Addressing Security and Privacy Challenges in Internet of Things

Arsalan Mosenia
Postdoctoral Researcher

Internet of Things

Enabling numerous services over the Internet

Interconnection of heterogenous entities

Over 50B Internet-connected devices by 2020

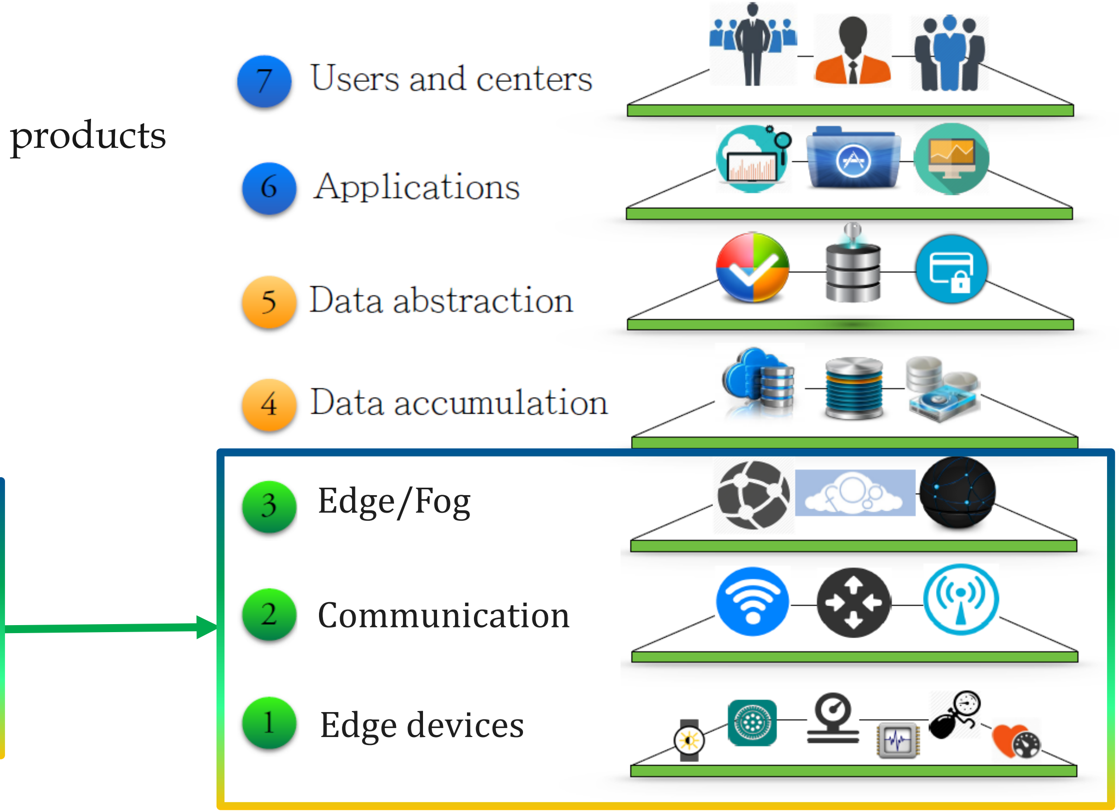
Challenges & Research Directions

Architectures	Data Analytics	Efficiency	Security
❖ New architectures ❖ Fog/Edge Computing ❖ Unused devices	❖ Huge amount of data ❖ Heterogeneity ❖ Missing records	❖ Real-time processing ❖ Small battery ❖ Small storage	❖ Security attacks ❖ Information leakage ❖ Security-friendly design

Security Challenges

Security and privacy

- ❑ Existence of insecure in-market products
- ❑ Lack of standardization
- ❑ Resource constraints
- ❑ Unknown threats
- ❑ ….



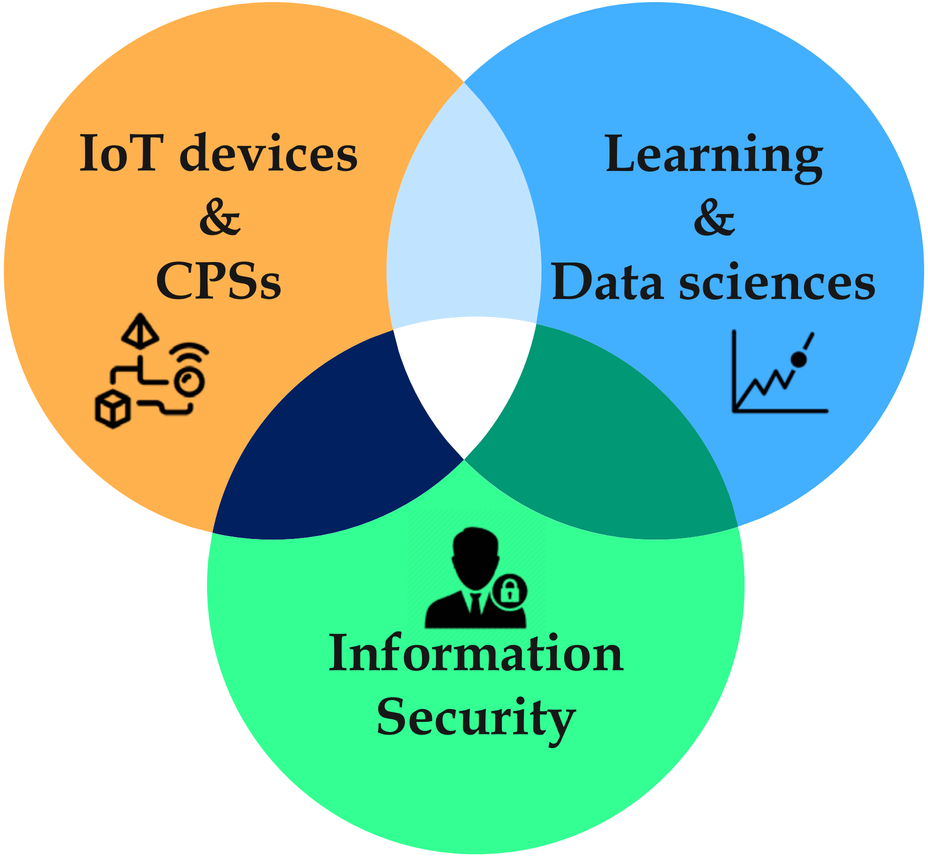
Potential Attackers

Attackers:
- ❖ Occasional hackers
- ❖ Cybercriminals
- ❖ Government

Attackers' Motivations:
- ❖ Controlling devices
- ❖ Stealing ***sensitive*** information

IoT-based systems:
- ❖ Huge amount of information
- ❖ Monitoring/automation

Research Themes



Research Themes

IoT & CPS Security

Uncovering Security/Privacy Flaws

Information Leakage
[IEEE TETC, **2016**]
[IEEE TMSCS, **2017**]

Security Vulnerabilities
[IEEE TETC, **2017**]
[ATC USENIX, **2018**]

[Survey, IEEE TMSCS, **2017**]

Development of Security-friendly Systems

Wearables & Implants
[IEEE TMSCS, **2015**]
[IEEE TC, **2017**]
[IEEE TMSCS, **2017**]
[IEEE TMSCS, **2017**]

Smart Vehicles
[UbiComp, **2018**]
[UbiComp, **2018**]

Underlying Networks
[USENIX Sec, **2018**]
[FWC, **2018**]

[Survey, ACM EDA, **2017**]

OpenFog Consortium

Founders

Princeton University, Intel, Cisco, Microsoft, arm, Dell

Contributing Members

Foxconn, Hitachi, GE, Sakura Internet, ZTE, ShanghaiTech University

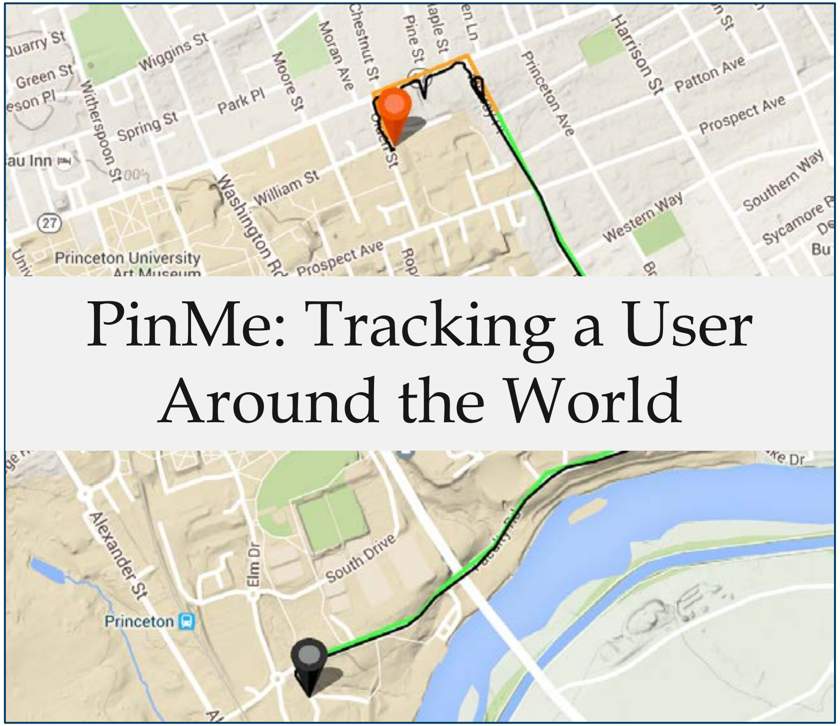
Affiliations

Barcelona Supercomputing Center, ETSI, IEEE ComSoc, IoT Acceleration Consortium

We define security standards for Fog/Edge Computing
[2 position papers, Fog World Congress, 2017]

61 members strong, headquartered in 17 countries as of January 2018

Outline



PinMe: Tracking a User Around the World

ProCMotive: Bringing Programmability and Connectivity to Vehicles

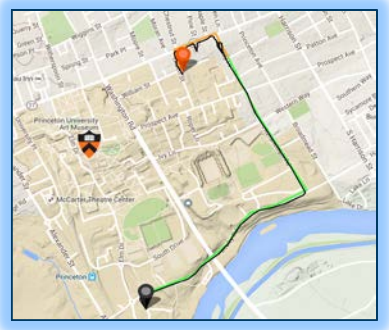
IoT & CPS Security

Uncovering Security/Privacy Flaws

- Information Leakage
- Security Vulnerabilities

Development of Security-friendly Systems

- Wearables & Implants
- Smart Vehicles
- Underlying Networks



Location Privacy

Attacks against location privacy lead to:

- ❖ advertisement, spams, or scams
- ❖ disclosure of personal activities
- ❖ …

Location privacy: determining ***when, how, and to what extent*** location data are shared

Prior Attacks on Location Privacy

Fundamental limitations of previous attacks:

- ❖ Substantial prior knowledge of the path
- ❖ An attack-specific training dataset
- ❖ Very limited accuracy, e.g., less than 45%

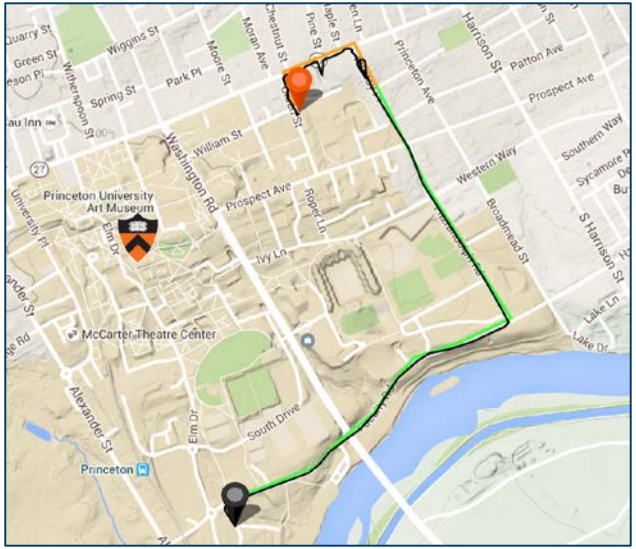
PowerSpy (GPS is **<u>off</u>**)
[Michalevsky et al.]

The extent of location-related information that can be inferred from ***<u>presumably non-critical</u>*** data was ***<u>not</u>*** well-understood!

Fundamental Challenges

A realistic privacy attack:

- ❖ Minimal prior knowledge
- ❖ No attack-specific training dataset
- ❖ High accuracy
- ❖ Different activities
- ❖ Robustness

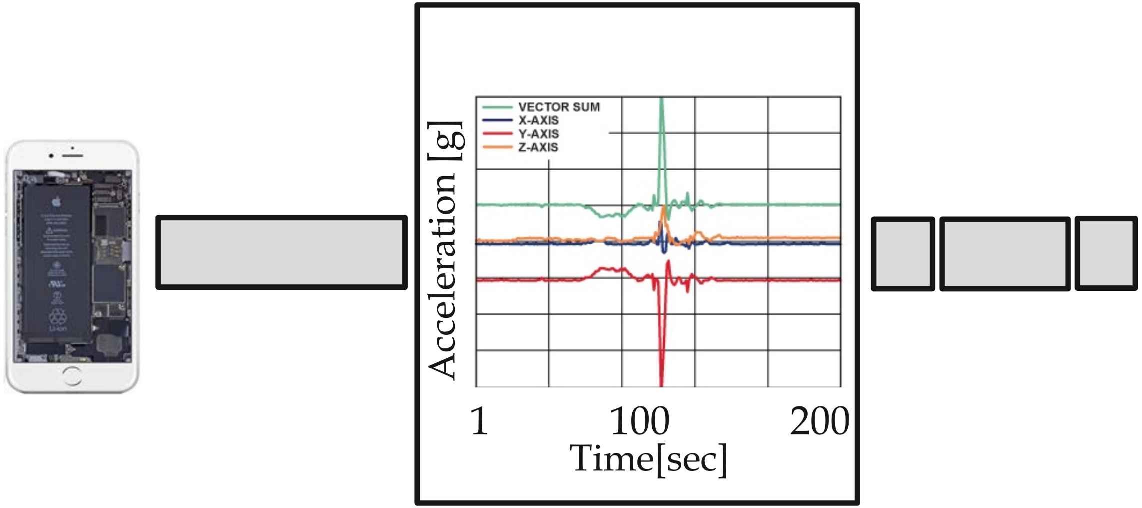


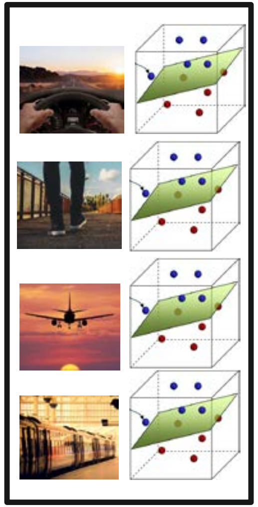
PinMe may offer a promising navigation system for autonomous vehicles

Sources of Information

Permission-free data

Step 1: Dynamic Partitioning & Activity Classification





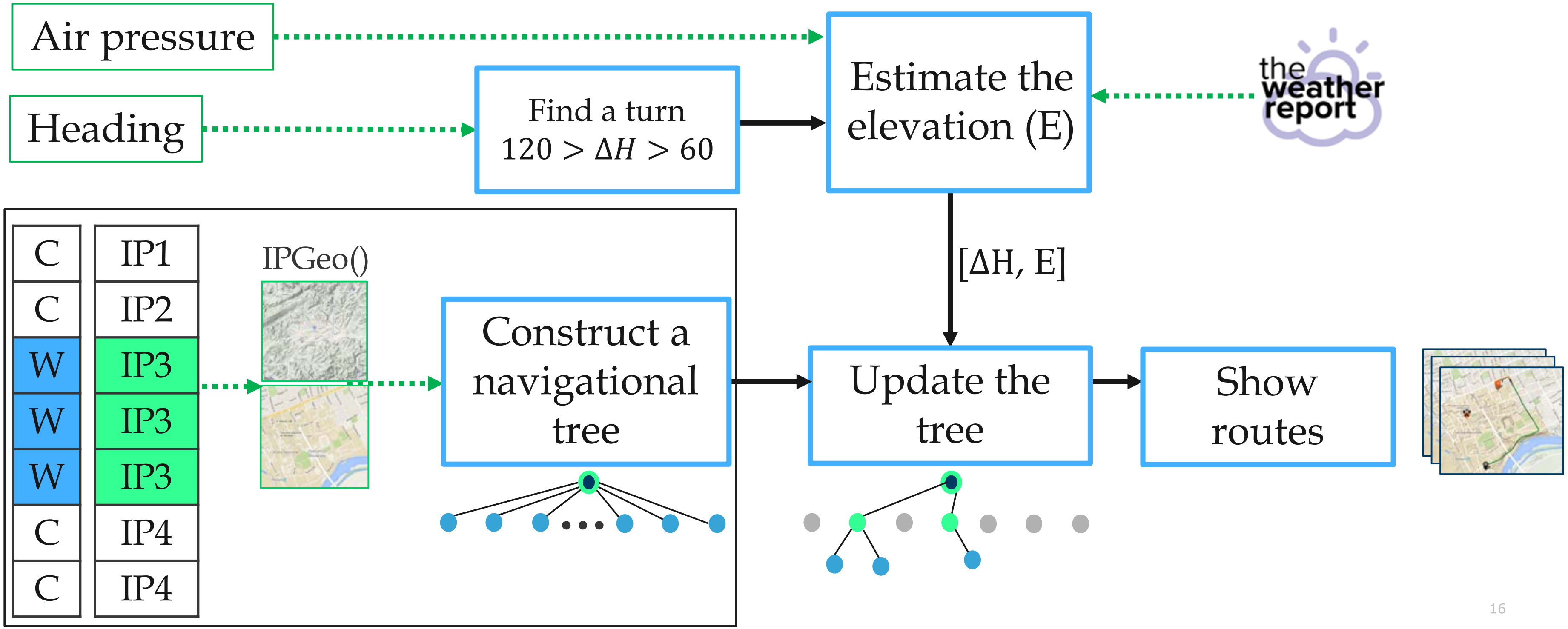
What if the user shakes the phone? **Merging**

Activity classification (4 SVMs):

- ❑ Air pressure
- ❑ Acceleration
- ❑ Heading (compass)

Step 2: Tracking the Vehicle

$$E_{turn} = E_{Station} + \frac{T}{C}\ln\left(\frac{P_{turn}}{P_{Station}}\right)$$

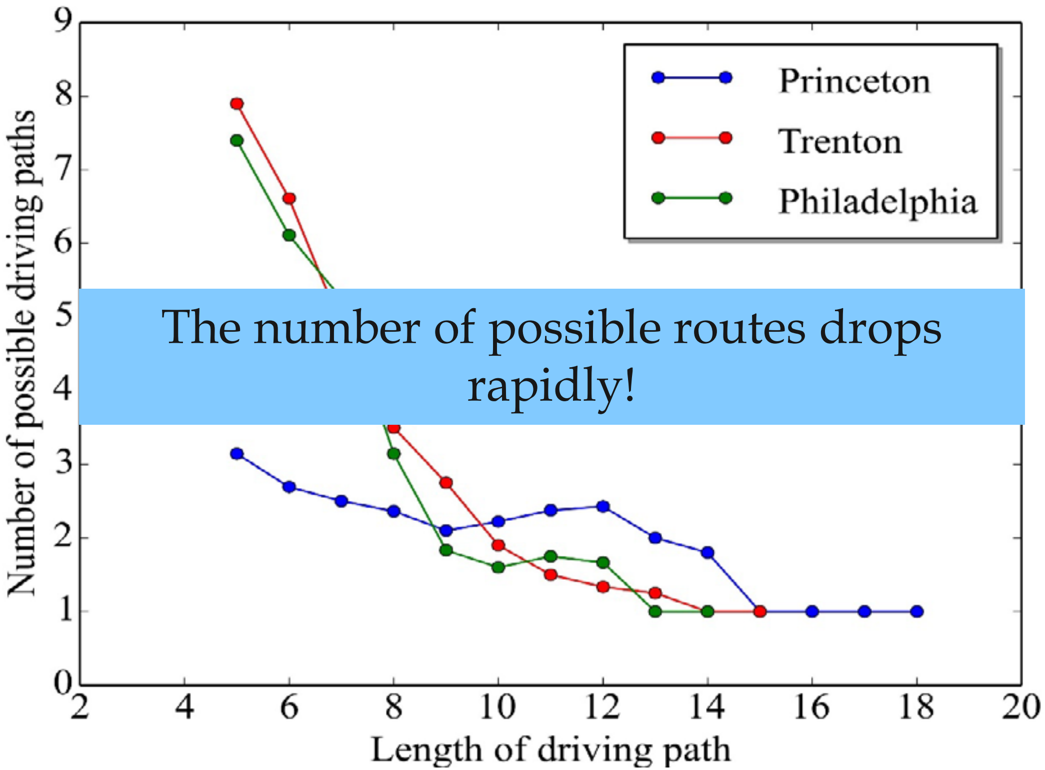


Real-world Evaluation

1. Three smartphone: Galaxy S4 i9500, iPhone 6S, and iPhone 6
2. Two datasets:
   - ❖ Set #1: **405 data chunks** collected during different activities **(271 chunks for driving)**
   - ❖ Set #2: **3 data streams** collected by **3 users (Mazda 3, Mazda CX7, Toyota Camry)**

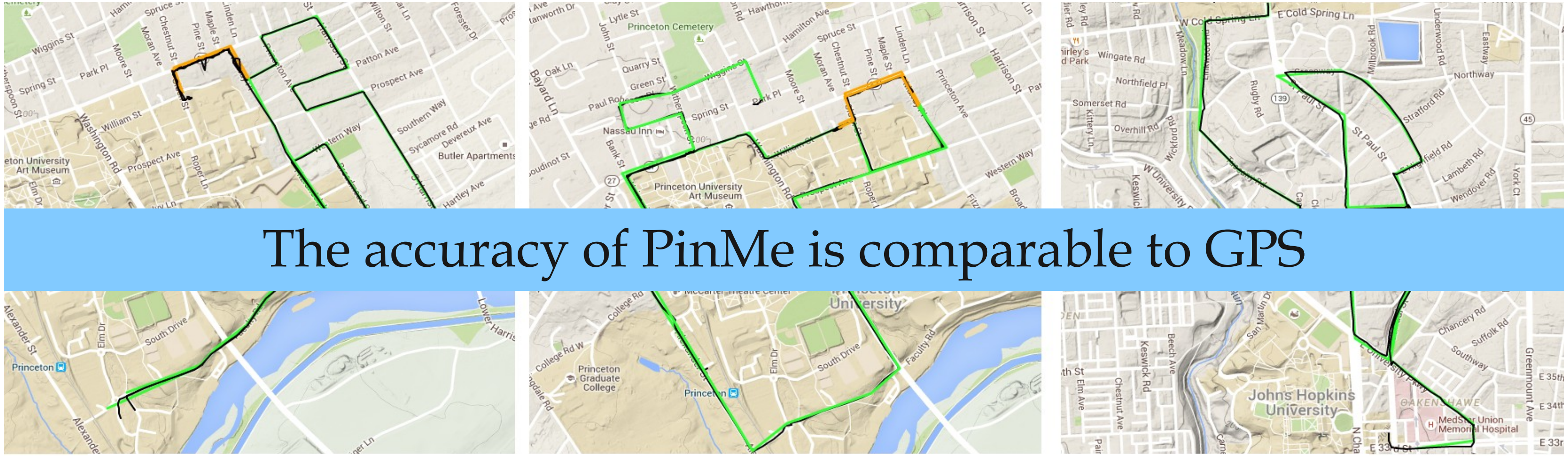


Results: Tracking the Vehicle



The number of possible routes drops rapidly!

Results: End-to-end Evaluation



(a) (b) (c)

Trajectories of three different users. Starting from the left and moving to right: (a) Princeton [Galaxy S4 i9500], (b) Princeton [iPhone 6], and (c) Baltimore [iPhone 6S]

Comparison

Tracking mechanism	#Activity	Prior info.	Training	OS	Sampling freq.	Device/Vehicle dependence	Success Rate
ACComplice Han et. Al, 2012	1	Y	Y	Android iOS	30 Hz	Y	10%*
PowerSpy Michalevsky et al., 2015	1	Y	Y	Android	N/A	Y	45%
Narian et al., 2016	1	N	N	Android	20-100	Y	10%*
PinMe	**4**	N	N	Android iOS	**5 Hz**	**N**	**100%**

Summary and Future Work

PinMe:

- ❖ sheds light on information leakage from seemingly-benign data
- ❖ offers a promising alternative to GPS

We:

- ❖ are performing a large-scale study
- ❖ started conversations with companies

U.S. Patent Pending

The most popular paper of IEEE Trans. Multi-scale Computing Systems, Jan. 2018

Extensive media coverage (e.g., Schneier on Security & Android Authority)

IoT & CPS Security

Uncovering Security/Privacy Flaws

- Information Leakage
- Security Vulnerabilities

Development of Security-friendly Systems

- Wearables Implants
- Smart Vehicles
- Underlying networks

State-of-the-art Vehicles

Stats:

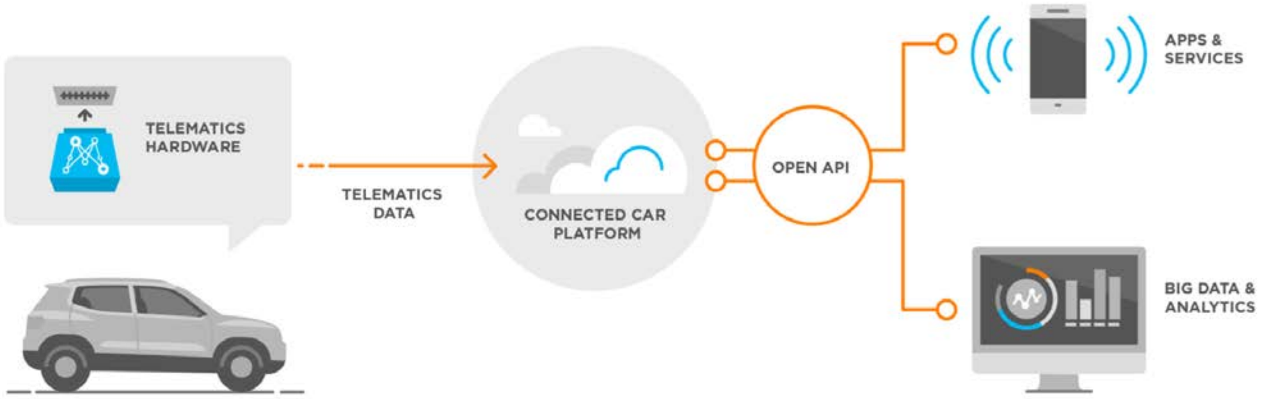
- Over 1B vehicles, 78M vehicles sold in 2017
- Average age of vehicles > 12 years
- Most of them *do not* support connectivity/programmability

Transmitters

Shortcomings:

1. Unavailability of service when wireless is lost
2. Lack of programmability
3. Significant cellular data usage
4. Intolerable response time
5. Security
6. Privacy

Product Recall



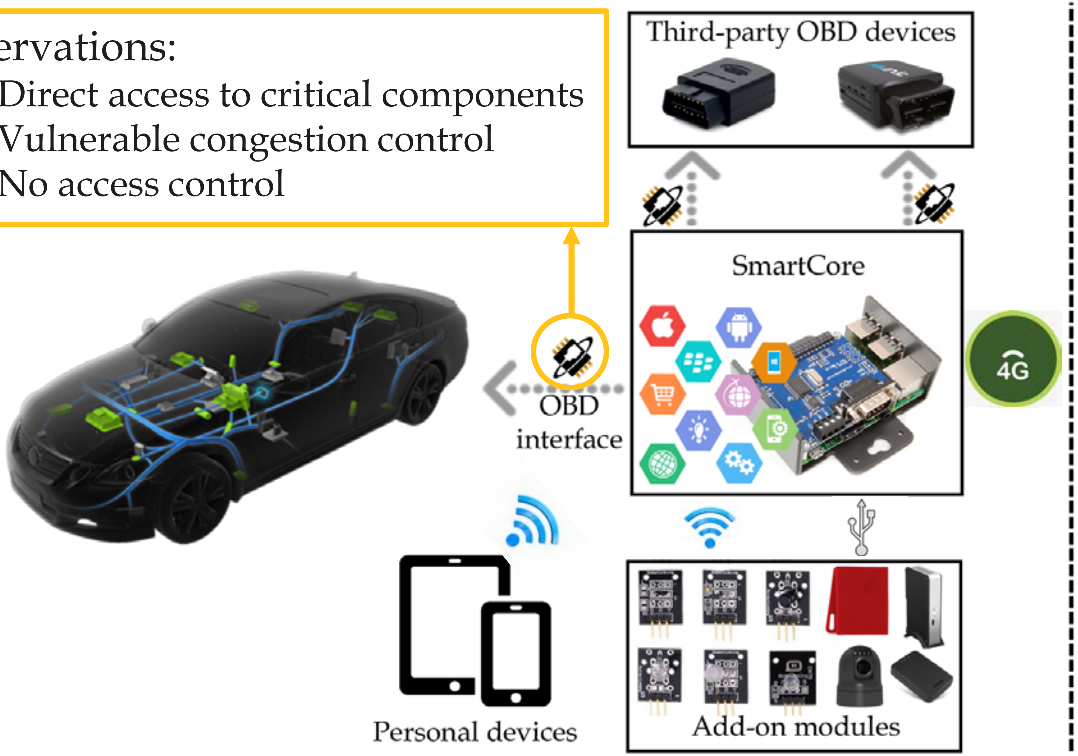
New Vehicular Apps

Enabling data-dominant, latency-sensitive, mission-critical, and privacy-sensitive applications

Architectural Overview

Key observations:

- Direct access to critical components
- Vulnerable congestion control
- No access control



Design Goals

Connectivity
Vehicle-to-Cloud
Vehicle-to-phone
Vehicle-to-Vehicle

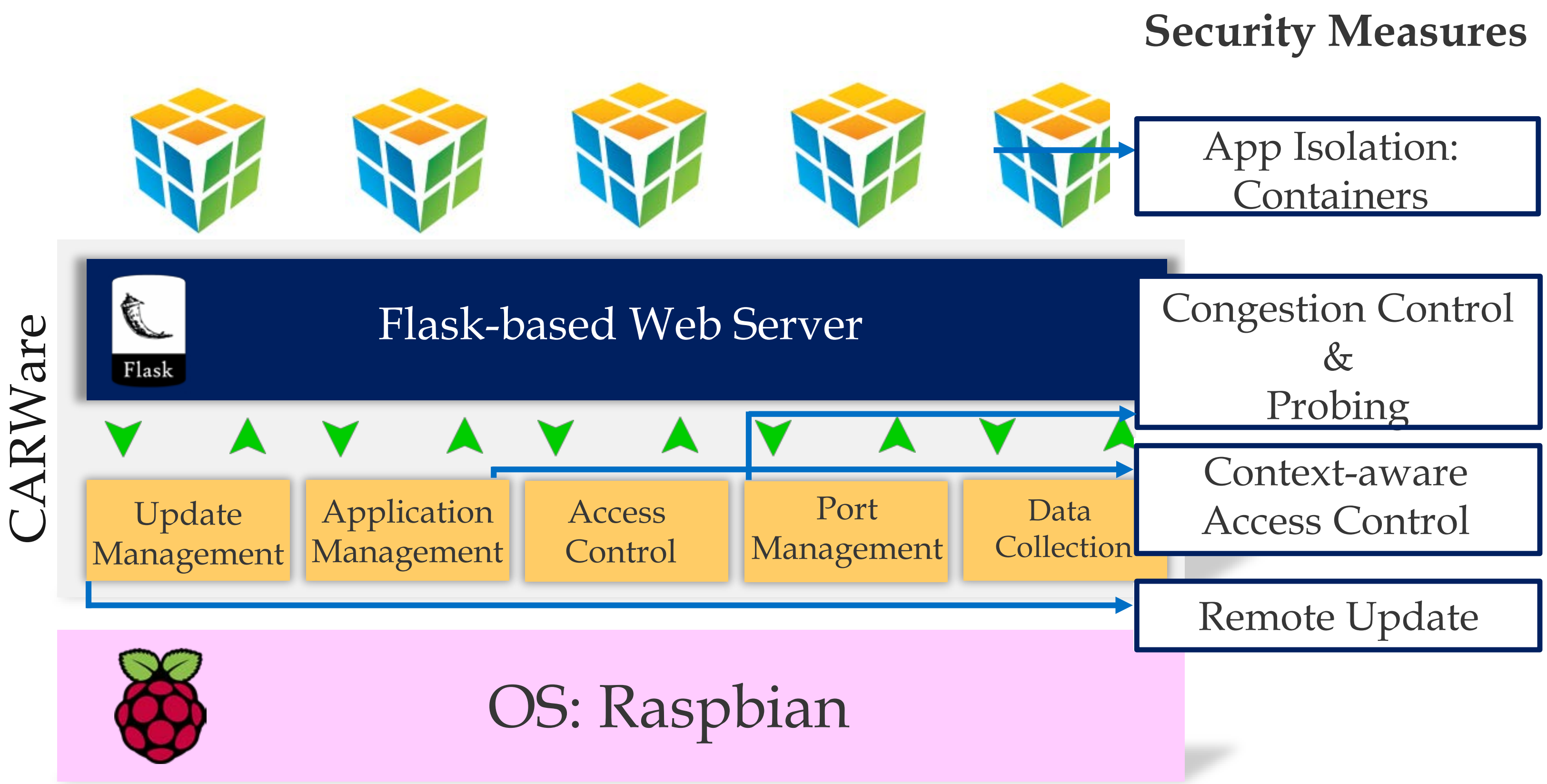
Security
Access control
Virtualization
(containers)

Privacy
Data manipulation
Minimal transmission

Programmability
Customized Apps
Low response time

Cost
Minimal transmission

Vehicular Add-on Middleware

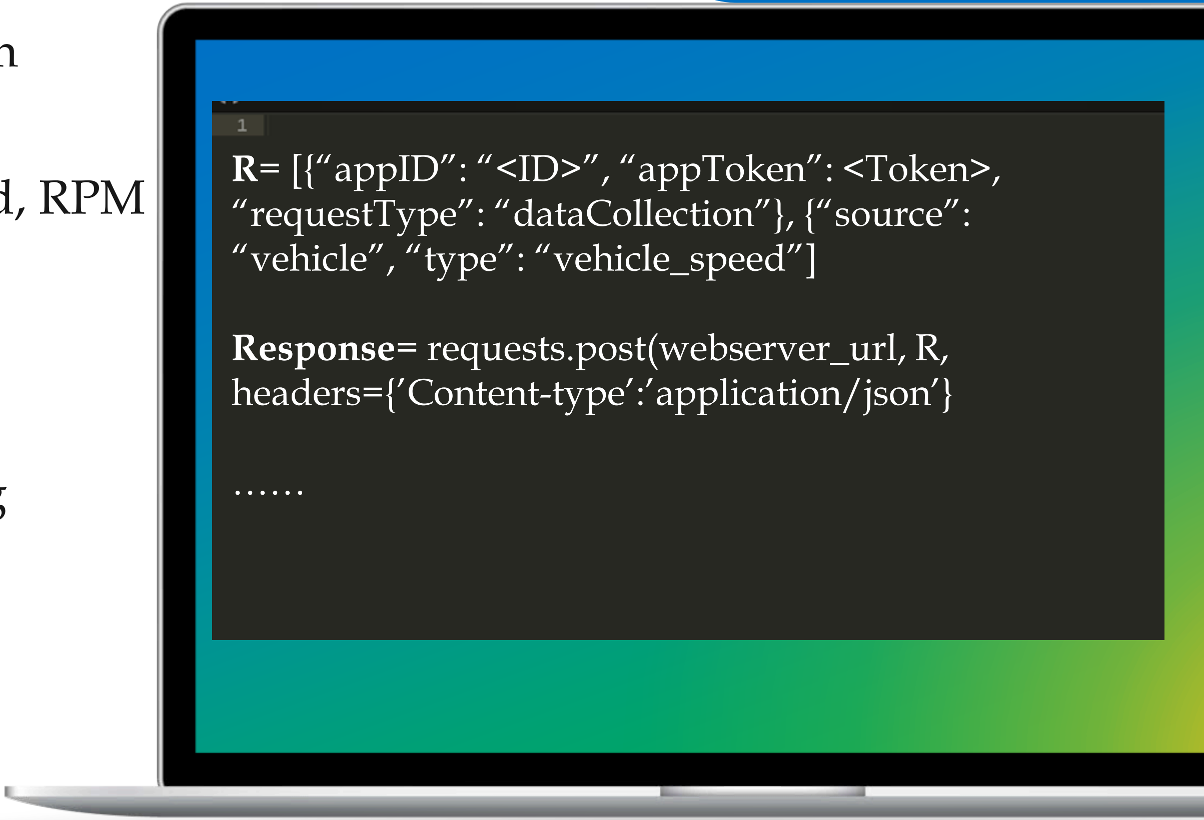


Data Collection

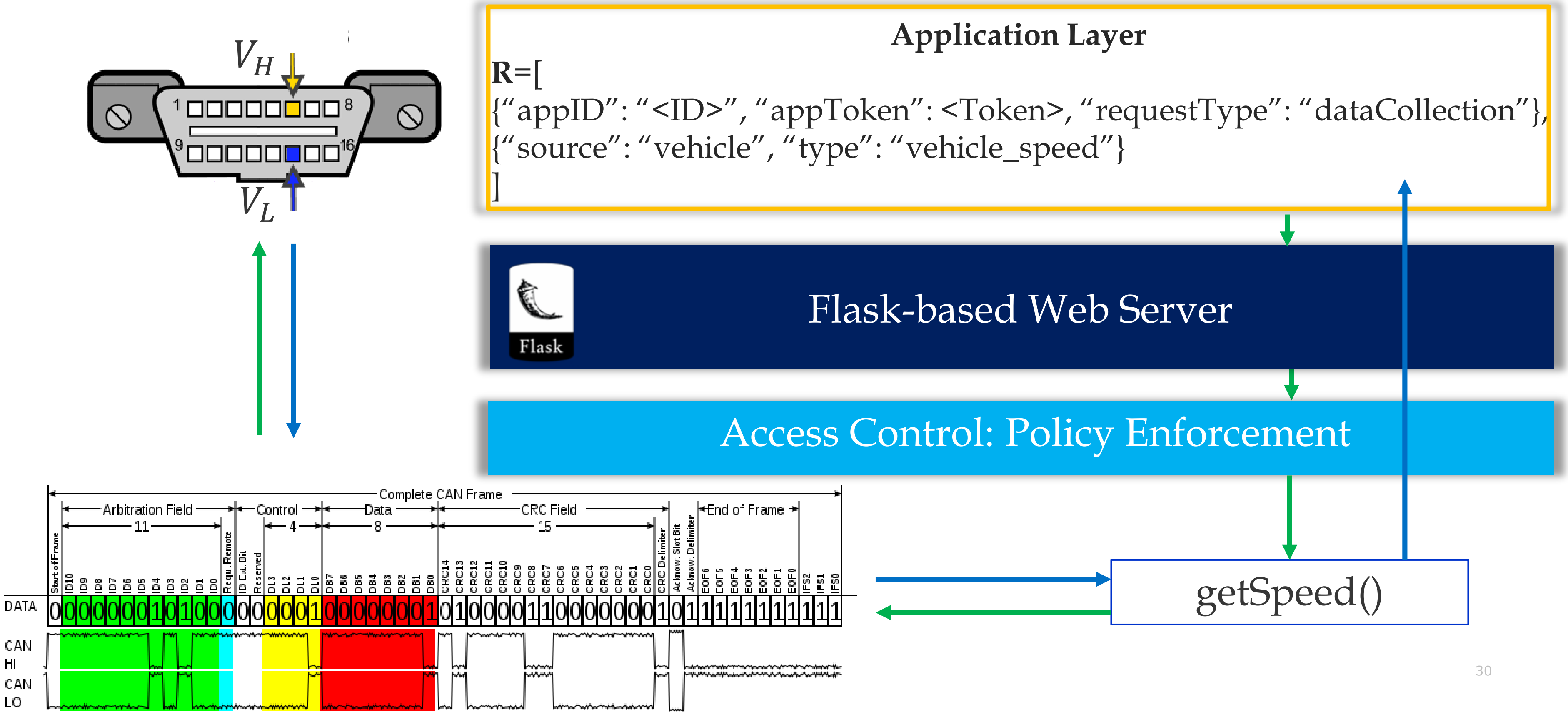
App Development

Enabling data collection from

- ❖ Built-in sensors
  - 20-40 sensors, e.g., speed, RPM
- ❖ Add-on modules:
  - ❑ GPS receiver
  - ❑ Camera
  - ❑ BLE-based Sensor Tag



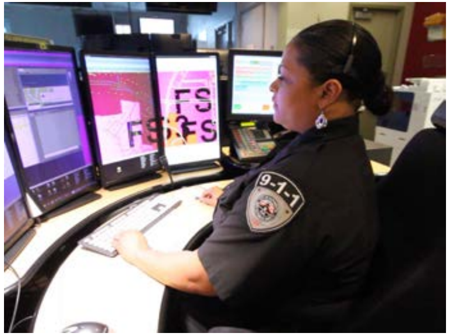
Data Collection (Cont.)



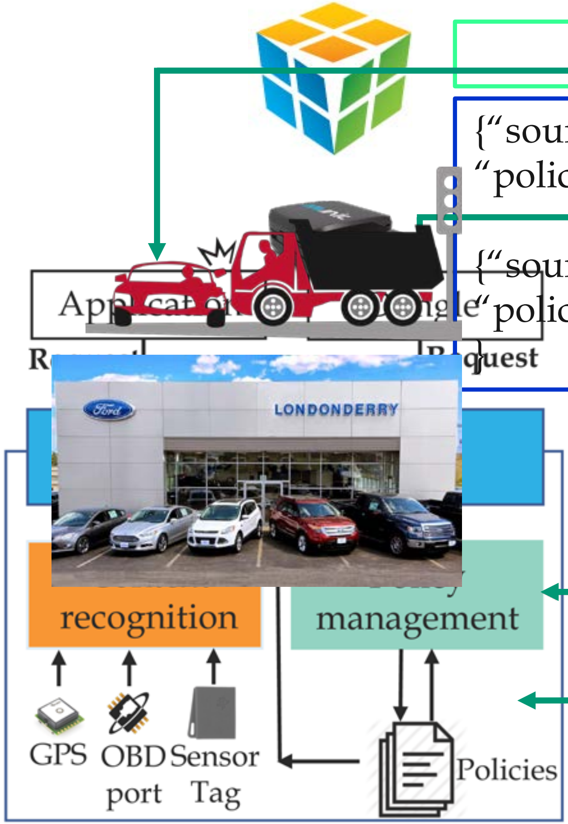
Access Control

Policy types:

- ❖ Strict
- ❖ Context-aware (over 10 contexts)
    1. Location-based
    2. Operational (e.g., idle/moving)
        - ❑ Example: Only send controlling commands when the vehicles is not moving!
    3. Situational (e.g., accident)



Access Control (Cont.)



Policy File

{“source”: “vehicle”, “type”: “vehicle_speed”,
“policyType”: “strict”, “access”: “always” }

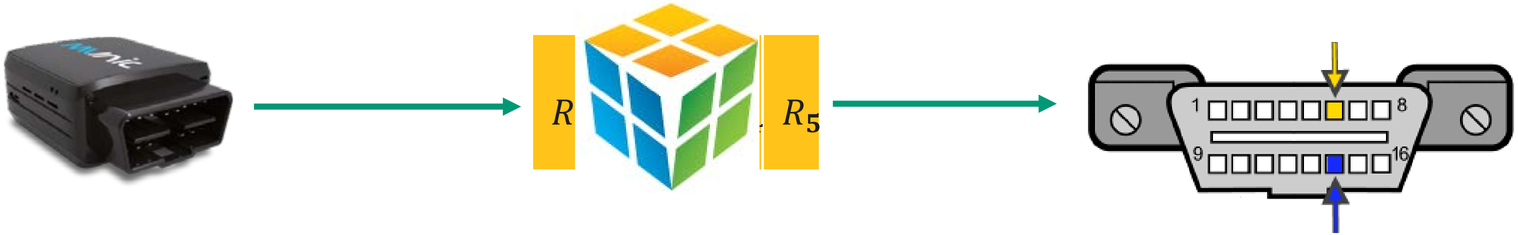
{“source”: “GPS”, “type”: “location”,
“policyType”: “situational”, “situation”: “accident”
}

API

Port Management

Public functions:

- **Dongle isolation**
- **Congestion control (rate adjustment)**
- **Probing**

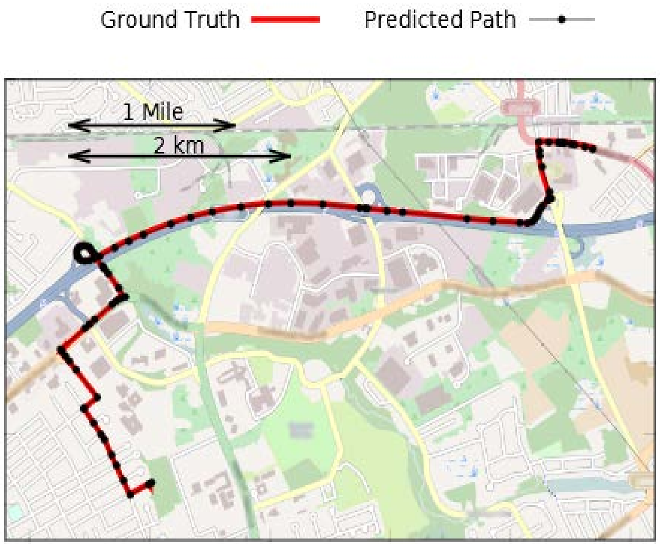


Case Study I: Insurance Monitor

Usage-based insurance plans offer very low rates!

However, their acceptance is limited:

- ❖ Security
  - ❑ Injecting commands [Savage et al.,2015]
  - ❑ Denial-of-service attacks
- ❖ Privacy
  - ❑ Reading the vehicle's private data
  - ❑ Tracking the vehicle [Gao et al., 2014]



Case Study I: Insurance Monitor

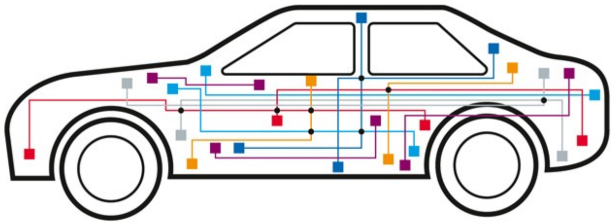
Security:

- ❖ Access control
  - ❑ Dongle can only **read** speed
- ❖ Port management
  - ❑ Behavioral analysis
    - ▪ Statistical analysis
    - ▪ Learning the profile

Privacy:

- ❖ Port management
  - ❑ Data manipulation

    Example: Noise addition



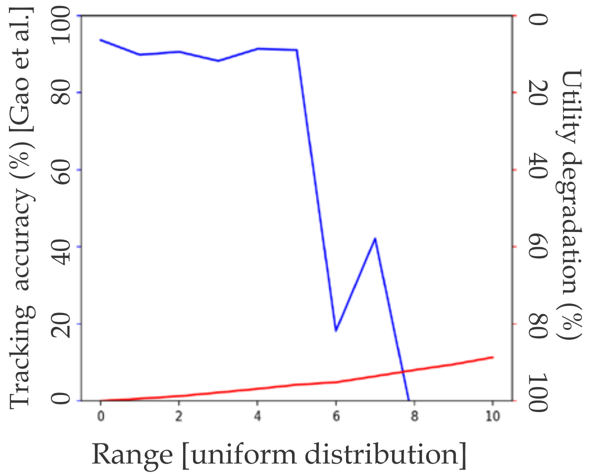
Results: Prevention of Command Injection

- Legitimate requests:
  - 100 requests (querying speed data) with the frequency of 1 → forwards all requests to the vehicle ✓
- Illegitimate requests:
  - 100 attempts to query other data → requests are dropped ✓
  - 100 queries with a high frequency → puts requests in a queue ✓

Case Study II: Experimental Results (Cont.)

Enhancing privacy: (i) shuffling, (iii) shuffling & rounding, (iii) noise addition

Noise addition: $V_i = V_i + Z_i$, where Z_i drawn from a uniform distribution with the range of R



Utility= No. of Speed Violations (Speed >30mph)

Case Study II: Amber Response

Stats:

43 children have been recovered every year

800,000 children are abducted in the U.S. every year

A more effective approach is highly needed

Case Study II: Amber Response (Cont.)

Three implementations:

- ❖ Cloud-based: On-cloud plate recognition
- ❖ SmartCore-based: Local plate recognition
- ❖ Hybrid: Plate area detection and color detection on SmartCore

SmartCore

#	Color
1	Black
2	Green

Few sensitive images:

- ❖ Enhanced privacy
- ❖ Reduced Costs
- ❖ Similar accuracy & Performance

ProCMotive can revolutionize vehicular industry

UbiComp 2018

U.S. Provisional Patent

Innovation Award (**2017**), IP Accelerator Award (**2018**)

Thank you!