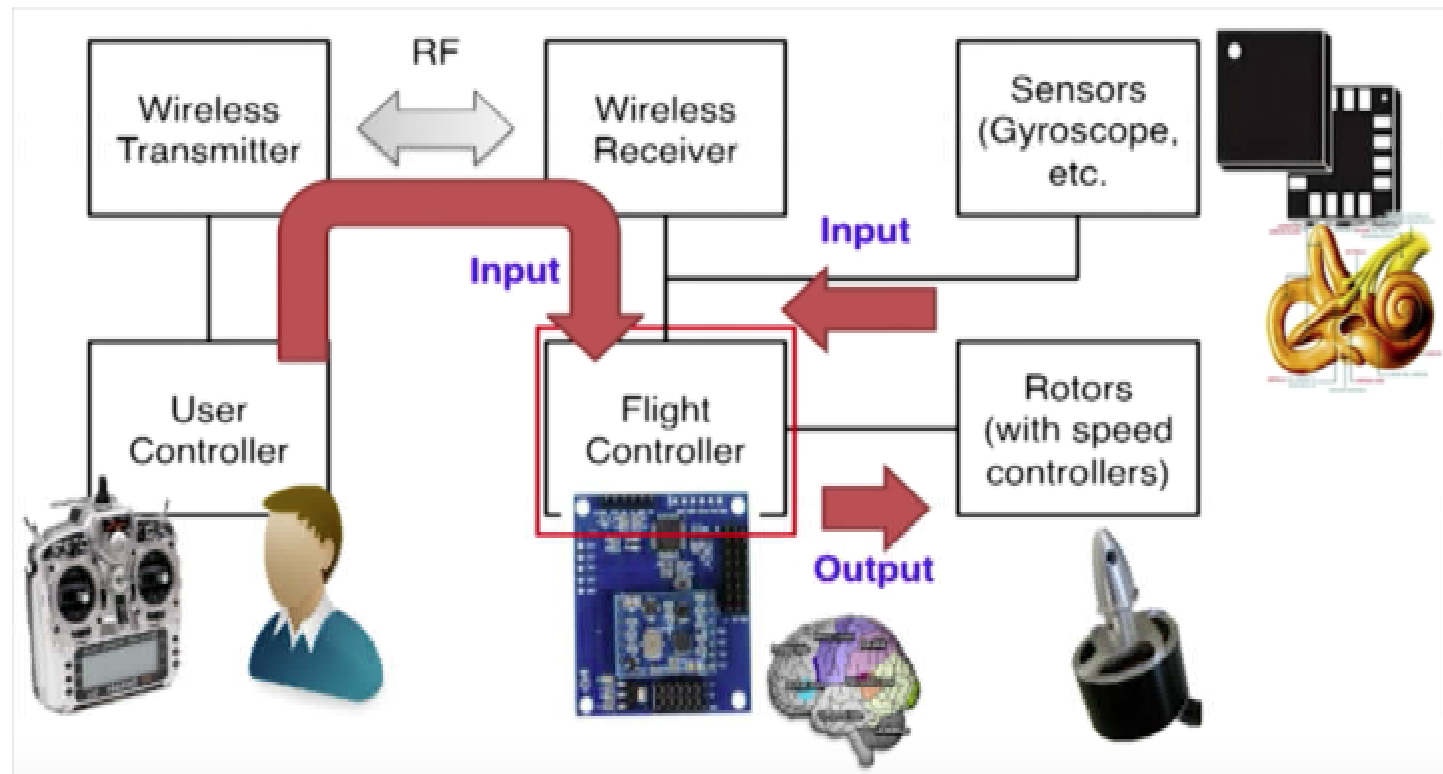


*"Physical Adversarial Examples for Object Detectors", [Video](#)*

# Drone Security

# Drone

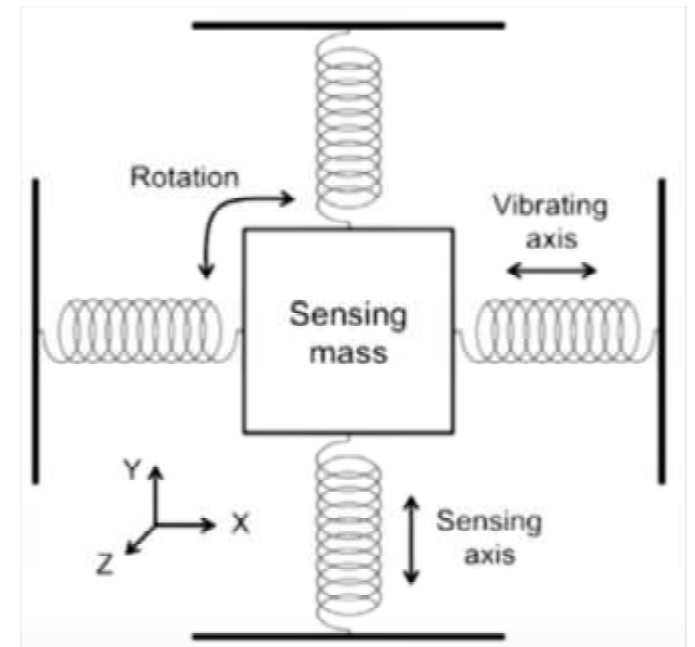
- 四軸飛行器



Yongdae Kim, "Hacking Sensors", USENIX Enigma 2017

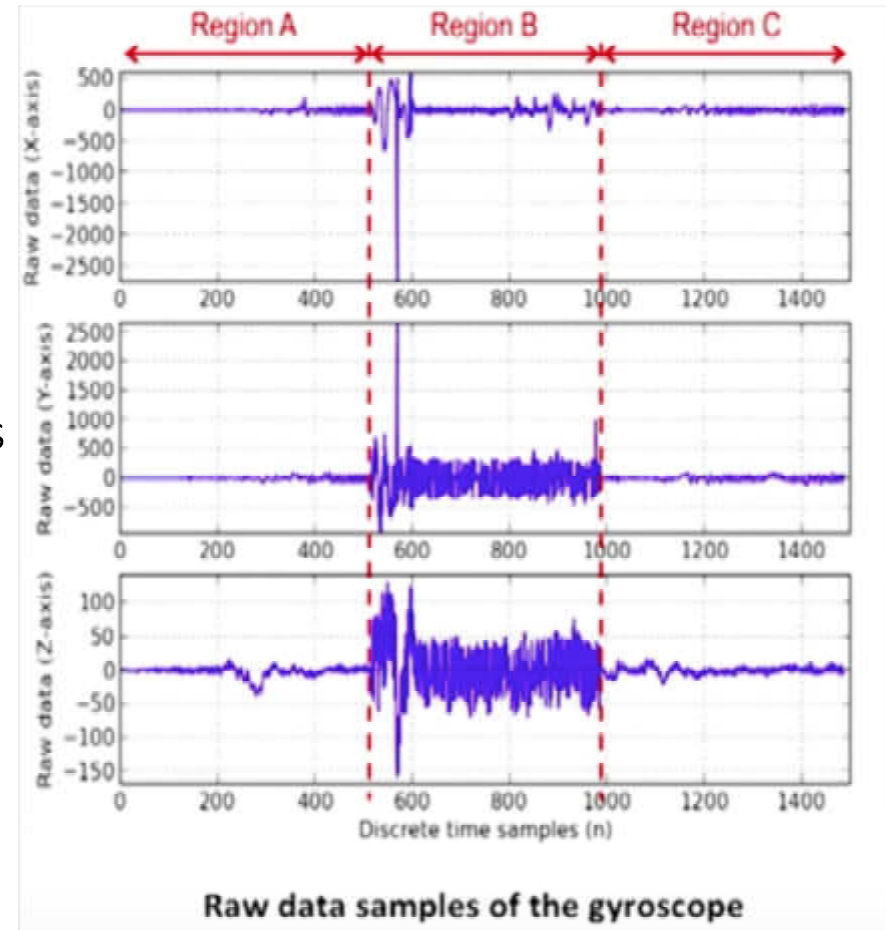
# Drone

- Inertial measurement unit (慣性測量單元)
  - Measures velocity, orientation, rotation
  - A combination of MEMS (微機電系統) gyroscope (陀螺儀), accelerometer (加速計)



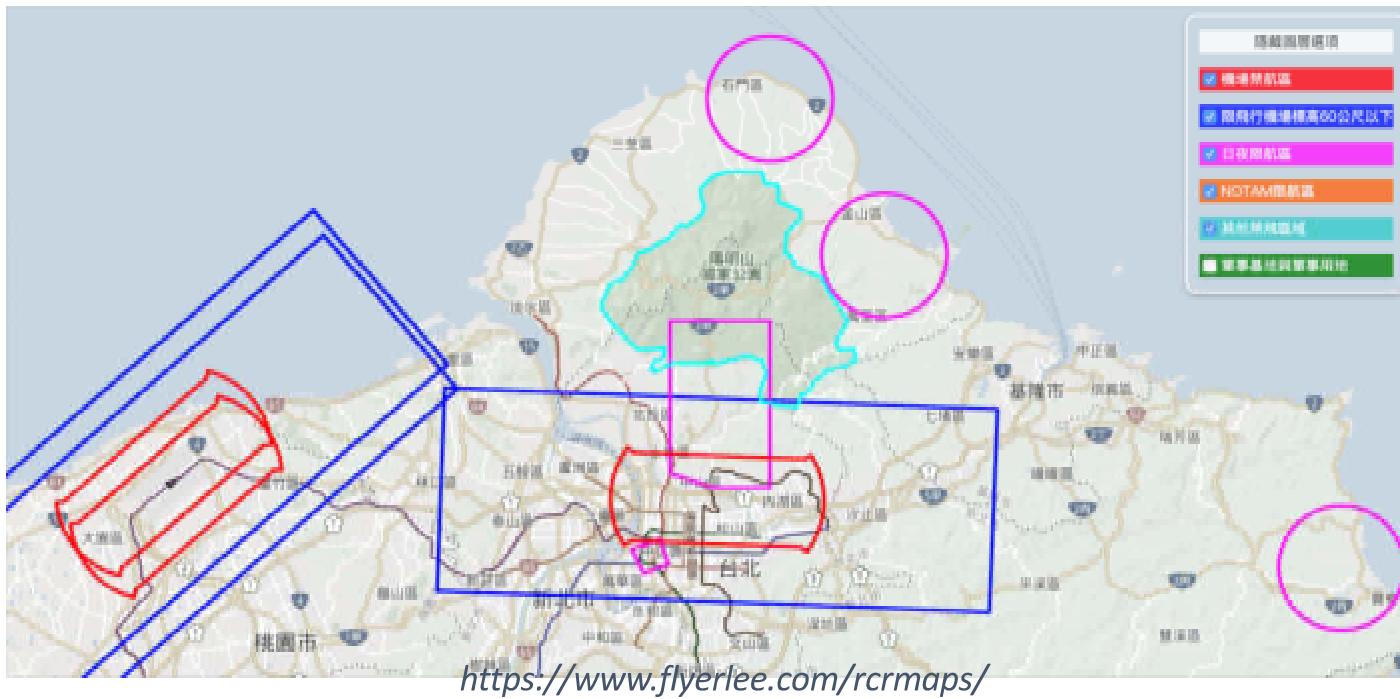
# Drone Security Issues

- Drone Hacking
  - Shutdown Attack
  - Find resonant frequencies (共振頻率) of MEMS / gyroscopes
  - Produce noises to interfere controlling units
  - [Demo](#) (13:25)



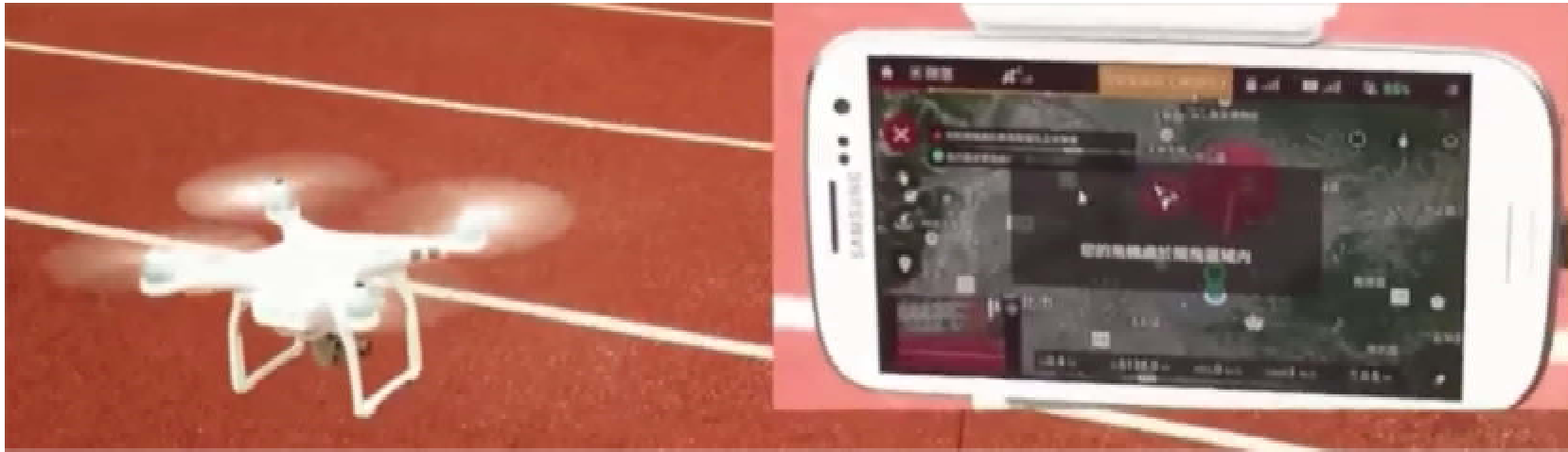
# Drone Security Issues

- Prohibited or restricted Airspace
  - Geofencing



# Drone Security Issues

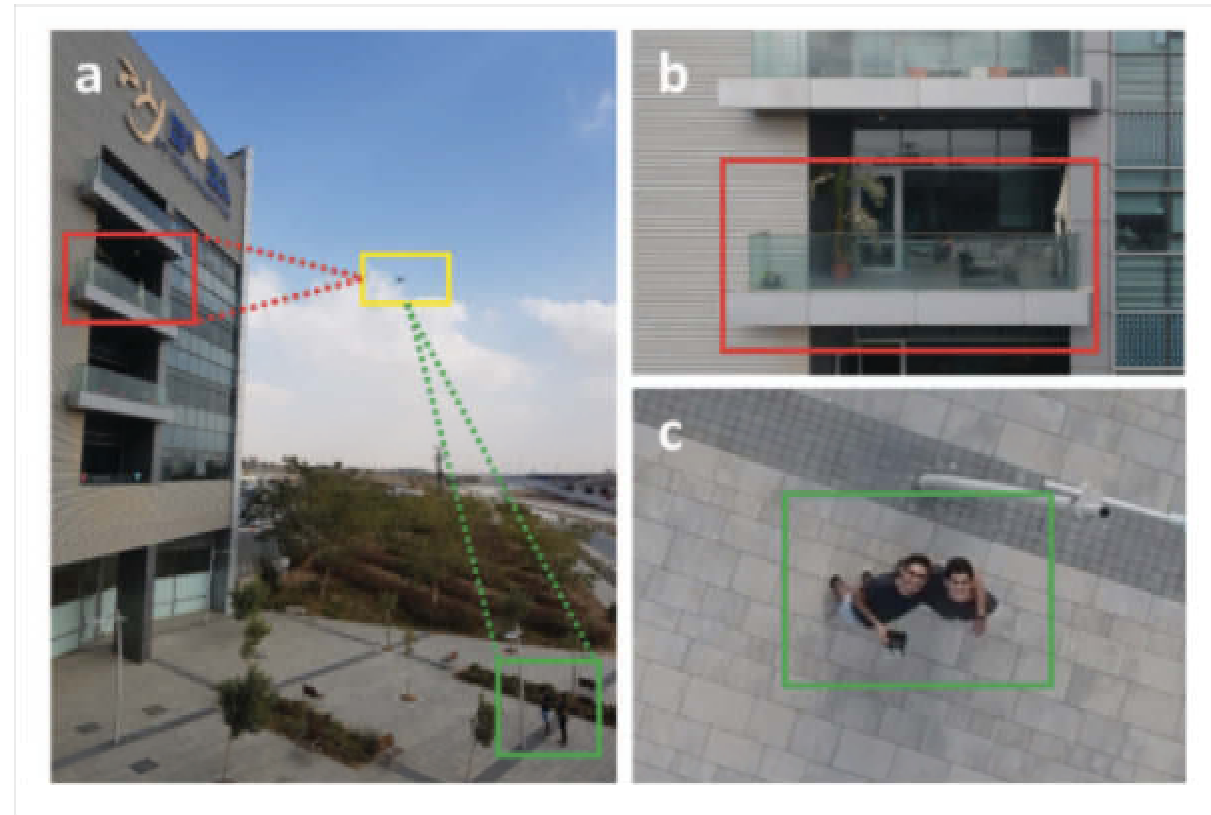
- Drone Hijacking
  - Reverse engineering the controlling app
  - Sending fake GPS signals to force the drone to land



*“Drones Hijacking: Multidimensional attack vectors and countermeasures”, DEFCON 24, [Demo](#)*

# Drone Security Issues

- “Open skies” problem
  - Drones fly in populated/urban areas
  - *“Is it delivering packages or spying on us?”*
- Detecting whether the camera is facing the victim
  - <https://youtu.be/4icQwducz68>
  - <https://youtu.be/9PVaDpMsyQE>
  - How good is this defense?





# Voice-controlled Device Security

Acknowledgement: many slides taken from Prof. Yuan Tien

# Voice Controlled Device (VCD)

- Voice Interaction
- Providing Real time information
- Play Music
- Communicate with other smart devices



# Attacks on VCD



"A guide to the security of voice-activated smart speakers," Symantec

# Attacks on VCD



“A guide to the security of voice-activated smart speakers,” Symantec

# Attacks on VCD



“A guide to the security of voice-activated smart speakers,” Symantec

# Attacks on VCD

## Hidden Voice Commands



“Okay Google take a picture”



Text

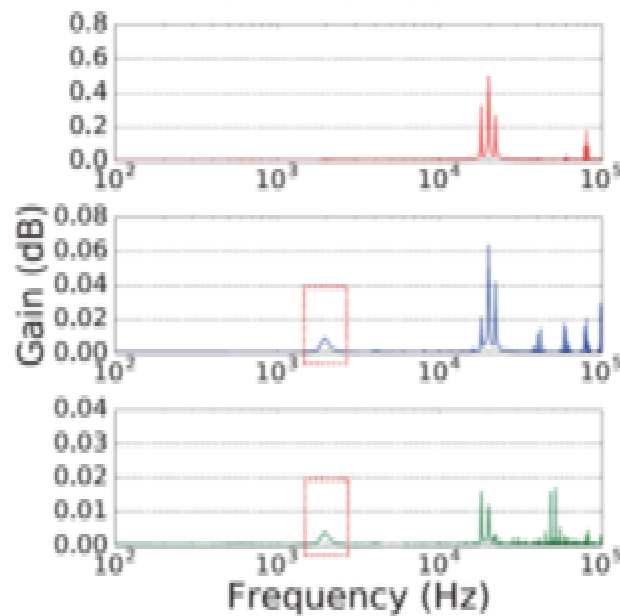
Attack



Text

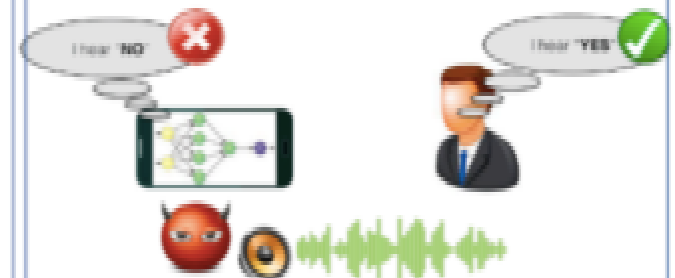
Ref: Carlini et. al. Usenix Security 2016

## Inaudible Voice Commands



Ref: Dolphin Attack CCS 2017, Backdoor MobiSys 2017

## Adversarial Voice Commands

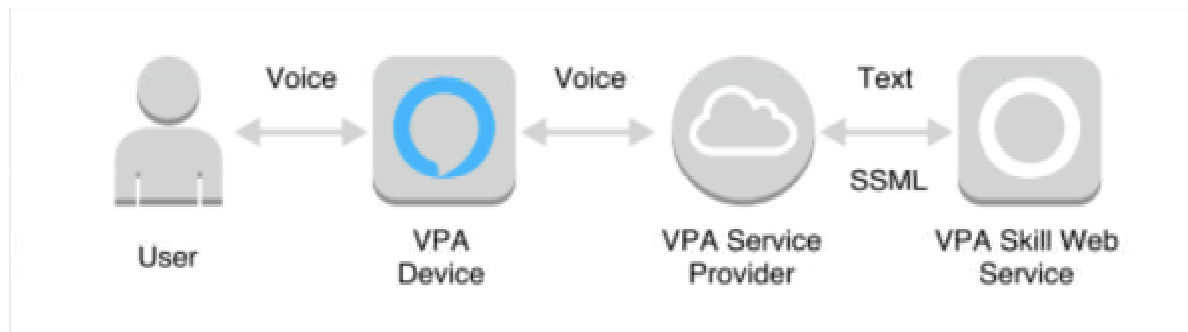


Ref: Alzantot et al. arXiv, 2017  
<https://git.io/vFs42>

Embed voice commands into a song: <https://sites.google.com/view/commandersong/>

# Attacks on VCD – Rouge Skills

- Skills
  - Similar to mobile app
  - Third party application that leverage Alexa voice services
  - Interacts with human voice
  - Currently, 30000 skills are active in amazon website





## Fish Geek

Matt Mitchell

*"Alexa ask Fish Geek to tell me a fact"*

*"Alexa ask Fish Geek to tell me trivia"*



## Phish Geek

EP

*"Alexa, open Phish Geek"*

*"Alexa, launch Phish Geek and tell me a fact"*



# Hijack by confusion

## Predictable Errors

Word	Prediction
Sail	Sale
Rip	Rap
Outshine	Outshyne
Lung	Lang
Accelerate	Xcelerate
Mill	No
Preferably	Preferrably
Earthy	Fi
Calm	Com
Coal	Call
Outdoors	Out Doors
Loud	Louder

Word	Prediction
Superhighway	Super Highway
Wet	What
Main	Maine
Boil	Boyle
Sell	Cell
Full	Four
Dime	Time
Bean	Been
Dull	Doll
Sweeten	Sweden
Luck	Lock
Con	Khan

# Hijack by confusion

- 66 different Alexa skills are called *cat facts*, 5 called *cat fact* and 11 whose invocation names contain the string “*cat fact*”, e.g. *fun cat facts*, *funny cat facts*.
  - “*Tell me funny cat facts*” will trigger *funny cat facts* rather than *cat facts*.
    - Longest string match
- The adversary who aims at *Capital One* could
  - register a skill *Capital Won*, *Capitol One*, or *Captain One*
  - register *Capital One Please*

Demo: <https://sites.google.com/site/voicevpasec/>

# Voice Squatting

Voice assistants may fail to understand user's intention, and **mistakenly invoke wrong skills**



“Dangerous Skills : Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems,” *IEEE S&P*, 2019.

# Voice Masquerading

Skill switching is not well supported, allowing a skill to masquerade itself as other skills or even the system

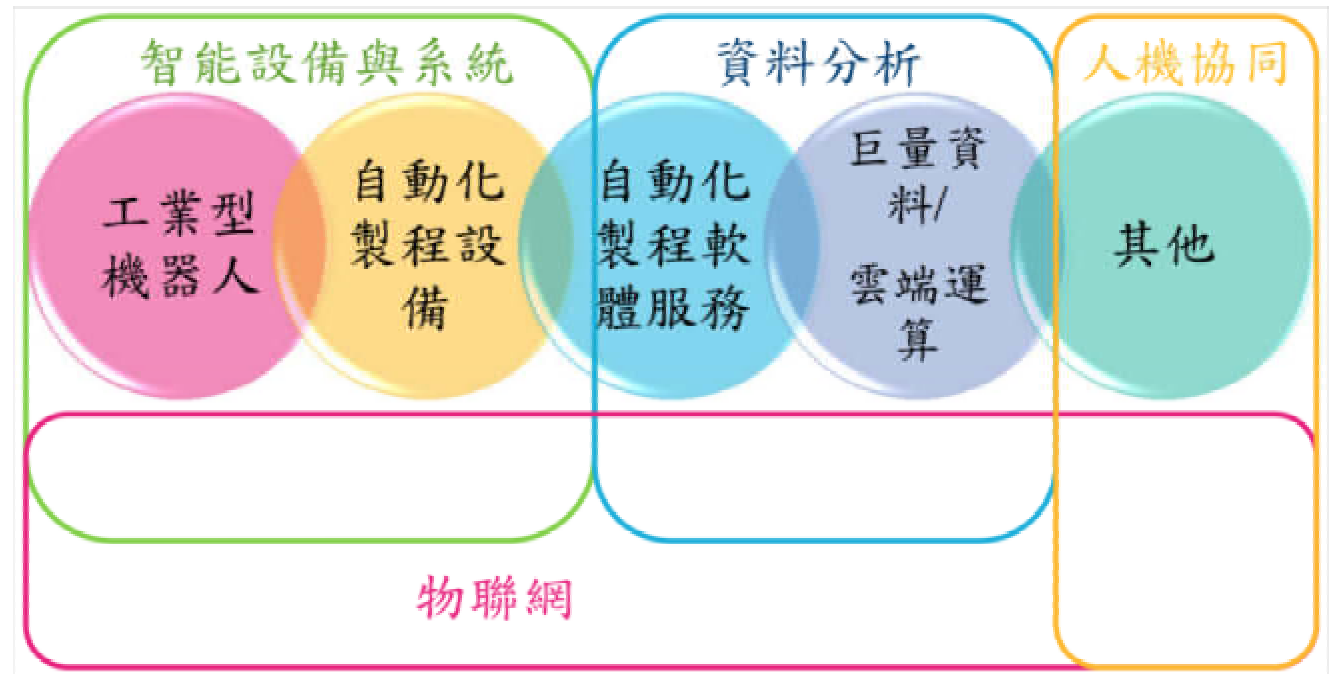


"Dangerous Skills : Understanding and Mitigating Security Risks of Voice-Controlled Third-Party Functions on Virtual Personal Assistant Systems," *IEEE S&P*, 2019.

# Smart Factory Security

# Industry 4.0

- CPS & IoT
- 感知意識
- 高度自動化
- 需求客製化
- 供應端優化



# Smart Factory

- What is “*Smart Factory*” ?
  - *“An environment where machinery and equipment are able to improve processes through automation and self-optimization”*
- Why “*smart*” ?
  - Collect data during production
  - Analyze data & make decisions
  - Able to communicate & cooperate with others

# Smart Factory

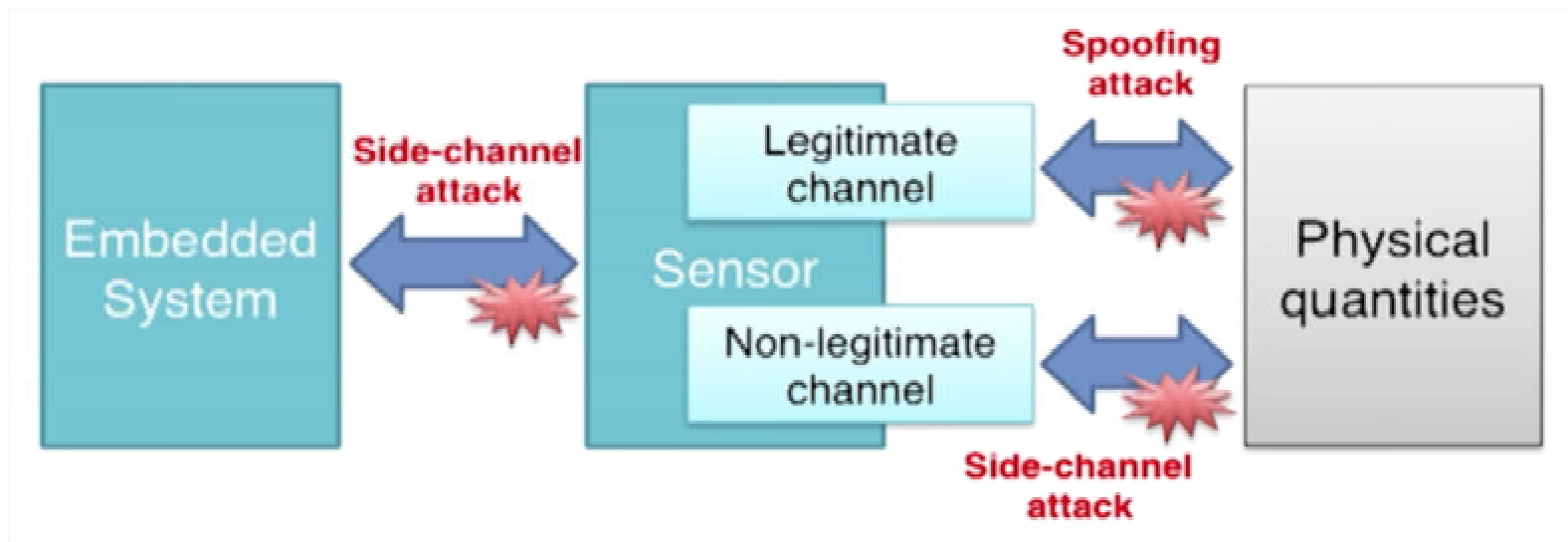
- Cyber-Physical System (CPS)
  - *“Integrations of computation, networking, and physical processes”*
- How does it work?
  - Sense data → Collect & Analyze → Make decisions → Execute commands → Feedback
- Example
  - MIT Distributed Robotic Garden
  - An autonomous greenhouse based on autonomous robots and sensors





# Smart Factory - Security Issues

- Sensing-and-actuation systems
  - Sensors measure inputs & transfer outputs to system
  - Systems decide their actuations according to sensor outputs
- What if sensor inputs are forged?



Yongdae Kim, "Hacking Sensors", USENIX Enigma 2017

# Smart Factory - Security Issues

- Hacking sensors
  - Heart-rate sensor spoofing [Demo](#) (4:08)



Yongdae Kim, "Hacking Sensors", USENIX Enigma 2017

# Smart Factory - Security Issues

- Possible threats
  - Eavesdrop / manipulate transferred data
  - Unauthorized access
  - ...
- How to improve security?
  - Encrypted communication
  - Intrusion detection
  - DDoS defense
  - ...

# Conclusion

- Different IoT applications face different security & privacy issues
- Need to work with area experts to discover potential risks
- How can we get ahead in this cyber arms race?