UNSW SYDNEY

Australia's Global University

The Internet of Things (IoT)

Securing Devices and User Data

Mehdi Nobakht

24 September 2019

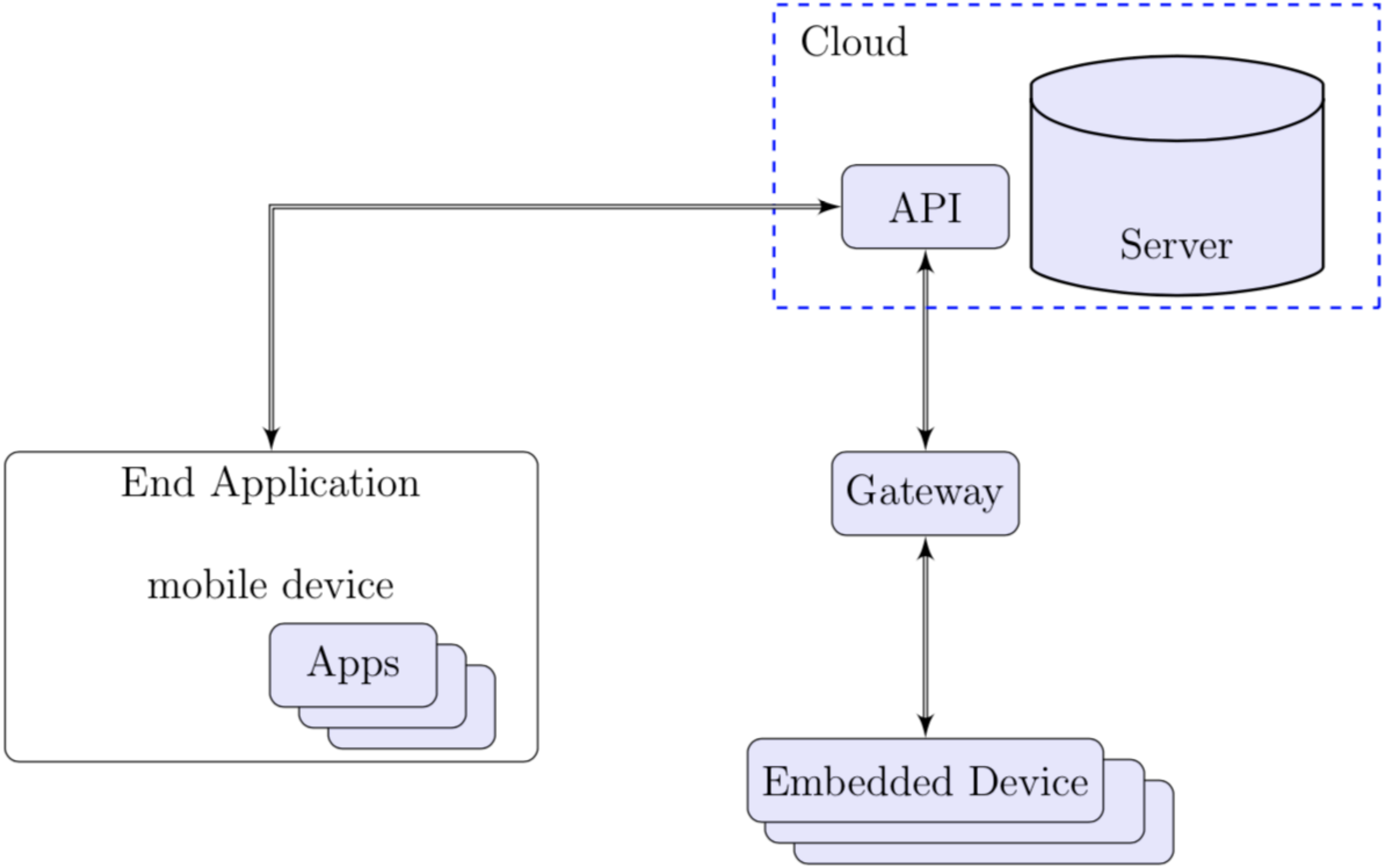
Who am I

- Mehdi Nobakht
  - Graduated in Electronics Engineering (2000)
  - Master in IT (2013)
  - Ph.D. in Computer Science (2018)
- My previous work
  - Software developer (10 years)
  - Telephony signaling protocols such as SS7, V5.2, …
- Research Area
  - Cyber-physical Systems/Internet of Things (IoT) Security
  - Adversarial Machine Learning and Data Security
  - Computer Networks
    - Software Defined-networking (SDN)
  - Distributed Ledger Technology (DLT)

Outline

- The Internet of Things (IoT)
  - A Security Disaster
- Unauthorized Access to Smart Devices
  - A background to SDN
  - Our solution: IoT-IDM
- Unauthorized Access to Smart Home Network
  - Our solution: IoT-NetSec
- Unauthorized Access to Users' Personal Data
  - Our solution: PGFit

The Internet of Things (IoT)



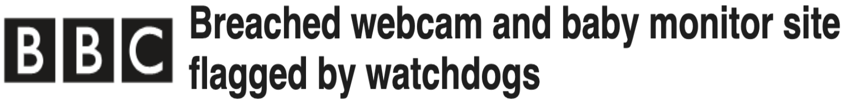
The Internet of Things (IoT)

- Emerging IoT solutions
  - Innovation
  - Efficiency
  - Cost-saving
  - Security

- IoT Security is hard
  - Resource Limitations
  - Mobility
  - Heterogeneity
  - Scalability

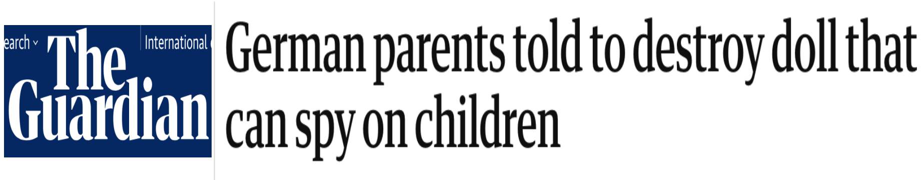
A Security Disaster

- Enormous attack surface
  - Device-level attacks
  - Network-level attacks



BBC

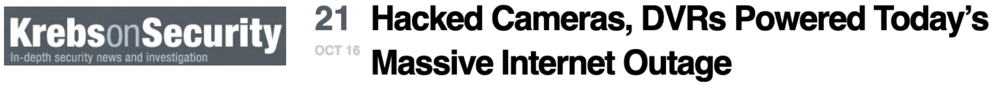
Breached webcam and baby monitor site flagged by watchdogs



earch International

The Guardian

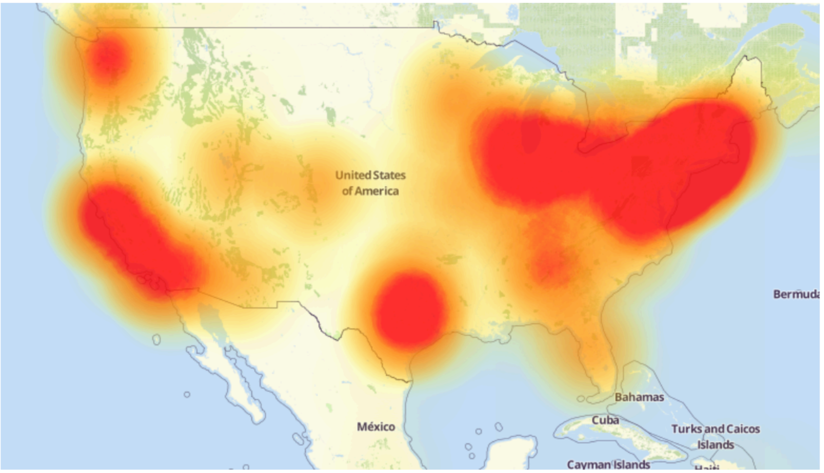
German parents told to destroy doll that can spy on children



KrebsonSecurity
In-depth security news and investigation

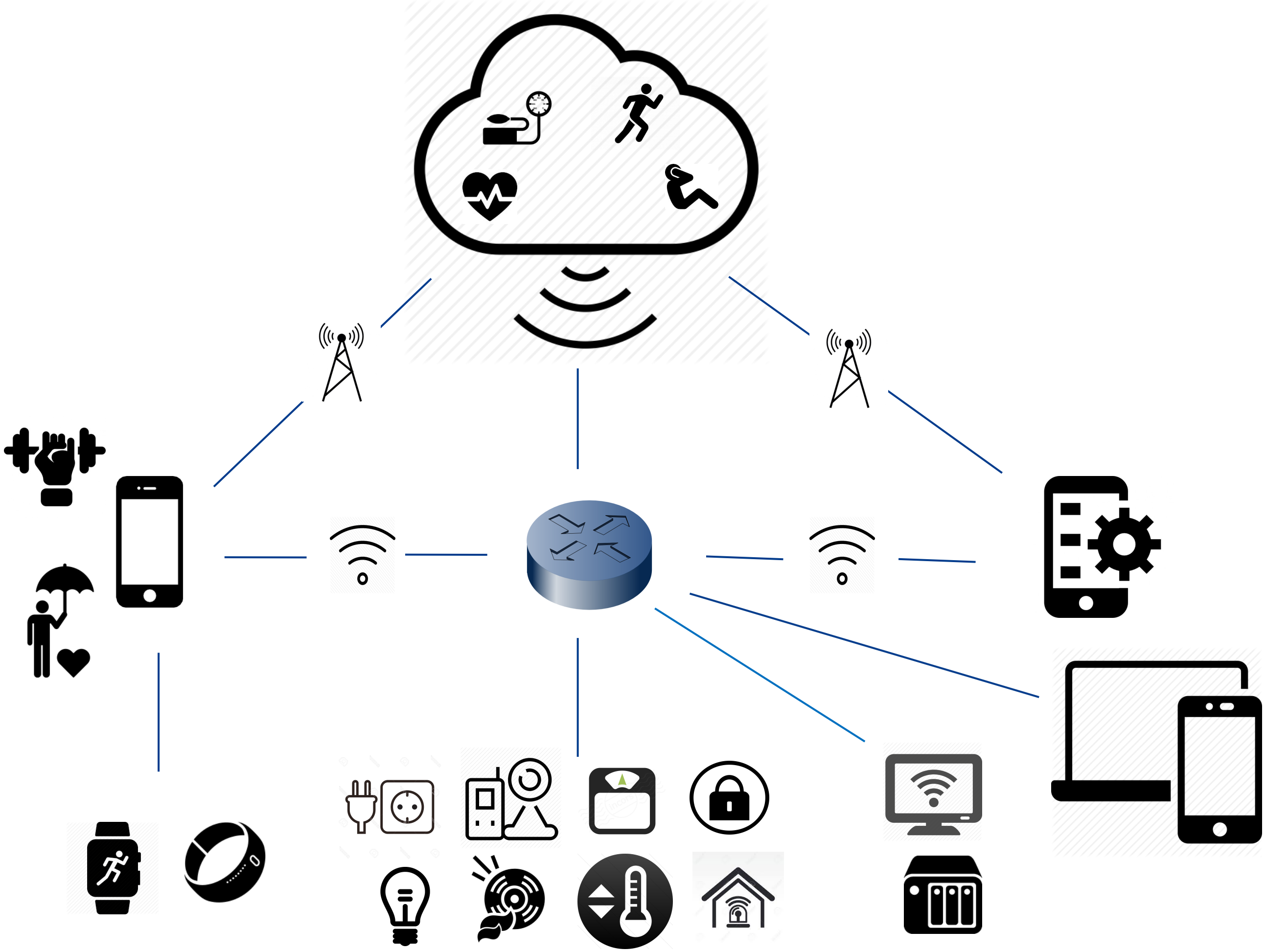
21 OCT 16

Hacked Cameras, DVRs Powered Today's Massive Internet Outage

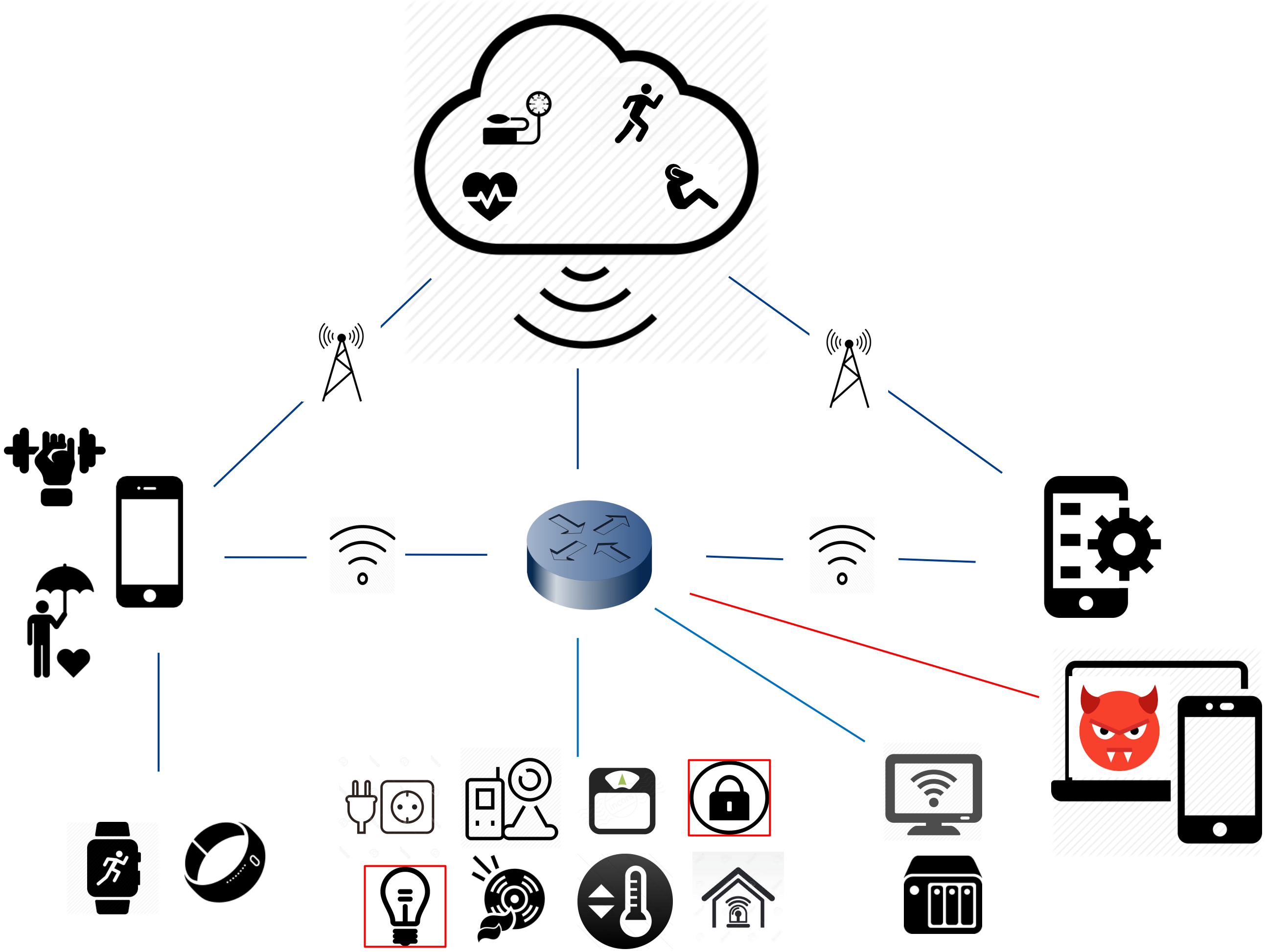


A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downdetector.com.

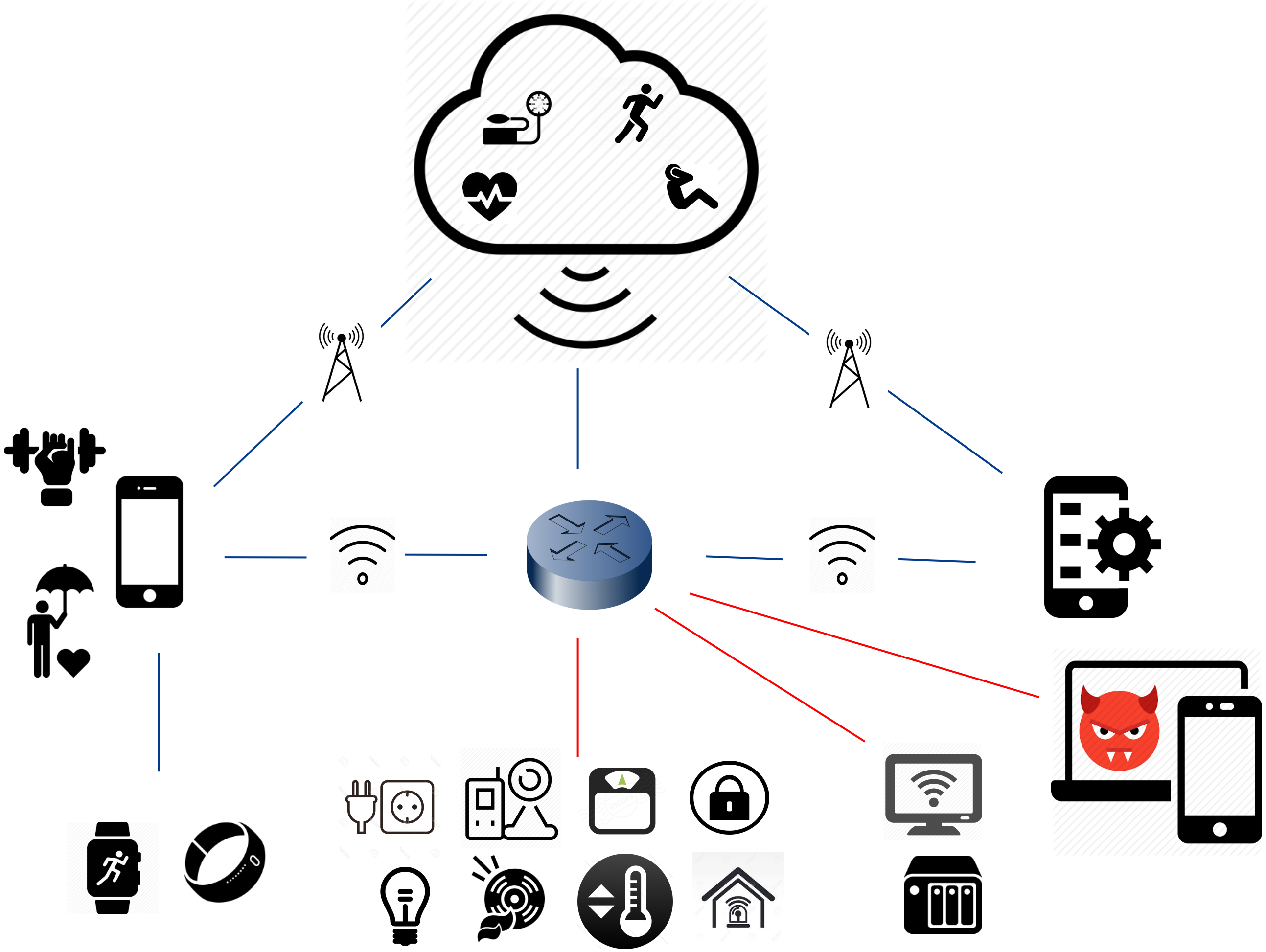
Home Area Network



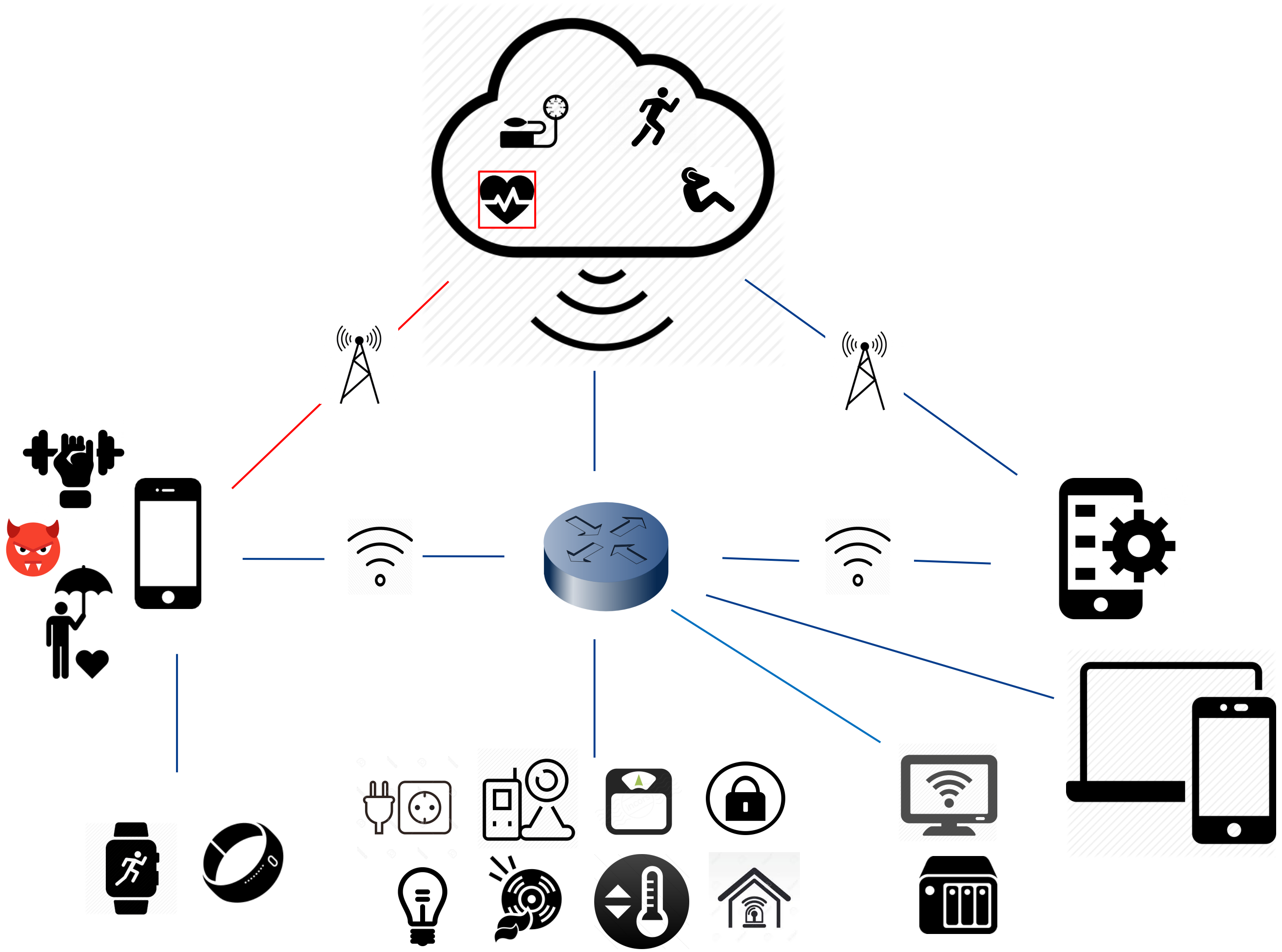
1. Unauthorized Access to Smart Devices



2. Unauthorized Access to Smart Home Networks



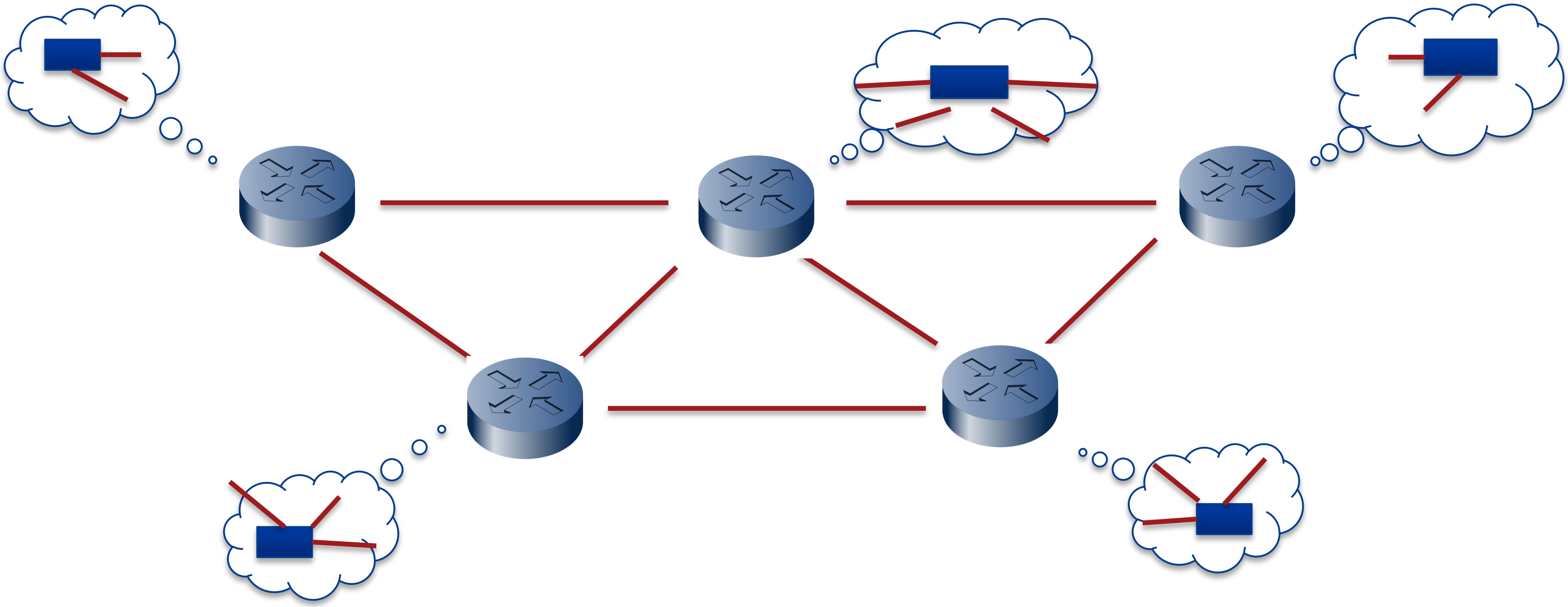
3. Unauthorized Access to Users’ Personal Data



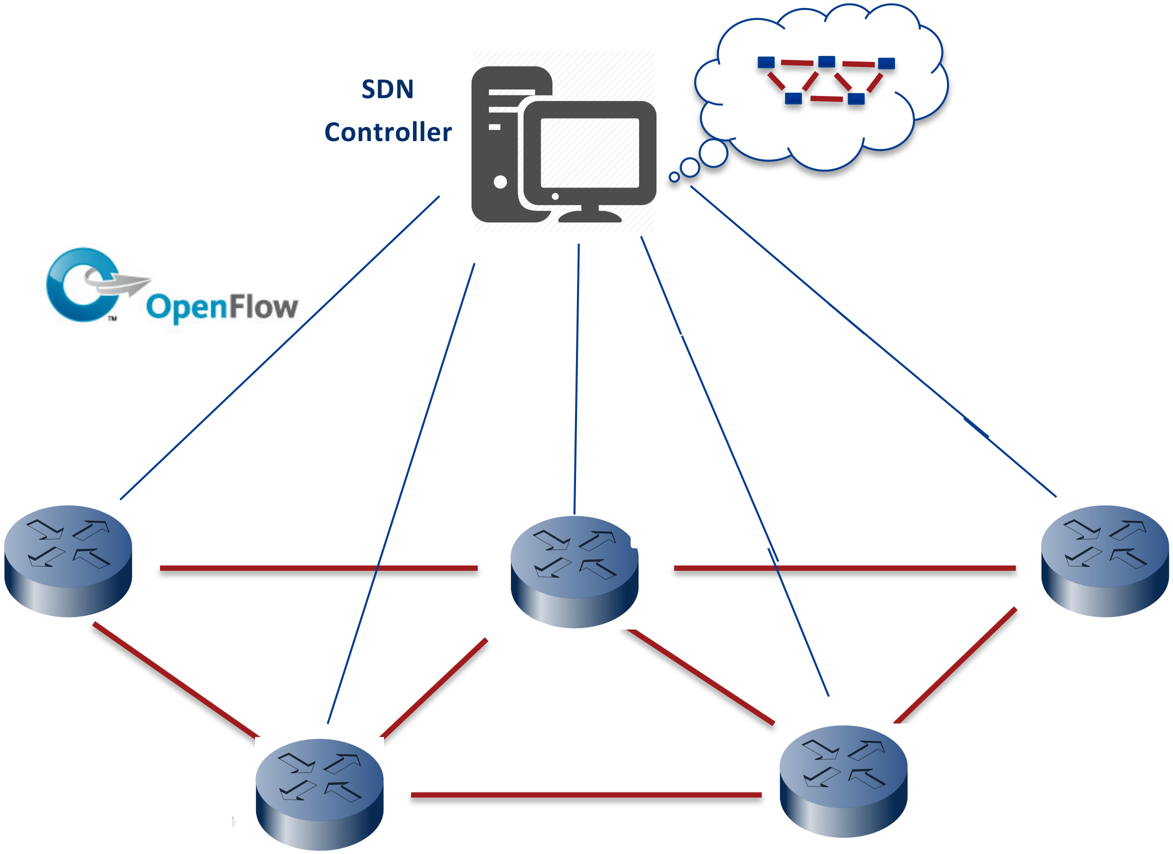
1. Unauthorized Access to Smart Devices

- Possible solutions:
  - Secure OS
    - Nature of devices
    - Legacy devices
  - Crypto
    - Nature of devices
    - Power
  - Access Control List (ACL)
    - Needs redesign
- Most of approaches to IoT security needs redesign or modification
  - Scalability challenge
  - Affordability
- Network-level – A new possibility

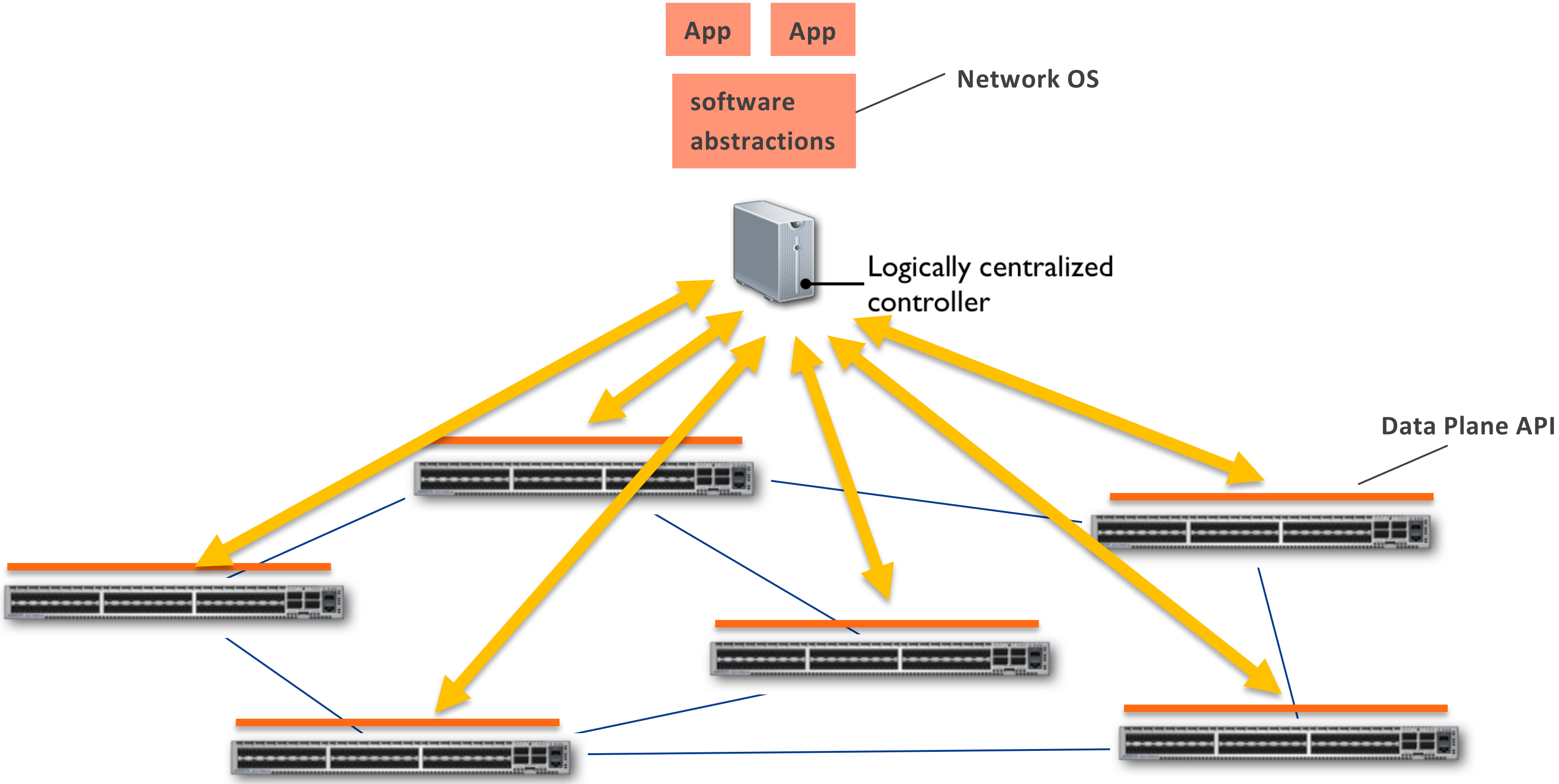
Legacy Network



Software Defined Networking (SDN)

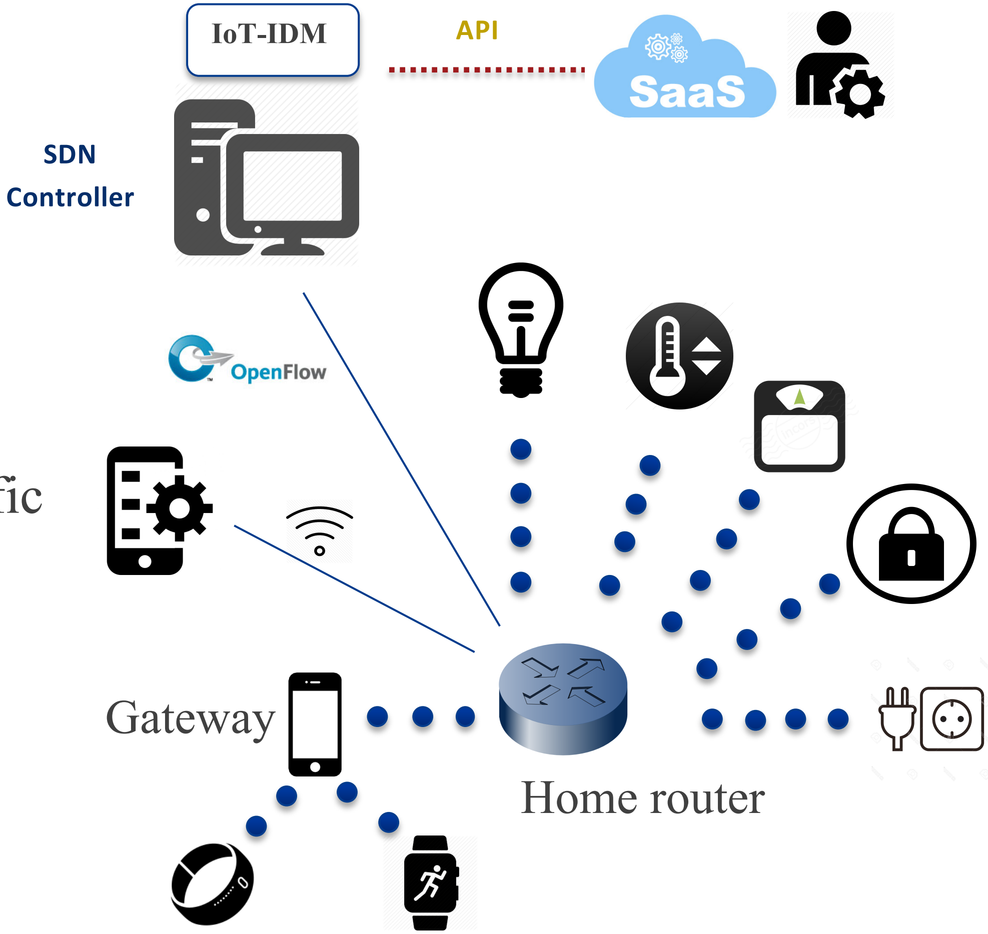


SDN Architecture



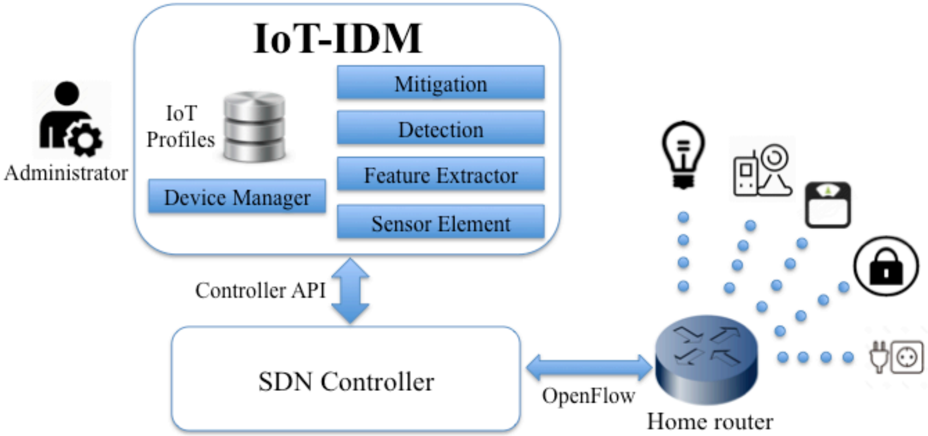
1. Unauthorized Access to Smart Devices

- IoT devices of interest
- Off-line examination for potential vulnerabilities
- Unauthorized access to devices
- Predictive models fo detection
  - Signature-based
  - Anomaly-based
  - Stateful (DPI)
- OpenFlow rules, port mirroring traffic
- Monitoring network activities
  - Suspicious activities
  - Malicious activities



IoT-IDM

- Intrusion Detection and Mitigation For Smart Home IoT **Devices**
- Inspect application layer protocol, e.g. HTTP
- Potential vulnerabilities due to unauthorized access
- Attack model: an adversary can infer users’ credential
- Our solution



- **M. Nobakht**, V. Sivaraman and R. Boreli, "A Host-Based Intrusion Detection and Mitigation Framework for Smart Home IoT Using OpenFlow," *2016 11th International Conference on Availability, Reliability and Security (ARES)*, Salzburg, 2016, pp. 147-156.

IoT-IDM accuracy

- Case study
  - Philips Hue light bulb
- Accuracy of IoT-IDM in detecting unauthorized attacks
- Precision = $TP/(TP + \mathrm{FP})$
  - What fraction of accesses to Hue that considered as attacks were actually illegitimate access
- Recall = $TP/(TP + \mathrm{FN})$
  - What fraction of all illegitimate accesses to Hue are correctly detected as attack

	precision	recall
Linear logistic regression	94.25%	85.05%
SVM	98.53%	95.94%

2. Unauthorized Access to Smart Home Network

- Network Service Attacks
  - Network reconnaissance
  - Heavy hitters
    - Denial of Service (DoS)
    - Distribute Dos (DDoS)
    - Port Scanning
- IoT Security Solutions
  - Entire IoT echo system
  - At network-level → SDN, OpenFlow Protocol
- Challenges in SDN-based approaches
  - Today's network → a mixture of network applications

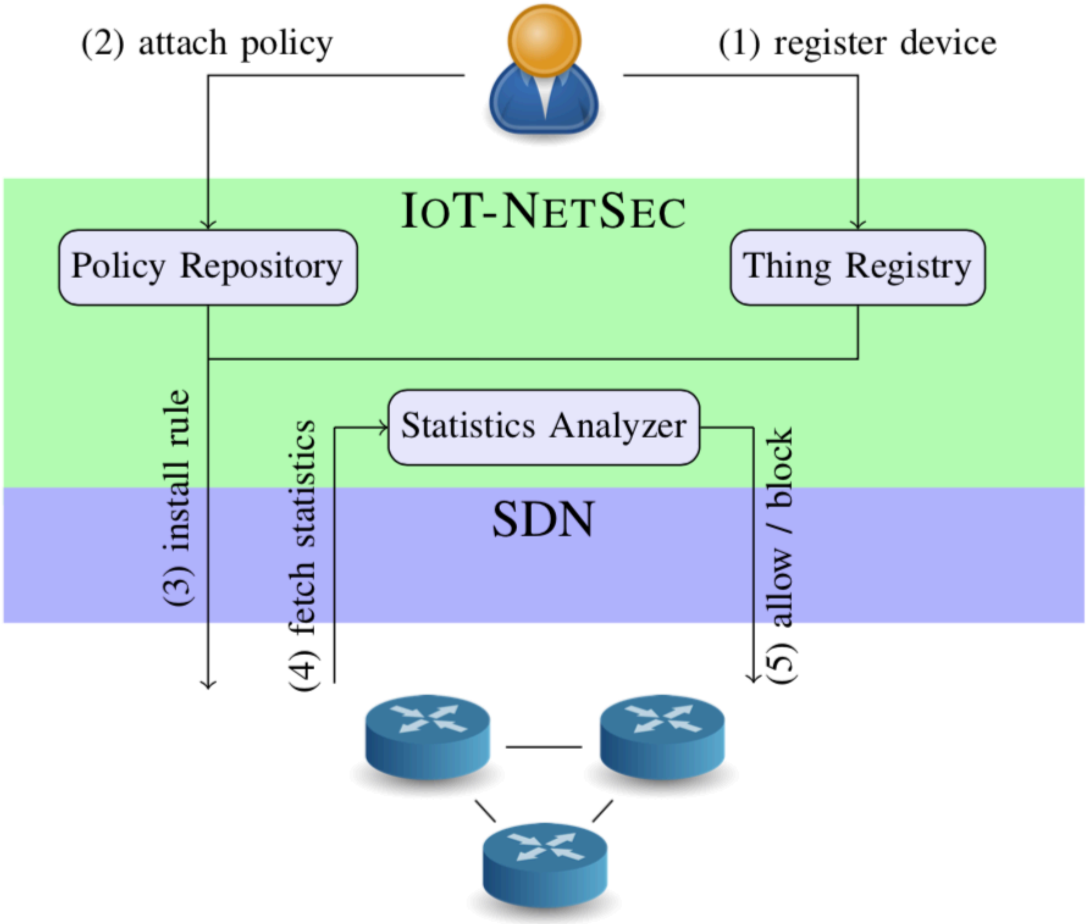
Challenges in SDN Approaches

- Is it practical to incorporate a general-purpose SDN-based security solution for today's networks?
  - High data volume and rate of today's home and enterprise network traffic
  - Traffic characteristics of IoT systems such as
    - intermittent connectivity
    - data usage pattern
    - most often low data rates
  - Limited resources for traffic measurement tasks, e.g., TCAM counters

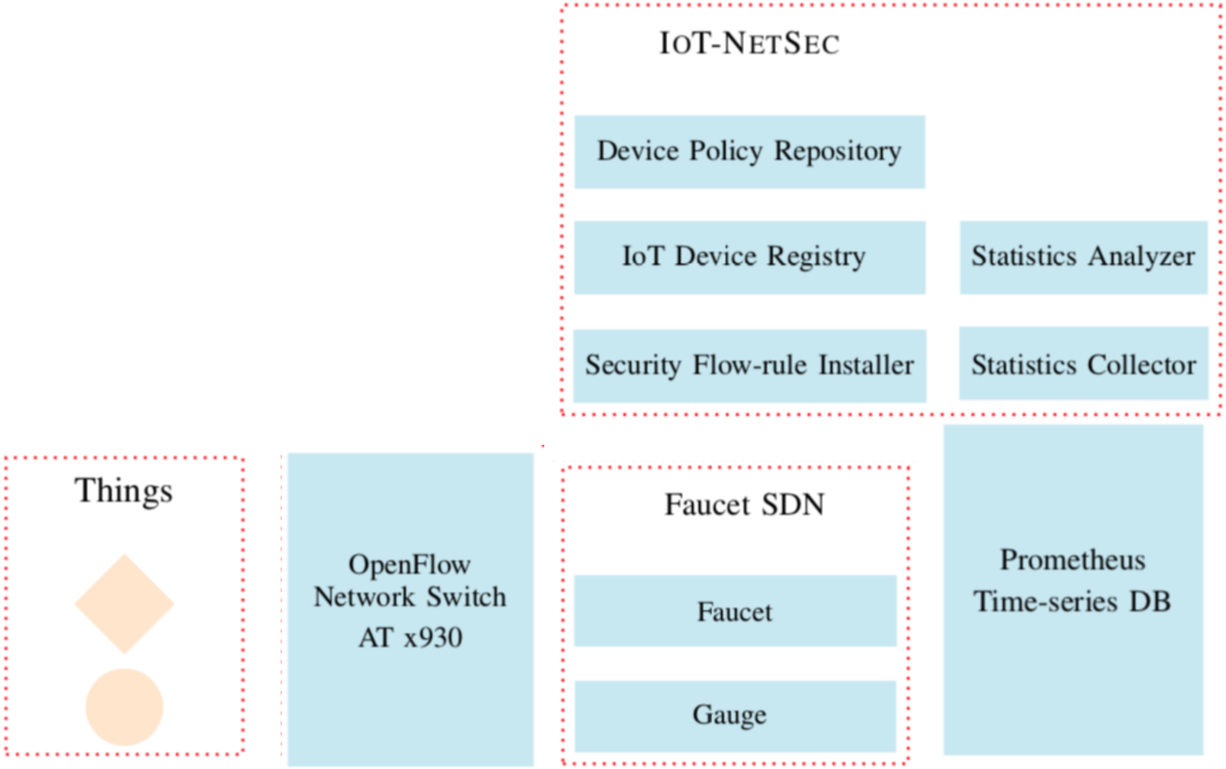
Our Idea: IoT-NetSec

- Network-level security monitoring only for a particular network segment which includes IoT devices
- Examines packet header fields including five tuples: source IP address, destination IP address, protocol, source port and destination port.
- Potential vulnerabilities
  - DoS, Port scanning, DDoS
- Attack model
  - an adversary has access to smart home network and runs attacks from compromised hosts within the network

IoT-NetSec


(2) attach policy
(1) register device
IoT-NetSec
Policy Repository
Thing Registry
Statistics Analyzer
(3) install rule
(4) fetch statistics
(5) allow / block
SDN

IoT-NetSec: Implementation



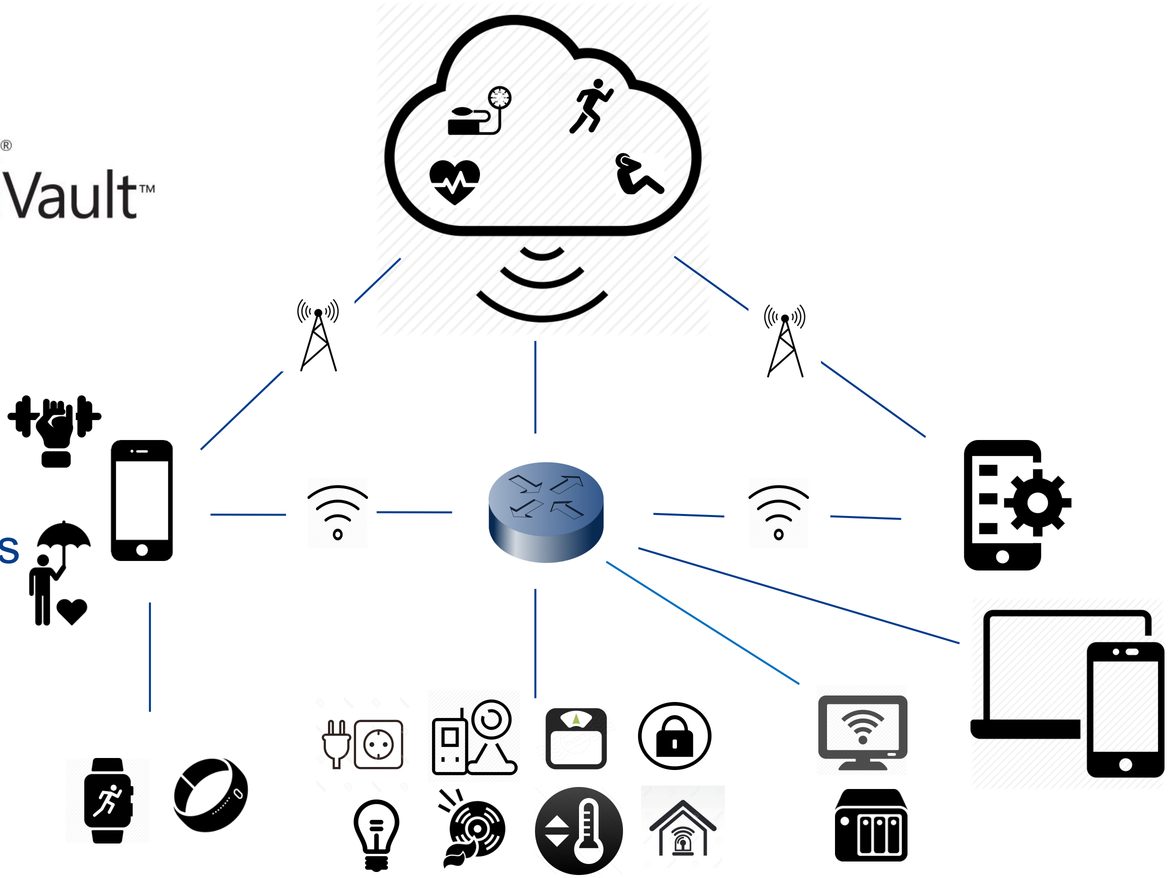
M. Nobakht, C. Russell, A. Seneviratne and W. Hu, "IoT-NetSec: Policy- based IoT Network Security using OpenFlow.", IEEE International Conference on Pervasive Computing and Communications Workshops, IEEE PerCom '19, Kyoto, Japan, 2019.

3. Unauthorized Access to Users’ Personal Data

Microsoft® HealthVault™

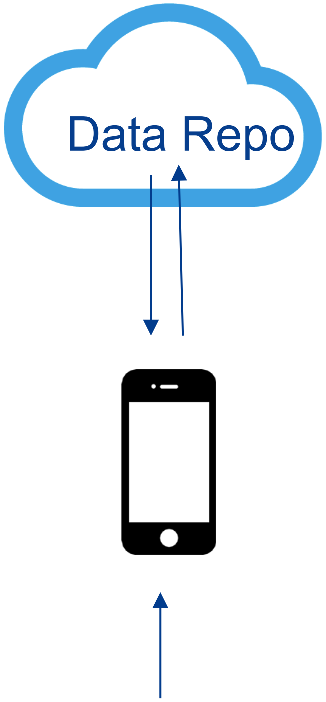
SAMSUNG

IoT Programming Frameworks



Google Fit

IoT Programming Frameworks



Data Repo

App

Activity

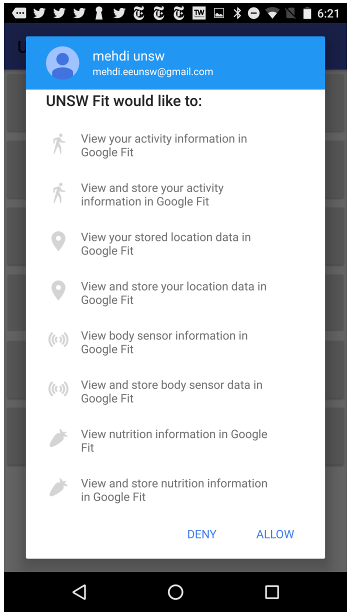
Biometric

Location

Nutrition

Read access

Write access



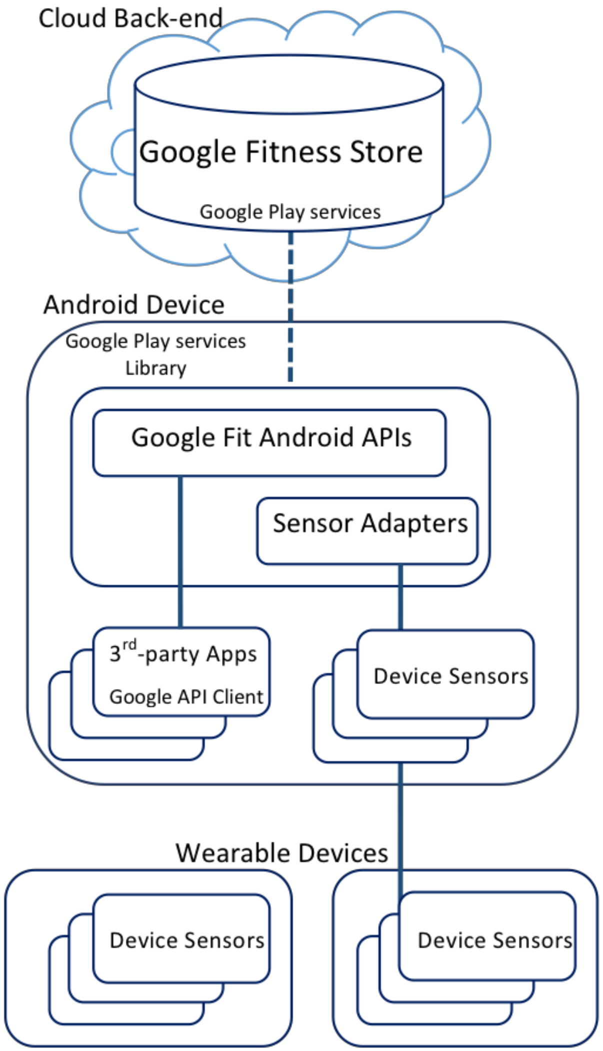
mehdi unsw
mehdi.eeunsw@gmail.com

UNSW Fit would like to:

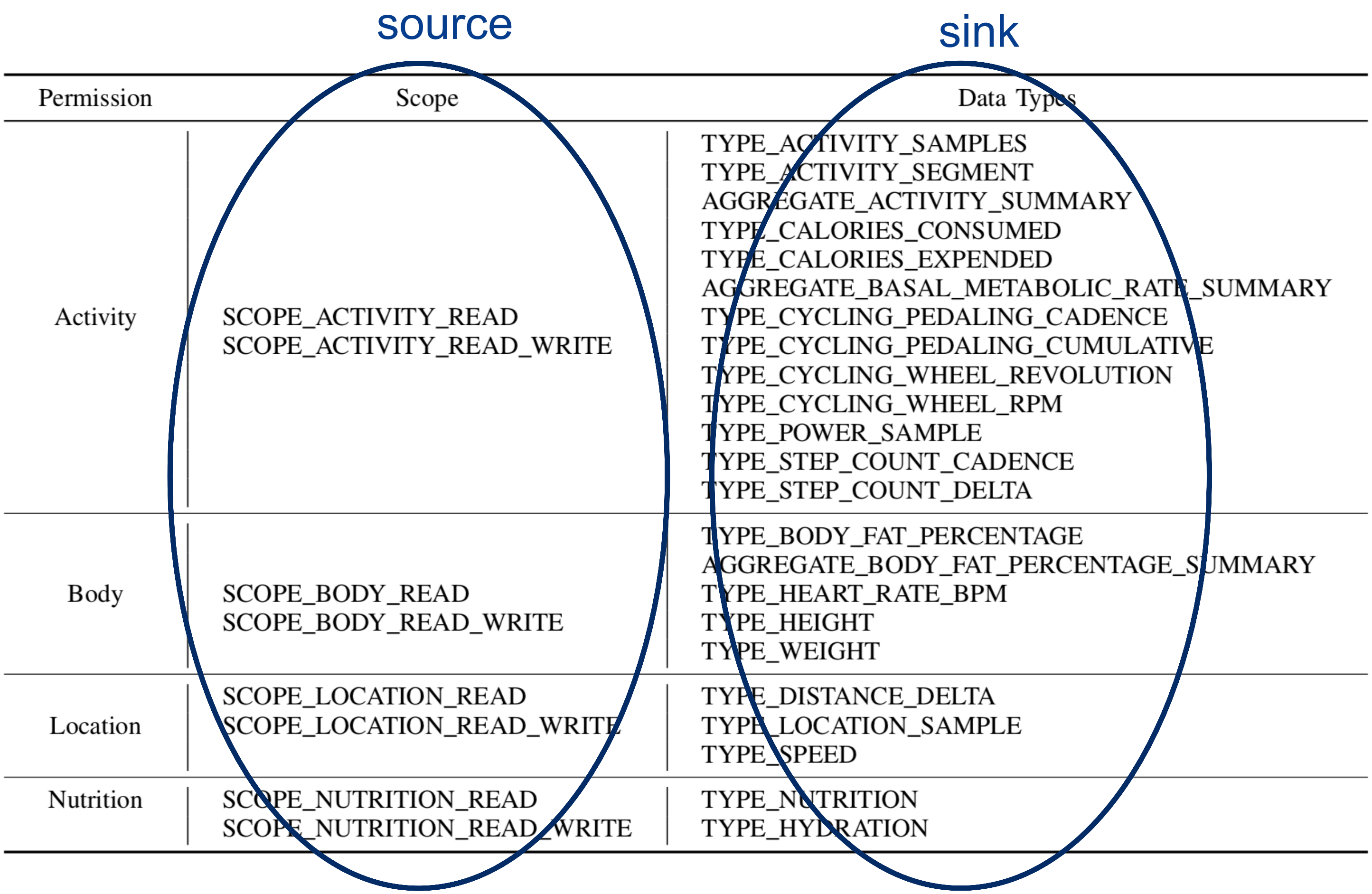
- View your activity information in Google Fit
- View and store your activity information in Google Fit
- View your stored location data in Google Fit
- View and store your location data in Google Fit
- View body sensor information in Google Fit
- View and store body sensor data in Google Fit
- View nutrition information in Google Fit
- View and store nutrition information in Google Fit

Google Fit

- *Data Sources*
- *Data Types*
- *Data Point*
- *Permissions and User Controls*
  - OAuth-based authentication



Google Fit

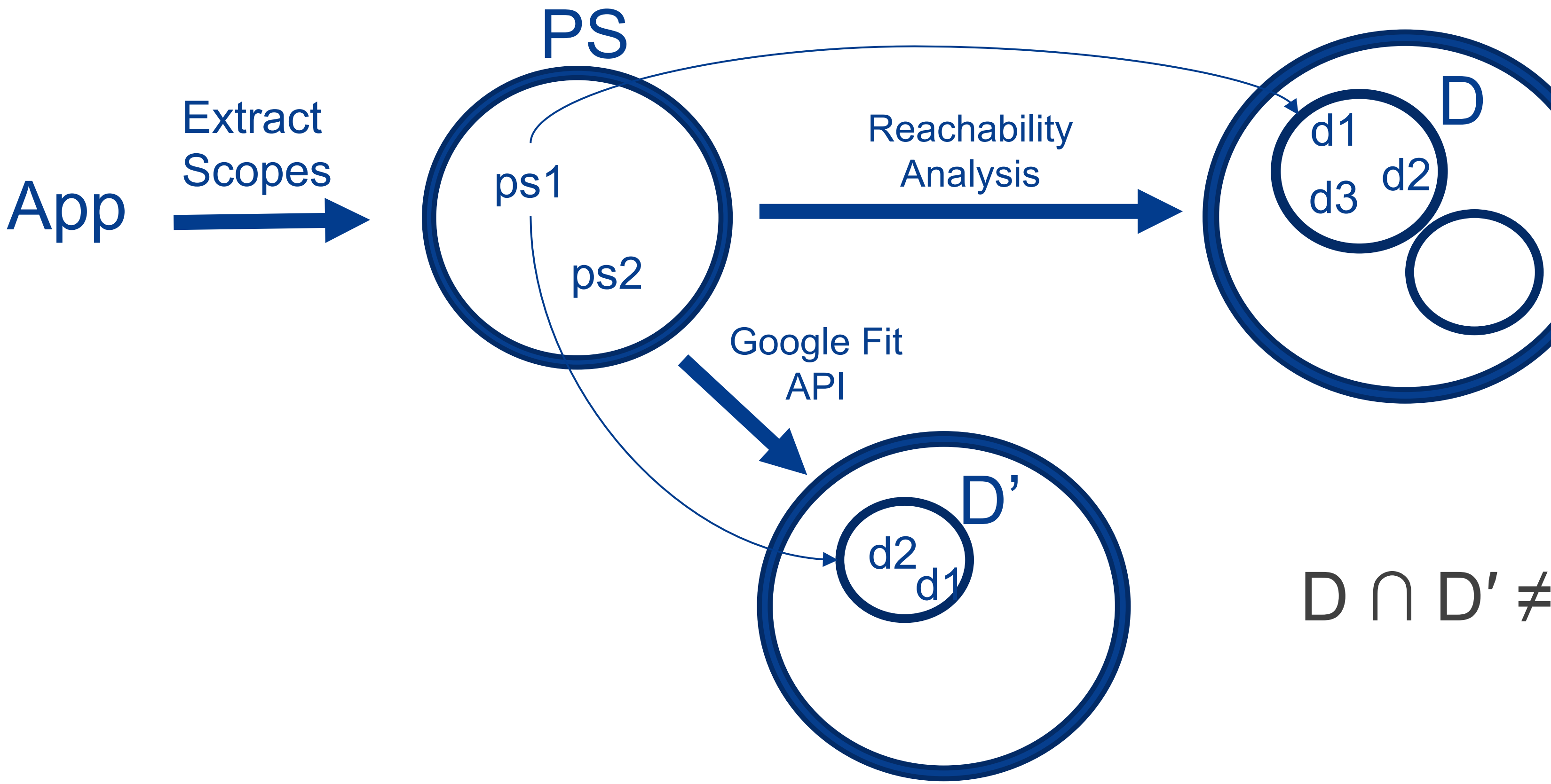


source

sink

Permission	Scope	Data Types
Activity	SCOPE_ACTIVITY_READ SCOPE_ACTIVITY_READ_WRITE	TYPE_ACTIVITY_SAMPLES TYPE_ACTIVITY_SEGMENT AGGREGATE_ACTIVITY_SUMMARY TYPE_CALORIES_CONSUMED TYPE_CALORIES_EXPENDED AGGREGATE_BASAL_METABOLIC_RATE_SUMMARY TYPE_CYCLING_PEDALING_CADENCE TYPE_CYCLING_PEDALING_CUMULATIVE TYPE_CYCLING_WHEEL_REVOLUTION TYPE_CYCLING_WHEEL_RPM TYPE_POWER_SAMPLE TYPE_STEP_COUNT_CADENCE TYPE_STEP_COUNT_DELTA
Body	SCOPE_BODY_READ SCOPE_BODY_READ_WRITE	TYPE_BODY_FAT_PERCENTAGE AGGREGATE_BODY_FAT_PERCENTAGE_SUMMARY TYPE_HEART_RATE_BPM TYPE_HEIGHT TYPE_WEIGHT
Location	SCOPE_LOCATION_READ SCOPE_LOCATION_READ_WRITE	TYPE_DISTANCE_DELTA TYPE_LOCATION_SAMPLE TYPE_SPEED
Nutrition	SCOPE_NUTRITION_READ SCOPE_NUTRITION_READ_WRITE	TYPE_NUTRITION TYPE_HYDRATION

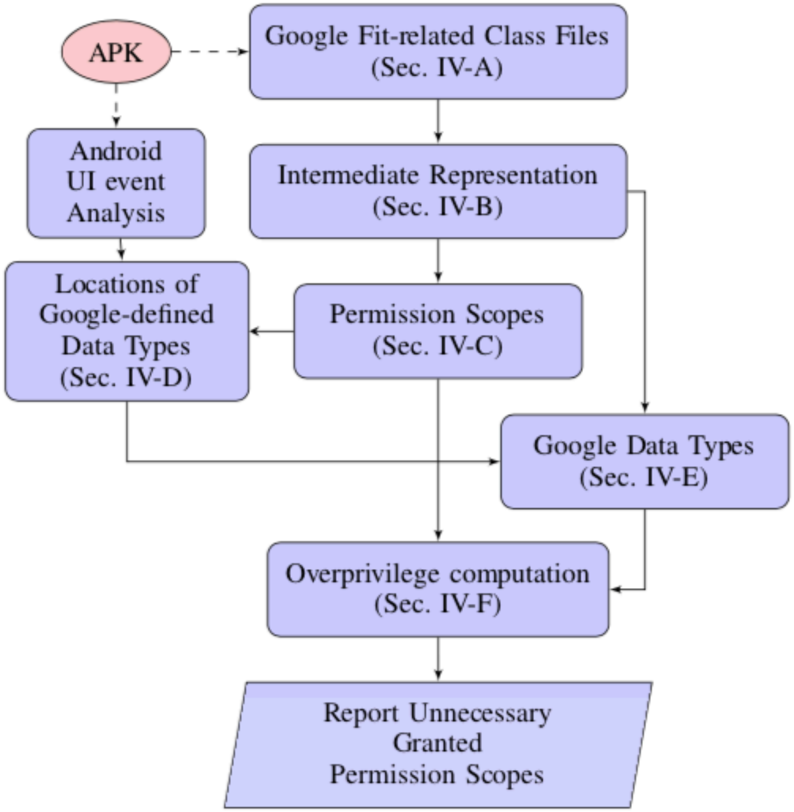
Permission Analysis



$D \cap D' \neq \emptyset$

PGFit: Static Permission Analysis

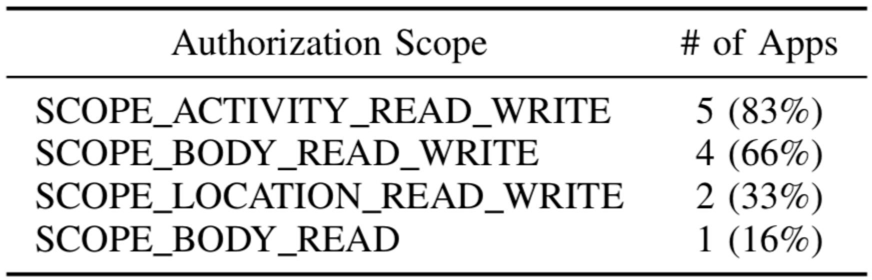
- *Identifying Google-related Class Files*
- *Intermediate Representation*
- *Extracting Permission Scopes*
- *Identifying the Location of Google-defined Data Types*
- *Extracting Google-Defined Data Types*
- *Overprivilege Computation*


APK
Google Fit-related Class Files (Sec. IV-A)
Android UI event Analysis
Intermediate Representation (Sec. IV-B)
Locations of Google-defined Data Types (Sec. IV-D)
Permission Scopes (Sec. IV-C)
Google Data Types (Sec. IV-E)
Overprivilege computation (Sec. IV-F)
Report Unnecessary Granted Permission Scopes

PGFit: Static Permission Analysis

- Applied PGFit to a set of 20 Google-enabled fitness applications
  - 14 applications contained Google Fit API calls in one compiled class file
  - 6 applications Google Fit API calls and data types were distributed in more than one class
  - 6 applications (30%) request at least one authorization scope but never use any data types corresponding to that scope.

UNNECESSARY SCOPE PERMISSIONS IN 20 APPS



Authorization Scope	# of Apps
SCOPE_ACTIVITY_READ_WRITE	5 (83%)
SCOPE_BODY_READ_WRITE	4 (66%)
SCOPE_LOCATION_READ_WRITE	2 (33%)
SCOPE_BODY_READ	1 (16%)

M. Nobakht, Y. Sui, A. Seneviratne and W. Hu, "Permission Analysis of Health and Fitness Apps in IoT Programming Frameworks". The 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE TrustCom '18, New York, 2018, pp. 533-538.

UNSW SYDNEY

Australia's Global University

Thank You

Mehdi Nobkht

Postdoctoral Research Fellow

UNSW Canberra

e mehdi.nobakht@unsw.edu.au

w https://mehdi-nobakht.github.io/